E 870

HÍRADÁSTECHNIKA

XLVI. ÉVFOLYAM 1995. MÁRCIUS

VÉDETT ÁTVITEL

Bevezető gondolatok ..... Kása I. 1

A hírközlő csatornák fizikai védelme, szórt spektrumú eljárások ..... Pap L. 2

Szimmetrikus kulcsú blokk rejtjelzők tervezési kritériumai ..... Vajda I. és Buttyán L. 10

Gondolatok az adatátvitel védettségéről ..... Papp Gy. 19

Információs és adatforgalmi rendszerek kriptográfiai védelme ..... Dudás J. 27

Informatikai biztonság, kommunikáció biztonság ..... Szekér K. 35

Gazdaság – Kutatás – Oktatás

Bankinformatikus képzés a Műegyetemen 40

Termékek – Szolgáltatások

Az EUROHÍVÓ digitális személyhívó szolgáltatás ..... Wilk Nóra 41

Hírek – Események

Könyvismertetés a Híradástechnika c. könyvről ..... Ladvánszky J. 43

Továbbképzés menedzsereknek ..... Béres A. 43

Nemzeti Informatikai Stratégia kezdeményezése 44

A MTESZ információs rendszere 44

HÍRADÁSTECHNIKA

A HÍRADÁSTECHNIKAI TUDOMÁNYOS EGYESÜLET FOLYÓIRATA

Főszerkesztő
BARANYI ANDRÁS

Rovatvezetők
BATTISTIG GYÖRGY
KORMÁNY TERÉZ
PRÓNAY GÁBOR
SOMOGYI ANDRÁS

Szerkesztők
BARTOLITS ISTVÁN
KÁSA ISTVÁN
LADVÁNSZKY JÁNOS
FÖLDVÁRINÉ OROSZ JULIANNA
ANTALNÉ ZÁKONYI MAGDOLNA
WILK NÓRA

Munkatárs:
LESNYIK KATALIN

Szerkesztőbizottság
TÓFALVI GYULA
elnök

BERCELI TIBOR
FRAJKA BÉLA
FRIGYES ISTVÁN
GORDOS GÉZA
MOJZES IMRE
PAP LÁSZLÓ
SALLAI GYULA

SZPONZOROK

MAGYAR TÁVKÖZLÉSI RÉSZVÉNYTÁRSASÁG

antenna hungária

ERICSSON

Ericsson Technika

SIEMENS

Siemens Telefongyár Kft

WESTEL
RÁDIÓTELEFON KFT

TKI

BHG
BUDAPEST

"AZ ÉPÍTÉS FEJLŐDÉSÉÉRT" ALAPÍTVÁNY

MAGYAR SAJTÓALAPÍTVÁNY

Szerkesztőség
Budapest XIV., Ungvár u. 64-66.
Telefon: 251-1163
201-7471
Telefax: 251-9878
201-7471

Előfizetési díj
Hazai közületi előfizetők részére
1 évre 6000,– Ft, egyes számok 650,– Ft
Hazai egyéni előfizetők részére
1 évre 960,– Ft, egyes számok 110,– Ft
Külföldi előfizetők részére
1 évre 6 angol szám 90 USD, 12 szám 150 USD, egyes számok 24 USD

HÍRADÁSTECHNIKA megjelenik havonta váltakozva magyar és angol nyelven. Kiadja a TypoTEX Elektronikus Kiadó Kft. 1024 Budapest, Retek u. 33-35. Telefon: Telefon/Fax: 115-1759. Felelős kiadó: Votisky Zsuzsa. Készült a Dabasi Jegyzetnyomdában. Szövegszedés: TypoTEX Elektronikus Kiadó Kft. A lap példányonként megvásárolható a kiadónál.
HU ISSN 0018-2028

BEVEZETŐ GONDOLATOK

ORSZÁGOS MŰSZAKI INFORMÁCIÓS KÖZPONT ÉS KÖNYVTÁR 1883

A hogyan a távközlési technika különféle alkalmazásai mindinkább átszövik életünket, fokozódó élességgel vetődik fel a távközlés biztonságának, védettségének kérdése. Míg régebben a távközlés védettsége elsősorban katonai vagy nemzetbiztonsági szempontból volt fontos, ma már a gazdasági szempontok, az üzleti alkalmazások is egyre indokoltabbá teszik, hogy fokozott figyelmet szenteljünk a távközlés biztonsági vonatkozásainak. A távközlés jövőjéről az Európa Unió számára készült Bangemann-jelentés ezzel kapcsolatban két fontos szempontra hívja fel a figyelmet, az egyik a személyiséghez fűződő jogok védelme, a másik pedig a távközlésnek az üzleti életben elfoglalt szerepe és növekvő fontossága. Az információs társadalom kiteljesedésével a társadalom és az egyén életére egyre nagyobb hatással van az információ továbbítása. Ebből következik, hogy mind az egyénnek, mind a társadalom egészének elsőrendű érdeke, hogy ez az információ-átvitel zavartalan legyen, mégpedig nemcsak úgy, hogy az üzenet torzításmentesen eljusson a címzetthez, hanem abban az értelemben is, hogy a továbbított adatok vagy ismeretek ne juthassanak kívülállók tudomására.

Az információ érték a távközlésben résztvevő felek számára és ezért védelemre szorul, függetlenül attól, hogy ismert-e egy potenciális támadó. Már egy zárt hálózatban is gondot jelenthet a távközlés biztonsága, bár itt a technológiából adódóan a hozzáférés korlátozott, az átviteli csatorna fizikailag bizonyos mértékig védhető, például fényvezetős átvitel vagy szórt spektrumú vezetéknélküli rendszer alkalmazásával. A fejlődés újabb irányai, a nyitott hálózatok térnyerése, az ezekre épülő új szolgáltatások megjelenése valamint a felhasználók növekvő mobilitása mind sebezhetőbbé teszik a távközlést.

Az üzleti vagy banki alkalmazásokban már ma is nagyértékű tranzakciókat bonyolítanak a távközlési csatornákon, a kereskedelmi távközlés (pl. távvásárlás) előrejelzett széleskörű elterjedésével a közvetlen gazdasági érdekeltség és sebezhetőség is egyre kiterjedtebb alkalmazói kört érint. Mindezek alapján nem túlzás az az állítás, hogy az információátvitel biztonsága a távközlés egyik központi kérdése. A távközlés védelme két szempontból is fontos szerepet játszik: egyrészt a távközlési csatornákban az információ kilép az információs csomópontok védett környezetéből, ezért a távközlési csatornában áramló információ fokozott veszélynek van kitéve; másrészt a távközlési csatornák kaput képeznek a külvilág és az információs csomópont között, ezeken keresztül lehet a csomópontokba is behatolni, az adatbázisokat veszélyeztetni.

A távközlés biztonságának új dimenziót ad a nemzetközi méretekben kiépülő információs autópálya (information superhighway), amely lényegében egy nagy átviteli kapacitású, nagy konnektivitású és széleskörűen hozzáférhető átviteli közeget jelent. Az információs autópálya lelkes ismertetése során általában a széleskörű és könnyen megvalósítható információcsere kétségtelen előnyeit szokták hangsúlyozni, azt a kedvező hatást, amelyet ez a nagyszerű lehetőség az információs társadalom kialakulására gyakorol. Nem nehéz azonban rádöbbenni arra, hogy egy ilyen távközlési közeg, amelyen hatalmas mennyiségű információ áramlik, és a sokirányú gazdasági tranzakciók színhelye, az információ kalózainak is nagyobb lehetőséget kínál, növeli a fenyegetést és támadás lehetőségét. A problémák egy része már az Internet hálózatban is megfigyelhető, és a szakértők nagy nyomatékkal hívják fel a figyelmet a biztonsági kérdések fontosságára.

A biztonságos távközlést és különösen a védett adatkommunikációt sokszor leegyszerűsítik egy alkalmas rejtjelzési, kriptográfiai technológia alkalmazására. Elismerve, hogy a kriptográfia a biztonságos távközlés nélkülözhetetlen eleme, hangsúlyozni kell, hogy önmagában nem képes a távközlés védelmére, a biztonságos távközlés megvalósítására. A védett távközlés, vagy pontosabban a távközlés védettségének egy bizonyos szintje összehangolt intézkedések sorozatával valósítható meg, amelyben a szervezeti és rendszertechnikai lépések ugyanolyan fontos szerepet játszanak, mint egy alkalmas átviteli vagy kriptográfiai technológia kiválasztása.

A védett távközlés és védett adatkommunikáció kérdései néhány speciális nagyérzékenységű területtől (pl. banktechnika, államigazgatás) eltekintve, nem kerültek a hazai távközlési szakemberek figyelmének központjába. Kétségtelen, hogy a közeljövőben még az említett területek igénylik a legnagyobb figyelmet és még itt is sok a tennivaló, de fontosnak tartjuk, hogy ezen túlmenően a távközlés biztonsági kérdései a szakemberek minél szélesebb körében tudatosuljanak. Ma már a védett távközlés és még ezen belül a védett adatkommunikáció is az ismereteknek olyan széles spektrumát igényli, amely egy ilyen korlátozott terjedelmű tematikus számban nem fedhető le, de szándékunk szerint ezek a bevezető cikkek megmutatnak néhány fontos szempontot és hozzájárulnak ahhoz, hogy a szakmai közösség tudatosan fogadja ezt a kihívást.

KÁSA ISTVÁN

Kása István a Budapesti Műszaki Egyetemen szerzett villamosmérnöki oklevelet 1960-ban. Ugyancsak itt szerzett mikrohullámú szakmérnöki oklevelet és doktori fokozatot. A műszaki tudomány kandidátusa fokozatot 1974-ben kapta meg. 1960 és 1991 között a Távközlési Kutató Intézetben (TKI) dolgozott különféle kutató, illetve vezető beosztásokban és számos kutatás-fejlesztési programban vett részt az alábbi témákban: mikrohullámú mérések, mikrohullámú aktív és passzív integrált áramkörök, mikrohullámú vevőrendszerek, mikrohullámú távközlés. 1991 júniusa óta a Magyar Távközlési Részvénytársaság PKI Távközlésfejlesztési Intézetében (PKI-FI) tudományos tanácsadó, a digitális földfelszíni és műholdas távközlés kérdéseivel foglalkozik. Mintegy 50 szakmai cikk, 10 találmány és két szakkönyv szerzője, a BME címzetes docense, valamint a HTE tagja.

A HÍRKÖZLŐ CSATORNÁK FIZIKAI VÉDELME, SZÓRT SPEKTRUMÚ ELJÁRÁSOK

PAP LÁSZLÓ

BUDAPESTI MŰSZAKI EGYETEM
HÍRADÁSTECHNIKA TANSZÉK
1111 BUDAPEST, SZTOCZEK U. 2.

A cikk áttekintést ad a szórt spektrumú elven működő rádiós kommunikációs rendszerek működéséről, felhasználási területeiről, típusairól és az átvitel legfontosabb paramétereiről, különös tekintettel a biztonságos hírközlés két fontos elemére, a külső zavarokkal szembeni ellenállóképességre és a többutas terjedéssel kapcsolatos védettségre.

1. BEVEZETÉS

A biztonságos hírközlési eljárások között a negyvenes évek óta kiemelkedő jelentőségűek a kiterjesztett (szórt) spektrumú vezetéknélküli technológiák (Spread Spectrum Technologies), melyek az elmúlt években — a hagyományos katonai alkalmazásokon túl — egyre fontosabb szerepet töltenek be a polgári gyakorlatban is.

A szórt (kiterjesztett) spektrumú átviteli rendszerek alaptulajdonsága, hogy a bennük alkalmazott speciális csatornakódolási (modulációs) eljárások következtében a csatornában felhasznált teljes sávszélesség, B (Hz) nagyobb, esetleg nagyságrendekkel nagyobb, mint a hagyományos modulációs rendszerekkel létrehozott jelek sávszélessége azonos R_b (bit/sec) sebességű alapsávi forgalom esetén (bináris rendszerekben leegyszerűsítve B (Hz)$\gg R_b$ (Hz)). A szórt spektrumú rendszerek legfontosabb paramétere az ún. sávszélesítési tényező $ST = B/R_b$, amely az előbb említett speciális csatornakódolási (modulációs) módszerek alkalmazása következtében fellépő sávszélesség-növekedést méri. A szórt spektrumú jelekben rejlő nagy redundanciát arra használjuk fel, hogy még abban az esetben is elfogadható átviteli minőséget biztosítsunk, ha az átviteli csatornában a normál Gauss-zajon kívül jelentős — a hasznos jel teljesítményét meghaladó — teljesítményű additív interferencia lép fel.

A szórt spektrumú átviteli rendszerek másik fontos tulajdonsága az álvéletlen (pseudo random) jelleg, ami annyit jelent, hogy az átviteli csatornában folyó kommunikáció egy rendszeren kívüli megfigyelő számára nagy sávszélességű, zaj jellegű véletlen folyamatnak tűnik, a rendszeren belüli partnerek viszont — ismerve a csatornakódolás szabályait — dekódolni tudják az átküldött információt.

A nagy kódolási redundancia jelentős védettséget ad a véletlen vagy szándékos külső zavarjelekkel, illetve a szórt spektrumú jeleket alkalmazó rádiós háló saját rendszerzajával szemben. Igaz ugyanis, hogy az átvitel során energianyereség (EG) keletkezik, ami azt jelenti, hogy adott hasznos jelteljesítmény (S) és zavaró teljesítmény (J) mellett a szórt spektrumú rendszerekben alkalmazott speciális demodulációs eljárások következtében a vevő demodulátorában a jel-zavar viszony ($(SJR)_d$) nagyobb, mint a csatorna jel-zavar viszonya ($(SJR)_{cs}$), és a két mennyiség hányadosa az energianyereségi tényező:

$$EG = \frac{(SJR)_d}{(SJR)_{cs}}$$

ami tipikusan azonos a sávszélesítési tényezővel (ST). Ez a zajelnyomási képesség jelenti a szórt spektrumú rendszerek egyik legfőbb alkalmazását. A szórt spektrumú jelek másik fő tulajdonsága, azaz az álvéletlen jelleg azt biztosítja, hogy idegen vevő számára a jel véletlen zajnak tűnik, és mivel a szórt spektrumú jel sávszélessége nagy, a teljesítmény spektrális sűrűsége alacsony, így mód van arra is, hogy a jelet a háttérzaj szintje alá rejtsük. Ezek mellett az alkalmazás egy igen fontos területe a szórt spektrumú jelekkel történő rádiólokáció és navigáció.

A spektrumszórás elvének főbb alkalmazási előnyeit az alábbiakban foglalhatjuk össze:

- Interferencia elnyomás
  - rendszeren kívüli jelekre (szándékos, illetve nem szándékos zavarás (AJ, Anti Jammig)),
  - rendszeren belüli jelekre (többszörös hozzáférés esetén a többi felhasználó jele (CDMA, Code Division Multiple Access)),
  - saját jelekre (többutas terjedésből származó jelekre).
- Teljesítménysűrűség csökkentés a csatornában abból a célból, hogy
  - eleget tegyük a nemzetközi (postai) előírásoknak (pl. műholdról a Földre érkező jelek esetében),
  - minimalizáljuk a jel detektálhatóságát a rendszeren kívüli személyek számára (spektrummonitorozás (AI, Anti Intercept)),
  - a jel teljesítménysűrűsége a környezeti zaj szintje alatt maradjon (zaj alatti hírközlés).
- Távolság- vagy sebességmérés.

A szórt spektrumú kommunikációs rendszereket tipikusan vezetéknélküli átvitelre használják a hosszúhullámú sávtól egészen a mikrohullámú tartományokig, de előfordulnak vezetékes alkalmazások is (pl. energiahálózati adatátvitel). Újabban a pont-pont közötti összeköttetéseken kívül terjedőben vannak a kommunikációs spread spectrum hálók, a rádiós LAN-ok.

2. AZ SST RENDSZEREK DEFINÍCIÓJA, FELÉPÍTÉSE ÉS TÍPUSAI

A kiterjesztett spektrumú technológia — a bevezetőben részletezett elveknek megfelelően — egyszerűen fogalmazva egy olyan új kódolási/modulációs eljárás —, amely digitális információk átvitelére szolgál oly módon, hogy a mo-

dulált jel sávszélességét a szükségeshez képest jelentősen megnöveli, ugyanakkor a modulált jelet fehér zajhoz teszi hasonlóvá. A spektrum kiterjesztése során a jel teljesítménye állandó marad, spektrális sűrűsége viszont lecsökken, ami azt eredményezi, hogy a kibővített sávú adás más keskenysávú rendszereket csak kis mértékben zavar, ugyanakkor a spektrum kiterjesztése számos előnnyel jár.

A spektrum kiterjesztésnek három alapmódszere ismert:

- Fázisugratásos vagy direkt szekvenciális rendszer, ahol az adó vivőjének a fázisát változtatjuk hirtelen egy álvéletlen kódsorozat szerint (PSK moduláció). Ezt a feladatot általában úgy oldjuk meg, hogy az eredeti digitális modulált jelet egy álvéletlen — legtöbbször bináris — kódsorozattal szorozzuk meg. Mivel az álvéletlen kódsorozat nagyobb sebességű, mint az eredeti adatjel, a sávszélesség jelentősen kibővül az eredeti modulált jel sávszélességéhez képest. A vevőben az eredeti modulált jelet úgy állítjuk vissza, hogy a vett jelet újra megszorozzuk az itt is ismert kódsorozattal, így a hasznos jel visszakerül az eredeti sávjába. A zavaró jeleket a vevőben csak egyszer szorozzuk meg az álvéletlen kódsorozattal, így azoknak a sávszélessége megnő és a teljesítménysűrűsége jelentősen lecsökken. Mindez azt eredményezi, hogy a hasznos — már keskenysávú — jel és a szélessávúvá tett zavar szűréssel hatékonyan szétválasztható. A direkt szekvenciális rendszerekben a spektrum kiterjesztésének mértéke az egy szimbólumidőre eső kódelemek számától függ.
- Frekvenciaugratás, ahol az adó frekvenciáját változtatjuk ugrásszerűen egy — az adóban és a vevőben egyaránt ismert — álvéletlen kódsorozat szerint. A frekvenciákat mindkét helyen egy előre meghatározott készletből választjuk ki, és az adó és vevő a frekvenciákat szinkronban változtatja. Mivel a vevő az adó jeleit követi, a zavaró jeleket pedig nem, azok csak kis eséllyel jutnak a vevő bemenetére, így a módszer most is alkalmas a zavar elnyomására. Lassú frekvenciaugratás esetén az ugratás ideje hosszabb a szimbólumidőnél, gyors frekvenciaugratás esetén viszont a vivő frekvenciája egy szimbólumidő alatt többször is változik.
- Időugratás, ahol az adó az időtengelynek csak bizonyos időréseit használja fel adásra, és ezeket az időréseket az adó és a vevő is egy mindkét helyen ismert álvéletlen kód alapján választja ki. A vevő itt is követi az adó működését, azaz csak azokban az időrésekben aktív, amelyeket az adó átvitelre kiválasztott. A zavaró jel csak akkor hatásos, ha éppen abba az időrésbe esik, amit az adó-vevő pár éppen használ, így itt is mód nyílik a zavar elnyomására.

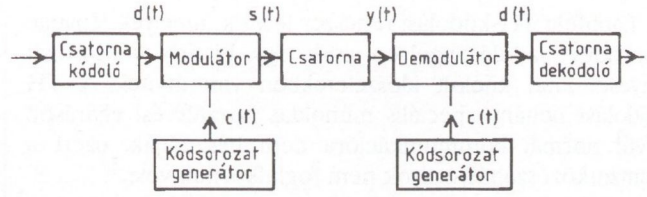
2.1. Pont-pont közötti összeköttetések

Egy adó és vevő pár közti összeköttetést részletezi a 1. ábra, amely egyúttal a pont-pont összeköttetés blokkvázlata is.

A modulátorból és a kódsorozat-generátorból álló egység felépítése határozza meg a rendszer típusát.

A három legelterjedtebb jelképzési eljárás:

- fázisugratásos (Direct-Sequence, DS);
- frekvenciaugratásos (Frequency Hopping, FH);
- időugratásos (Time-Hopping, TH) rendszer.



1. ábra. A szórt spektrumú pont-pont összeköttetés modellje

Az alábbiakban röviden áttekintjük ezen rendszerekkel kapcsolatos legalapvetőbb fogalmakat.

DS-jelképzés

A moduláció típusa digitális fázismoduláció, tipikusan bináris PSK (DS/BPSK). Az 1. ábrabeli kódsorozat generátor kimenetén egy $+1$, -1 értékű bináris, c_n, $n = 0, 1, \ldots$ sorozatnak megfelelő

$$c(t) = c_n, \quad nT_c \leq t < (Nn + 1)T_c$$

jel jelenik meg, ahol T_c az elemi jelidő (chipidő). A csatornakódoló kimenetén szintén egy $+1$, -1 értékű bináris, d_m, $m = 0, 1, \ldots$ sorozatnak megfelelő

$$d(t) = d_m, \quad mT_s \leq t < (m + 1)T_s$$

jel jelenik meg, ahol a T_s szimbólumidő a T_c elemi jelidő (chipidő) N-szerese, azaz $T_s = NT_c$. A modulátor kimenő jele

$$s(t) = \sqrt{2S}c(t) \cdot d(t) \cdot \cos(\omega_0 t + \phi), \tag{2.1}$$

ahol ω_0 a vivőfrekvencia, S a teljesítménykonstans, továbbá ϕ a véletlen vivőfázis.

FH-jelképzés

Többféle modulációs technika kerülhet alkalmazásra, amelynek a spektrumszórás szempontjából a lényege a vivőfrekvencia kódsorozatnak megfelelő ugratása. A legegyszerűbb esetet véve, tekintsünk egy frekvenciaugratásos bináris frekvenciamodulációs rendszert (FH/BFSK). A modulátor kimenetén az

$$\begin{aligned} s(t) = &\sqrt{2S}\cos(\omega_0 t + \omega_n t + d_n \cdot \Delta\omega \cdot t + \phi_n), \\ &nT_s \leq t < (n + 1)T_s, \end{aligned} \tag{2.2}$$

$n = 0, 1, \ldots$, jel jelenik meg, ahol $\{\omega_n\}$ a frekvenciaugrások sorozata, $\{\phi_n\}$ véletlen fázisok sorozata, továbbá $\Delta\omega$ a BFSK adatmoduláció paramétere. A frekvenciaugrások $\{\omega_n\}$ sorozatának elemei valamely $\{c_n\}$ kódsorozat elemeinek egy-egyértelmű leképezésével kaphatók, ahol Q frekvencia esetén $\omega_n \in \{\omega^{(0)}, \omega^{(1)}, \ldots, \omega^{(Q)}\}$.

A (2.2) szerinti FH/BFSK rendszerben a frekvenciaugratások sebessége megegyezik a szimbólumsebességgel. Általában az egy ugratási frekvencián a tartózkodási, ún. T_h ugratás-idő (hop-time) nem egyezi meg a T_s szimbólumidővel. Ennek megfelelően lassú frekvenciaugratásról beszélünk (SFH, Slow Frequency Hopping), ha $T_h \geq T_s$, illetve gyors frekvenciaugratásról (FFH, Fast Frequency Hopping), ha $T_h < T_s$. Tipikus SFH rendszer a szórt spektrumú csomagkommunikációs rendszer, amelynél egy-egy ugratás frekvencián egy-egy sok byte hosszúságú csomag kerül átvitelre.

TH-jelképzés

Többféle TH-kódolási rendszer létezik, amelyek lényege az, hogy az időtengelyen csak egy bináris kódsorozat egyesei által kijelölt időszeletekben van átvitel. A TH kódolást néhány speciális műholdas hozzáférési eljáráson kívül normál kommunikációra nem használják, ezért a nemzetközi szabályozások nem foglalkoznak vele.

Hibrid rendszerek

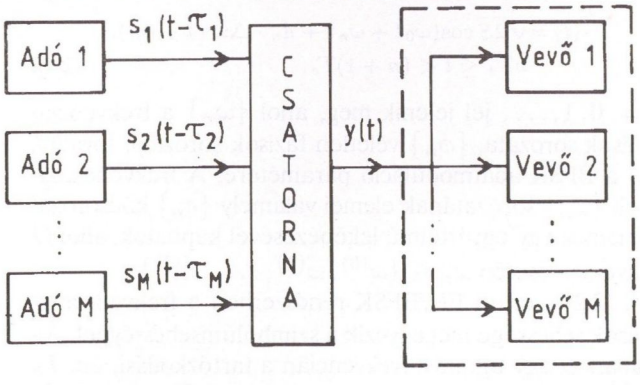
A fent felsorolt szórt spektrumú átviteli rendszerek kombinációit hibrid rendszereknek nevezzük. Ezek között a lassú és gyors frekvenciaugratás, illetve a fázisugratás és frekvenciaugratás kombinációját alkalmazza leginkább a gyakorlat, bár kommersz célú berendezésekben a hibrid eljárások felhasználása meglehetősen költségesnek tűnik.

2.2. A kódosztásos csatornamegosztás (CDMA)

Tekintsünk egy sokfelhasználós vezetéknélküli hírközlő hálózatot. A feladat T számú potenciális felhasználó hírközlési igényének kiszolgálása, amelyhez egy B sávszélességű csatorna áll rendelkezésre. Egyidejűleg a teljes populáció egy M méretű részhalmaza aktív, ahol általában M sokkal kisebb, mint T. A felhasználói információforrások az adási igény felmerülése után folyamatosan adni kívánnak vagy kis aktivitással szakaszosan működnek. A felhasználók időben *aszinkronok*. A hálózat tipikus topológiája szerint elosztott, pont-pont összeköttetéseket tartalmazó, illetve központtal rendelkező csillag hálózat.

A CDMA alapelve az, hogy minden felhasználóhoz egy saját kódot rendelünk, s amikor egy adott felhasználónak kívánunk információt továbbítani, akkor ezen információt a címzett kódjával kódolva továbbítjuk. A kódolás lehetővé teszi, hogy bár az M felhasználó adása időben átlapolódva, frekvenciatartománybeli megosztás nélkül van jelen a csatornában, az összegjelből vételi oldalon szeparálhatók az egyes felhasználók adásai valamely megbízhatósággal. Ezen megbízhatóság (dekódolási hibavalószínűség) megkívánt értéke szabja meg az M, azaz az egyszerre aktív felhasználók számának maximumát.

A 2. ábrán a csillag topológiájú hálózat vázlata látható.



2. ábra. A többszörös hozzáférésű csatorna

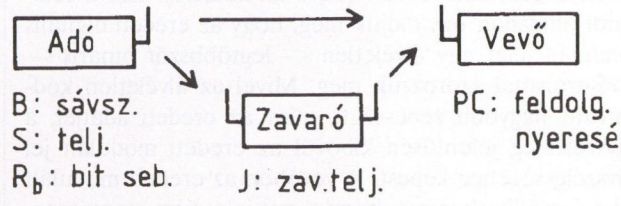
A csatorna kimenetén idealizált, torzítás- és fadingmentes esetben az

$$y(t) = \sum_{i=1}^{M} \gamma_i s_i(t - \tau_i) + n(t) \qquad (2.3)$$

összegjel jelenik meg, ahol τ_i, $0 \leq \tau_i < T_w$ a késleltetés-, γ_i, $0 < \gamma_i \leq 1$ a csillapításparaméter. $n(t)$ additív komponens zavarásmentes környezetben termikus zaj, míg zavart környezetben termikus zaj és zavarjel összeg.

3. AZ SST RENDSZEREK ÁTVITELI TULAJDONSÁGAI

Az SST rendszerek — mint már korábban említettük — a frekvenciasáv pazarló felhasználása következtében különleges, előnyös tulajdonságok hordozói. E tulajdonságok közül talán az interferencia elleni védettség (AJ, Anti Jamming) a legjelentősebb. Ennek hátterében az alábbi egyszerű fizikai jelenség áll (3. ábra).



3. ábra. A zavart csatorna

Legyen a szórt spektrumú jel sávszélessége B, teljesítménye pedig S, és legyen a sávszélesítési tényező értéke $ST = N$ (a sávszélesítési tényezőt igen sok közlemény leegyszerűsítve feldolgozási vagy eljárási nyereségkként (PG, Processing Gain) is említi, utalva arra, hogy a sávszélesség növelése az alábbi egyszerű megfontolások alapján éppen ezzel az értékkel növeli meg a rendszer jel-zavar viszonyát külső keskenysávú zavaró forrás esetén, a szokásos keskenysávú átvitel esetéhez viszonyítva).

Ha a fenti rendszer adatátviteli sebessége R_b, akkor — bináris átvitel esetén — éppen R_b (Hz) szélességű sávban volna mód a jel átvitelére. Ehelyett azonban a kommunikációt $B = N R_b$ sávszélesség felhasználásával bonyolítjuk le.

Tételezzük fel, hogy a hasznos jel mellett a vevő bementére J teljesítményű zavaró jel jut, amely rontja a hibamentes átvitel esélyeit. A kérdés az, hogy ez a zavaró jel szórt spektrumú átvitel esetén mennyire hatásos.

A vevő a 2. fejezetben leírt módon a bejövő jelet — az adóban végrehajtott sávszélesítési művelet inverzével — újra visszatranszformálja az R_b szélességű sávba, miközben a J értékű zavaró teljesítményt „elkeni" a B sávszélességben. Ha a vevő a döntés előtt az R_b sávszélességű hasznos jelet és a zavaró jelet szűréssel választja szét, akkor a döntés helyén az effektív jel-zaj viszony az

$$\frac{E_b}{N_j} = \frac{ST_b}{J/B} = \frac{S}{J}\frac{B}{R_b} = N \cdot \frac{S}{J} \qquad (3.1)$$

alakban adható meg, ami azt jelenti, hogy a döntés helyén (bináris átvitelt feltételezve) a jel-zavar viszony az eredeti S/J viszony N-szeresévé növekszik. A spektrumkiterjesztés egyenes következménye tehát az, hogy esetünkben a külső — véges teljesítményű — zavaró jel hatása a csatornában jelentősen — éppen az eljárási nyereség mértékével — csökken. Fontos kihangsúlyozni, hogy mindez csak a véges teljesítményű zavaró jel hatására vonatkozik, de nem érvényes a szélessávú fehér (tipikusan Gauss-) zajra, ugyanis a fehér zaj vevőbe jutó teljesítménye (diszperziómentes szélessávú csatornában) a sávszélesség növelésével éppen olyan mértékben nő, mint amilyen mértékű a feldolgozási, eljárási nyereség, így kimondhatjuk, hogy *diszper-*

ziómentes fehér-zajos csatornában az SST alkalmazása semmilyen előnnyel nem jár a keskenysávú átviteli rendszerekkel összehasonlítva.

A sávszélesség növelése a forrása az SST rendszerek másik előnyös tulajdonságának a többutas terjedés (fading) elleni védettségnek is (AM, Anti Multipath). Rádiós átviteli rendszerekben az adó és vevő közötti csillapítás a többutas terjedés következtében időről-időre véletlenszerűen változik egy-egy frekvenciasávban (szelektív fading). Keskenysávú modulációs technikák alkalmazása esetén mindez oda vezet, hogy a vett jel szintje időről-időre lecsökken, és így a csatornában lévő zaj szintjének relatív növekedése következtében a hibaarány a csatornában jelentősen megnő (ez akkor igaz, ha a szelektív fading hatása a jel teljes spektrumára kiterjed). Ez ellen a jelenség ellen a mérnöki gyakorlat úgy védekezik, hogy a rendszert túlméretezi, és egy ún. fadingtartalékot alkalmazva olyan nagy adóteljesítményt választ, hogy az még a legrosszabb esetben is elegendő biztonságot adjon a kis hibaarányú átvitelre. A teljesítmény felesleges (10 – 20 dB)-es növelése jelentősen terheli a frekvenciasávot és meglehetősen gazdaságtalan, de elkerülhetetlen megoldás. A szórt spektrumú technika alkalmazásakor a jelet tipikusan olyan széles sávban visszük át, hogy a szelektív fading most a jel összteljesítményének csak egy elenyésző részét tudja csillapítani, ami azt jelenti, hogy lecsökken vagy alig érzékelhető a fading által okozott statisztikus ingadozás a vevőben. Így nincs szükség a fadingtartalék alkalmazására, azaz 10 – 20 dB-lel kisebb teljesítménnyel is biztonságos átvitelt lehet biztosítani, ami jelentős gazdasági előnyökkel jár. Az előzőekben kiemelt állítások mellett tehát hangsúlyozni kell, hogy *az SST technikák alkalmazása diszperzív (fadinges) fehér-zajos csatornában jelentős előnyökkel jár, mivel nincs szükség a fadingtartalékra, azaz csökkenthető az átvitelhez szükséges adóteljesítmény.*

Az SST rendszerek alkalmasak arra, hogy azonos frekvenciasávban egyszerre több jelet vigyünk át oly módon, hogy a jeleket egymástól mindössze a spektrum kiterjesztésére használt kódokkal különböztessük meg (CDMA, Code Division Multiple Access). Erre azért van mód, mert a vevőben a saját kódot használó adó hasznos jele mellett a többi — idegen kódot használó — jel zavaró jelnek számít, amit a rendszer — a külső forrásokból származó jelhez hasonlóan — elnyom. Ezen elnyomás mértéke elsősorban az érintett kódok statisztikus kapcsolatától (hasonlóságától, korrelációjától) függ.

A spektrum kiterjesztése — a korábbiakban már említett módon — jelentősen csökkenti a jel teljesítményének spektrális sűrűségét, ami (i) módot ad arra, hogy a jelet nehezen lehessen detektálni, illetve zaj alatti teljesítménysűrűséggel is lehessen kommunikálni (AI, Anti Intercept), és (ii), amely lehetővé teszi, hogy más keskenysávú átviteli rendszereket a kis teljesítménysűrűségű jel csökkentett mértékben zavarjon.

Mindezek mellett a fázisugratásos, direkt szekvenciális rendszer módot nyújt a pontos időkésleltetés mérésére is (pl. GPS navigáció).

3.1. Az SST rendszerek működése zavar környezetben.

Az SST rendszerek védettsége

a) DS rendszerek vizsgálata keskenysávú zavarok esetén

A szórt spektrumú kommunikáció célja és egyben eredeti alkalmazása a szándékos, illetve nem szándékos külső zavarjelek elnyomási képességén alapult. Tekintsük példaként a leggyakoribb fázisugratásos (DS) rendszert, amelynél bináris BPSK modulációt alkalmaznak (DS/BPSK). A $d = -1$ információs bitet egy N hosszú, $+1$, -1 elemű c kódszóba, a $d = 1$ információs bitet $-c$ kódszóba kódoljuk (N-szeres spektrumszórás) a $[0, T_b]$ bitidőben. Értelemszerűen a megfelelő időfüggvényeket használva az $s(t)$ leadott jel:

$$s(t) = \sqrt{2S}d(t)c(t)\cos(\omega_0 t + \Phi_0), \quad S = \frac{E_b}{T_b}, \tag{3.2}$$

ahol S a jel teljesítménye, ω_0 a vivőfrekvencia, $d(t)$ az adatjel, $c(t)$ a bináris spektrumszóró kód, T_b a bitidő, E_b az egy bitre jutó jelenergia, Φ_0 pedig a vivő fázisa (továbbiakban $\Phi_0 = 0$).

Idealizált, torzítás- és fadingmentes csatorna kimenetén, a vevőnél megjelenő $y(t)$ jel az alábbi:

$$y(t) = s(t) + J(t) + n(t),$$

ahol $J(t)$ a zavaró jel, továbbá $n(t)$ a termikus zaj, és általános esetben

$$J(t) = \sqrt{2J}a(t)\cos(\omega_j t + \Phi(t)) \tag{3.3}$$

egy általános keskenysávú zavaró jel, J teljesítménnyel, $a(t)$ változó amplitúdóval, ω_j vivővel és $\Phi(t)$ változó fázissal, valamint a zaj felírható az

$$n(t) = \sqrt{2}n_c(t)\cos(\omega_0 t) + \sqrt{2}n_s(t)\sin(\omega_0 t) \tag{3.4}$$

ún. modulációs alakban, ahol $n_c(t)$ és $n_s(t)$ független alapsávi, $N_0/2$ teljesítménysűrűségű Gauss-zajpár.

A kódgenerátoroknak az adóban és a vevőben szinkronban kell járniuk. A vevő tulajdonkképpen szinkronizáló eszközök komplex egysége, ami kód- és vivőszinkronizálást jelent.

A szinkron elérése után korrelátoros vételt alkalmazunk, ami az

$$\int_0^{T_b} y(t)\left[\sqrt{2}\frac{c(t)}{\sqrt{T_b}}\cos(\omega_0 t)\right]dt \tag{3.5}$$

műveletet jelenti, s amelynek eredményeképpen egy

$$y' = d\sqrt{E_b} + \int_0^{T_b} \frac{c(t)n_c(t)}{\sqrt{T_b}}dt + \tag{3.6}$$

$$+ \int_0^{T_b} \frac{\sqrt{J}}{\sqrt{T_b}}c(t)a(t)\cos((\omega_0 - \omega_j)t + \Phi(t))dt$$

jel-zaj összeg keletkezik.

A (3.6) kifejezés jobb oldalának első tagja a hasznos jel, második tagja a fehér zajból származó összetevő, harmadik tagja pedig az általános modulált zavaró jelből keletkező alapsávi komponens. A vétel minőségét a vevőben a (3.6) kifejezés teljesítményviszonyai határozzák meg, ahol egyszerűen belátható, hogy az első tag teljesítménye (négyzetes várható értéke) éppen E_b, a második tagé

$$E_z = \frac{N_0}{2}\frac{1}{T_b}\int_0^{T_b} c^2(t)dt = \frac{N_0}{2}; \qquad (3.7)$$

a harmadik tagé pedig

- állandó amplitúdójú ($a(t) = a$), állandó fázisú ($\Phi(t) = \Phi$) és $\omega_j = \omega_0$ frekvenciájú zavaró vivő esetén

$$E_j = \frac{JT_b}{N}a^2\cos^2(\Phi), \qquad (3.8)$$

- állandó amplitúdójú ($a(t) = a$), véletlen fázisú ($\Phi(t)$ konstans, de véletlenül vesz fel értékeket a $0 - 2\pi$ tartományban) és $\omega j = \omega_0$ frekvenciájú zavaró vivő esetén

$$E_j = \frac{JT_b}{2N}a^2; \qquad (3.9)$$

- állandó amplitúdójú ($a(t) = a$), véletlen fázisú ($\Phi(t)$ konstans, de véletlenül vesz fel értékeket a $0 - 2\pi$ tartományban) és $\omega j \neq \omega_0$ frekvenciájú zavaró vivő esetén

$$E_j = \frac{JT_b}{2N}a^2\frac{\sin^2\left(\frac{\Delta\omega}{2}\frac{T_b}{N}\right)}{\left(\frac{\Delta\omega}{2}\frac{T_b}{N}\right)^2}; \ \Delta\omega = \omega_0 - \omega_j. \qquad (3.10)$$

Amiből a vevő effektív jel-zaj viszonya az

$$SNR = \frac{E_b}{E_z + E_j} = \frac{E_b}{\frac{N_0}{2} + E_j} \qquad (3.11)$$

kifejezés segítségével számolható. A (3.11) alapján világos, hogy zavaró jel nélkül a jel-zaj viszony

$$SNR' = 2\frac{E_b}{N_0}, \qquad (3.12)$$

ami megegyezik a szokásos fehér Gauss-zajos csatornák jel-zaj viszonyával. A zavaró jel teljesítménye pl. a (3.8) kifejezés szerint $a^2 = 1$ és $\Phi = 0$ esetén

$$E_j = \frac{JT_b}{N},$$

így háttérzaj nélkül (ha $N_0 = 0$) a jel-zaj viszony

$$SNR = \frac{E_b}{JT_b}N = \frac{S}{J}N, \qquad (3.13)$$

ami éppen a korábban egyszerűbb meggondolások alapján számolható jel-zaj viszony javulását mutatja. Megjegyezzük, hogy a fenti számítások akkor igazak, ha a kódsorozat elemei független bináris, valószínűségi változók.

Érdemes továbbá megjegyezni, hogy általános esetben, ha a $c(t)$ sorozat elemei adottak és a sorozat ismert, a (3.6) kifejezés harmadik tagjának a teljesítménye állandó amplitúdójú ($a(t) = a$), véletlen fázisú ($\Phi(t) = \Phi$, de Φ véletlenül vesz fel értékeket a $0 - 2\pi$ tartományban) és $\omega_0 \neq \omega_j$ frekvenciájú vivő esetében az

$$E_j = \frac{J}{2T_b}a^2|\mathcal{F}_{c(t)}(\Delta\omega)|^2 \qquad (3.14)$$

kifejezésből számolható, ahol

$$\mathcal{F}_{c(t)}(\omega) = \int_0^{T_b} c(t)\cdot\exp(-j\omega t)dt \qquad (3.15)$$

a spektrumszóró kódsorozat Fourier-transzformáltja. Mindez arra utal, hogy keskenysávú zavarokra a rendszer azokon a frekvenciákon érzékenyebb, ahol a spektrumszóró kódsorozat spektruma (Fourier-transzformáltja) nagyobb abszolút értékű. Az ún. maximális hosszúságú kódsorozatoknál a spektrum nem rendelkezik lokális maximumokkal, és az egyéb kódoknál (Gold, Kasami stb.) a csúcsok 1–3 dB-lel nagyobbak lehetnek az átlagértéknél, ami lényegében ekkora romlást jelent a védettségben ezen a speciális frekvencián (szelektíven látszólag csökken az eljárásból származó effektív nyereség). Lényeges megemlíteni, hogy modulált általános vivő esetén, ha $a(t)$ és $\Phi(t)$ nem konstans (és a moduláció statisztikailag független a spektrumszórásra használt kódsorozattól), a rendszer effektív nyeresége a (3.1) értékkel igen jól közelíthető.

b) DS rendszerek vizsgálata CDMA típusú zavarok esetén

Egy SST rendszer egy másik szélessávú rendszerrel szemben védett, ha a másik rendszerben alkalmazott spektrumszóró kódokkal a kódkeresztkorreláció nem kedvezőtlenebb, mint két véletlenszerűen választott kódsorozat között. Ebben az esetben egy S_1 adási teljesítményű CDMA adás zavaró hatása ekvivalensen legfeljebb egy S_1/B teljesítmény-spektrálsűrűségű additív zajként jelenik meg. Nagyon fontos kiemelnünk, hogy mindez csak megfelelő kódkonstelláció esetén igaz.

CDMA rendszerek tervezése esetén igen kritikus azon kódok tervezése és kiválasztása, amelyek a különböző adásokat megkülönböztetik egymástól. Két különböző kódsorozatot használó adó jelének találkozásakor a fellépő fizikai jelenségek most is jól leírhatók a (3.6) kifejezés segítségével, azzal a különbséggel, hogy a vevő által megfigyelt T_b időtartamban most az idegen jel két szomszédos bitjének a hatása is érvényesül, vagyis a detektálás helyére a (3.6) kifejezés harmadik tagja helyett az

$$\int_0^{\tau}\frac{\sqrt{S_1}}{\sqrt{T_b}}d'c'(t+T-\tau)c(t)\cos(\Phi')dt+$$
$$+\int_{\tau}^{T_b}\frac{\sqrt{S_1}}{\sqrt{T_b}}d''c'(t-\tau)c(t)\cos(\Phi')dt \qquad (3.16)$$

jel jut, ahol d' és d'' az idegen forrás két egymást követő bitje, $c'(t)$ az idegen adó spektrumszóró jele, τ az átlapolódás paramétere, Φ' pedig egy időkülönbségtől is függő fázis.

Az idegen jel által hordozott teljesítmény (energia) értékét a (3.16) kifejezésből számíthatjuk az

$$E_1 = \frac{S_1}{T_b}\cos^2(\Phi')\mathbb{E}\left\{\left[\int_0^{\tau}d'c'(t+T-\tau)c(t)dt+\right.\right.$$
$$\left.\left.+\int_{\tau}^{T_b}d''c'(t-\tau)c(t)dt\right]^2\right\} \qquad (3.17)$$

összefüggés segítségével. A zárójelben lévő kifejezés lényegében két kódsorozat ($c(t)$ és $c'(t)$) információs bitekkel súlyozott keresztkorrelációja. Amennyiben a két kódsorozat egyenként is független $+1$, -1 értékkészletű véletlen elemekből áll, az idegen jel által szállított energia átlagos értékére az

$$E_1 = \frac{S_1}{T_b}\cos^2(\Phi')\frac{T_b^2}{N} = \frac{S_1 T_b}{N}\cos^2(\Phi') \qquad (3.18)$$

összefüggést kapjuk. Ekkor a hasznos jellel szemben az idegen jel hatása éppen N-szeresen csökken, azaz az eljárási nyereség megegyezik a keskenysávú esetben kapott értékkel. Hangsúlyozni kell azonban, hogy CDMA esetén több determinisztikus kódot feltételezve ez az ideális elnyomás tipikusan nem érhető el. *A rendszeren belüli zavarokra a szórt spektrumú átvitel tipikusan érzékenyebb, mint a rendszeren kívüli összetevőkre.*

c) FH rendszerek vizsgálata keskenysávú zavarok esetén

- *Lassú frekvenciaugratásos rendszerek keskenysávú zavarokkal terhelt csatornában*

Tételezzük fel, hogy a kérdéses lassú frekvenciaugratásos rendszerben egy frekvenciasávban több szimbólumot (bitet) viszünk át, jelöljük ezek számát K-val. Tételezzük fel, hogy a hasznos jel teljesítménye a vevő bemenetén S, és a frekvenciasávok száma Q. Legyen a csatornában egy olyan zavaró jel, amely J teljesítményű és egy időben csak egyetlen frekvenciaugratásos részsávot képes lefedni.

Ekkor a zavarral terhelt csatornában az aktuális jel-zaj viszonyt az N_0 teljesítménysűrűségű fehér (tipikusan Gauss-) zaj figyelembevételével az

$$SNR_J = \frac{ST_b}{\frac{JT_b}{2} + \frac{N_0}{2}} \qquad (3.19)$$

arány határozza meg, a zavar által nem érintett csatornában viszont a jel-zaj viszony

$$SNR_0 = \frac{ST_b}{\frac{N_0}{2}} \qquad (3.20)$$

értékű.

A rendszer eredő hibaarányát ezek után a következő összefüggés alapján számolhatjuk:

$$P_e = \frac{1}{Q}P_b(SNR_J) + (1 - \frac{1}{Q})P_b(SNR_0), \qquad (3.21)$$

ahol az $1/Q$ annak az esélye, hogy az FH rendszer jele éppen ütközik a zavaró jellel, a $P_b(\cdot)$ függvény pedig az FH rendszerben alkalmazott modulációtól (tipikusan BFSK vagy MFSK) és a vételi algoritmustól (tipikusan nem koherens vevő) függő hibaarány-függvény. Fontos megjegyezni, hogy a hibák nagy zavaró szint esetén tipikusan csomósan jelentkeznek (egyszerre K egymást követő szimbólum sérül meg). Ez ellen általában két algoritmussal védekeznek: (i) zagyválást alkalmaznak a csatornában, így a hibacsomók helyett elszigetelten egyedi hibák keletkeznek, és (ii) hibajavító kódolást is használnak, amely a véletlen egyedi hibák ellen hatékony védelmet nyújthat. Természetesen a csatornában mérhető hiba (P_e) értékét ez a tény nem befolyásolja.

A keskenysávú zavarok egy jellegzetes változata az ún. részleges (parciális) sávú zavar. Ilyenkor az történik, hogy a zavaró jel J teljesítménye nem egy, hanem q különböző hopping sávot érint ugyanabban az időben. Az eredő hibaarányt most úgy lehet számolni, hogy figyelembe veszünk két tényt: (i) a J eredő teljesítmény q-ad része jut egy-egy frekvenciasávba, (ii) a frekvenciaugratásos jel most q/Q eséllyel találkozik a zavaró jellel. Mindebből az következik, hogy a jel-zaj viszony (N_0 teljesítménysűrűségű fehér háttérzaj esetén) az érintett csatornában

$$SNR'_J = \frac{ST_b}{\frac{JT_b}{2q} + \frac{N_0}{2}} \qquad (3.22)$$

értékű lesz, és a hibaarány a

$$P'_e = \frac{q}{Q}P_b(SNR'_J) + (1 - \frac{q}{Q})P_b(SNR_0) \qquad (3.23)$$

kifejezésből számolható. Egyszerűen igazolni lehet, hogy az esetek többségében valamilyen $q \neq 1$ értékű parciális zavarás okozza a legnagyobb hibaarányt, azaz az átvitelre általában ez a legveszélyesebb.

Megjegyzendő, hogy nem koherens bináris FSK alapmoduláció esetén (ez a leggyakoribb moduláció) a (3.22)-ben és (3.23)-ban szereplő hibafüggvény

$$P_b(SNR) = \frac{1}{2}\exp(-\frac{1}{2}(SNR)) \qquad (3.24)$$

alakú.

- *Gyors frekvenciaugratásos rendszer zavarokkal terhelt csatornában*

Gyors frekvenciaugratásos rendszerben egy szimbólum átviteléhez több frekvenciasávot használunk fel, és tipikus, hogy az egyes részsávokban átvitt jeleket (szinuszos vivőket) nem koherensen összegezzük a döntés előtt. Jelöljük az egy szimbólum alatt végrehajtott frekvenciaugratások számát L-lel, és tételezzük fel, hogy egy szimbólum átviteléhez mindig különböző frekvenciákat használunk a Q lehetségesből. Ekkor keskenysávú (egy részsávot érintő) zavaró jel esetén a jel-zaj viszony (N_0 teljesítménysűrűségű fehér zajt is feltételezve) biztosan egy ütközés és $Q = L$ mellett kis háttérzaj esetén az

$$SNR_J \cong \frac{ST_b}{\sqrt{2}\left[\left(\frac{JT_b}{Q}\right)^2 + \frac{JT_b}{Q}\frac{ST_b}{Q}\right]^{\frac{1}{2}}} \qquad (3.25)$$

alakban adható meg. Ebből jól látható, hogy az $L = Q$ növelésével a jel-zaj viszony javul, és hogy ilyenkor a zavarelnyomás lényegében Q-val arányos.

Részsávú (parciális sávú) zavarás esetén a zavaró jel teljes teljesítményét q számú frekvenciasávban teríti el. Ilyenkor nagyobb esély van az ütközésre, de a teljesítmény egy-egy sávban arányosan csökken. Ekkor a jel-zaj viszony kis háttérzaj esetén az

$$SNR_J \cong \frac{ST_b}{\sqrt{2}\left[\left(\frac{JT_b}{qQ}\right)^2 q + \frac{JT_b}{qQ}\frac{ST_b}{Q}q\right]^{\frac{1}{2}}} \qquad (3.26)$$

alakban adható meg. A zavarelnyomás ekkor tipikusan $Q \cdot \sqrt{q}$-val arányos, azaz a parciális sáv növelése az elnyomást növeli.

Ez utóbbi vizsgálat választ ad arra az esetre is, ha a zavar a teljes sávra kiterjed, ekkor ugyanis a $q = Q$, vagyis a zavarelnyomás mértékét $Q^{3/2}$ közelíti.

3.2. Az SST rendszerek működése fadinges csatornában

Az SST rendszerek számos alkalmazása során az átviteli csatorna jellemzői időben gyorsan változnak. Ennek tipikus példái a cellás mobil rendszerek és az épületen belüli kommunikációs alkalmazások. Az SST rendszerek alaptulajdonságaikból következően igen alkalmasak fadinges csatornán keresztüli robusztus digitális kommunikációs összeköttetések megvalósítására. Az alábbiakban először beve-

zetésként az épületen belüli kommunikációval kapcsolatosan utalunk néhány alapvető fogalomra és tulajdonságra, majd analitikus, kvantitatív leírásmód egyszerűbb modelljeiben világítjuk meg az SST anti-multipath alkalmazások lényegét különböző reális csatornamodellek mellett.

a) Többutas jelterjedésből származó interferencia elleni védelem alapelvei: az épületen belüli vezetéknélküli adatkommunikáció példája

Épületen belüli URH és mikrohullámú rádiós kommunikáció speciális feladat a kommunikációs csatorna erős terjedési veszteségei (elnyelődés), valamint a többutas hullámterjedés okozta diszperziós és fadingproblémák miatt. Ezen rádiócsatorna típusra általánosan használható modell nincsen, mivel a terjedési viszonyok igen erősen függnek a kérdéses épület belső struktúrájától, az épület szerkezeti anyagaitól, a helyiségekben található berendezésektől, a terjedési útban mozgó személyekből stb.

A terjedési csillapítás energiaelnyelődésekből származik. Egy falon áthaladó rádióhullám csillapítása a frekvencia növekedésével növekszik. A terjedési csillapítás erősen függ tehát az adó és vevője távolságától és a köztük levő szakasz topológiájától.

Az időben változó erősségű jelelhalkulások (fading) oka a késleltetésparaméterek lassú változása következtében előálló gyors fázisváltozások a komponens terjedési utakon. Ebből a szempontból nincs jelentősége a késleltetésparaméterek abszolút értékének, csak kicsi változásainak. Az épületen belüli kommunikációs csatornán tipikusan lassú Rice-fading, esetenként lassú Raileigh-fading áll elő.

A diszperzió (jelalaktorzulás) jelenségénél viszont a késleltetésparaméterek nagysága a döntő. Ha késleltetések eltérése összemérhető a szimbólum- (bit-) idővel (esetleg meg is haladja azt), akkor a digitális átvitelben szimbólumközti áthallást okoz.

A csatorna diszperziós tulajdonságainak mérésére alkalmas szórt spektrumú DS mérőjel közel ideális autokorrelációjú m-sorozatot alkalmaz. A vételi oldalon kvadratúra demodulátoros (azaz nemkoherens) vevő áll rendelkezésre, amelynek kimenetén a leadott és a csatornán át többutasan érkező jelek korrelációjának burkolója jelenik meg. Ezen kimeneti jelben autokorrelációs csúcsok csomagja jelenik meg periodikusan, amely csomagban a csúcsok amplitúdója, illetve késleltetése a megfelelő terjedési út csillapításának, illetve késleltetésének felel meg. Tulajdonképpen egy ilyen mérővevő lehet a lelke egy hírközlés célú vevőnek is, amely kiegészül a szinkronizáló egységgel, biztosítva a maximális korrelációs csúcs befogását. A különböző terjedési utak így felbonthatók, s a jelenergiák kombinálhatók. Összefoglalóan azt mondhatjuk, hogy a DS/SS átvitel alkalmazásával implicit diverzitit valósítunk meg. A szórt spektrumú csatornák tehát kevésbé érzékenyek a reflexiókból eredő többutas terjedési problémákra.

A továbbiakban ezen implicit diverziti egyszerűsített kvantitatív leírásmódját mutatjuk be a DS/BPSK átviteltípus példáján.

b) DS-BPSK átvitel fadinges csatornán

- *Lassú, nemszelektív fadinges csatorna esete: a keskenysávú átvitel*

A csatornába lépő jel

$$x(t,\Phi) = c(t)d(t)\sqrt{2S}\cos(\omega_0 t + \Phi), \tag{3.27}$$

ahol $d(t)$, illetve $c(t)$ a bipoláris (± 1 értékű) adat-, illetve kódsorozat, T_b bitidővel, illetve T_c chipidővel. Ekkor $B \cong \cong 1/T_c$. Legyen a vett jel amplitúdója A. Ekkor a vett bitenergia:

$$E_b = A^2 T_b/2. \tag{3.28}$$

A vevő bemenetén a zaj teljesítménysűrűség-spektrumát N_0-lal jelölve, ismeretes, hogy a koherens vétel bithibaaránya:

$$P_b(A) = Q((A^2T_b/N_0)^{1/2}) \leq \frac{1}{2}\exp(-A^2T_b/2N_0). \tag{3.29}$$

A feltételezett fadinges csatorna modellje egyszerűen egy Rayleigh-eloszlású véletlen c csillapításkonstans, amellyel $A = c\sqrt{2S}$. Alkalmazva a

$$p_A(a) = \frac{a}{\sigma^2}\exp(-a^2/(2\sigma^2)), \quad a \geq 0 \tag{3.30}$$

Rayleigh-eloszlást, az ismert

$$P_b \leq \frac{1}{2}\left\{\frac{1}{1+\overline{E}/N_0}\right\} \tag{3.31}$$

összefüggést kapjuk, ahol $\overline{E}$ a vételi átlagos bitenergia.

Tehát a lassú, nemszelektív Rayleigh-fadinges csatornán egyéb kódolási eljárás bevezetése nélkül az adási teljesítmény (S) növelésével a vételi bithibaarány csak fordított arányban csökken. Ez a tipikus eset a keskenysávú (nem spektrumszórás elvén működő) rendszerekben, ahol a teljes sáv egyszerre csillapodik. Ekkor csak külön redundáns kódolás alkalmazása segít, azaz ekkor is a sávszélesítés irányába kell mennünk konstans forrássebességet tekintve. Tulajdonképpen ennek a redundáns kódolásnak egy szélsőséges eseteként fogható fel a spektrumszórásos rendszerben alkalmazott kódolás, ahol igen nagy redundanciát viszünk a rendszerbe.

- *Lassú, szelektív fadinges csatorna esete: a szélessávú átvitel*

A spektrumszórásos rendszerek szelektív fadinges csatornával szembeni robusztus viselkedésének szemléletes oka az, hogy egyszerre a teljes jel-teljesítményspektrumnak csak egy-egy, időben változó kisebb szelete szenved időben változó csillapodást, s így a teljes bitenergiának csak kisebb része vész el. Ezt a teljesítményszemléletet pontosabbá tesszük egy rövid analízissel.

A csatornába lépő jel

$$x(t,\Phi) = c(t)d(t)\sqrt{2S}\cos(\omega_0 t + \Phi),$$

a csatorna kimeneti jele

$$y(t) = \sum_{k=1}^{J} c_k x(t-\tau_k;\Phi_k) + n(t), \tag{3.32}$$

ahol

$$|\tau_i - \tau_j| \geq T_c, \tag{3.33}$$

tetszőleges i, j pár esetére. Ekkor (3.33) következtében az egyes terjedési utak felbonthatók a vevőben, az alkalmazott $c(t)$ kódok speciális autokorrelációs függvénye alapján. Az adott fading-modellben az egyes terjedési utak csillapítás-paramétereit statisztikailag független valószínűségi változókkal modellezve, az egyes útfelbontások a vevő kimenetén

$$r_k \cong d_0 c_k \sqrt{E_b} + n_k, \tag{3.34}$$

ahol n_k független, gaussi valószínűségi változók $N_0/2$ szórással, $k = 1, 2, \ldots, J$. Az optimális vétel az r_k változók c_k súlyú lineáris kombinációjával kapható:

$$r = \sum_{k=1}^{J} c_k r_k. \tag{3.35}$$

A csillapításparamétereket Rayleigh-eloszlásúnak véve, a vételi bithibaarány

$$P_b \leq \frac{1}{2} \prod_{k=1}^{J} \left\{ \frac{1}{1 + \overline{E}_k / N_0} \right\}, \tag{3.36}$$

ahol $\overline{E}_k$ a k-adik terjedési úton vett átlagos bitenergia, amely összefüggés (3.31) párja többutas esetre. A (3.31) összefüggést a $J = 1$ jelút esetének tekintjük, és azt az egyszerű esetet vesszük, hogy jelutanként azonos a vett jelenergia, azaz $\overline{E}_k / N_0 = \overline{E} / N_0$ konstans, akkor (3.36) alapján

$$P_b \leq \frac{1}{2} \left\{ \frac{1}{1 + \overline{E} / N_0} \right\}^{J}, \tag{3.37}$$

összefüggést kapjuk, ami azt jelzi, hogy a felbontott, statisztikailag független utak J számával exponenciálisan csökken a hibavalószínűség, s ezzel az S leadott jelteljesítmény növelésével, ha nem is (3.31)-beli reciprok összefüggéshez képest, lényegesen gyorsabb a hibavalószínűség csökkenés.

Ezzel megkaptuk az elvi és gyakorlatban is követhető magyarázatát a spektrumszórásos szélessávú átvitel fadinghatásokkal szembeni robusztusságának. Megemlítjük továbbá, hogy a csatornához megfelelően tervezett hibajavító kódokkal további lényeges hibaarány-javulás érhető el. Az igazán hatékony SST rendszerek ennek megfelelően komplex kódolási eljárásokkal dolgoznak.

c) FH átvitel fadinges csatornán

A frekvenciaugratásos átvitel szelektív fadinges csatornával szembeni robusztussága még szemléletesebben látható, mint a DS típusú átviteleké. Nevezetesen a legkisebb frekvenciaugrás távolságát úgy célszerű választani, hogy az legalább akkora legyen, mint a Δf_c koherencia sávszélesség. Ebben az esetben az egyes ugratási frekvenciacsatornákon a jel jó közelítéssel statisztikailag független fadinghatásnak lesz kitéve, tehát a teljes sávon nem tud egyidejűleg fellépni elhalkulás. A csatornamodell ismeretében így méretezhető az FH rendszer. Külön hibajavító kódolás alkalmazásával a bevitt redundancia árán, további jelentős dekódolási bit-hibaarány javulás érhető el.

4. ÖSSZEFOGLALÁS

A cikk a biztonságos hírközlés egy hatékony fizikai módszerével, a spektrum kiterjesztésének (szórásának) eljárásával foglalkozik, áttekintést adva a legfontosabb alapfogalmakról és a technológiákkal kapcsolatos főbb paraméterekről. Az anyag a védettség fő ismérveit emeli csak ki, és legfeljebb utalásokat tartalmaz a ma igen aktuális CDMA alkalmazásokkal kapcsolatban.

A szerző köszönetét fejezi ki Vajda Istvánnak és Mihály Zsigmondnak az anyag elkészítéséhez nyújtott hatékony segítségükért.

IRODALOM

[1] Holmes, J. K.: Coherent Spread Spectrum Systems, Wiley-Interscience, New York, 1982.

[2] Pickholtz, J. F., Schilling, D. L. and Milstein, L. B.: „Theory of Spread Spectrum Communications – A Tutorial", *IEEE Trans. Commun.*, Vol. COM-30, pp. 825-834, May 1982.

[3] Simon, M. K., Omura, J. K., Scholtz, R. A. and Levitt, B. K.: Spread Spectrum Communications, Vol. I., II., III., Computer Science Press, Rockville, 1985.

[4] Papp László: A szórt spektrumú kommunikáció néhány elméleti és gyakorlati problémája, Doktori értekezés, MTA, 1990.

[5] Mohamed, K. A. and Pap, L.: „Analysis of Frequency-Hopped Packet Radio Networks with Random Signal Level", *IEEE Selected Areas in Communications*, Vol. 12, pp. 723-732, May 1994.

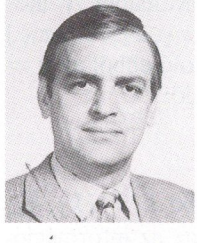
[6] Pap, L.: „General Jamming Model of Spread Spectrum Systems", *IEEE International Conference on Communications*, ICC'93, May 23rd-26th, Conference Record, Vol. 1/3, pp. 473-477, 1993.

PHYSICAL PROTECTION OF COMMUNICATION CHANNELS, SPREAD SPECTRUM TECHNOLOGY

L. PAP

DEPARTMENT OF TELECOMMUNICATIONS, TECHNICAL UNIVERSITY OF BUDAPEST
H-1111 BUDAPEST, SZTOCZEK U. 2.

The paper is concerned with the basic principles, the application fields, the types and the most important technical parameters of the spread-spectrum radio communication systems. The contribution concentrates on the following two main features of this reliable communication technology: the resistivity of the system to the jamming, the immunity of the system against the multipath propagation.



Pap László 1967-ben végezte el a Budapesti Műszaki Egyetem Villamosmérnöki Karának Híradástechnikai Szakát. 1980-ban kandidátusi, 1992-ben akadémiai doktori fokozatot szerzett. 1992 óta egyetemi tanár, a Híradástechnikai Tanszék vezetője, 1994 óta a Villamosmérnöki és Informatikai Kar dékánja. Fő érdeklődési területe a hírközléselmélet, a kódolás és moduláció, a szinkronizáció, a mobil kommunikáció és a modern távközlési rendszerek elmélete.

SZIMMETRIKUS KULCSÚ BLOKK REJTJELZŐK TERVEZÉSI KRITÉRIUMAI

VAJDA ISTVÁN és BUTTYÁN LEVENTE

BUDAPESTI MŰSZAKI EGYETEM
HÍRADÁSTECHNIKA TANSZÉK
1111 BUDAPEST, SZTOCZEK U. 2.

A kriptográfiailag erős bináris helyettesítő leképezések (S-boxok) alapelemek a helyettesítés-permutáció típusú rejtjelzőkben. Vizsgáljuk az erős Boole-függvényekre vonatkozó tervezési kritériumok közötti összefüggéseket. Megmutatjuk a véletlen tervezés néhány kapcsolódó vonatkozását. Egyszerű korlátokat adunk a rétegek szükséges számára vonatkozóan. Végül utalunk a statisztikai tesztek, mint első tervezési hibaszűrők alkalmazására bevezető szinten.

1. BEVEZETÉS

Az információátvitel biztonsági kérdései a jövő nyilvános távközlési hálózataiban lényeges szerepet fognak játszani. Az átvitt információ tartalmának algoritmikus rejtése, az átvitel közbeni illetéktelen módosíthatatlanságának biztosítása, a kommunikáló partnerek hitelességének ellenőrizhetősége, továbbá a hozzáférés védelem alapvető feladatok. A számítástechnikai ismeretek széleskörű terjedése, a számítástechnikai és átviteltechnikai eszközök elérhető ára, a nyilvános távközlő csatornák adatbiztonsági sérülékenysége veszélyeket is hordanak magukban. A korszerű információfeldolgozási és továbbítási módszerek, mint például ez egyre nagyobb teljesítményű személyi számítógépek alkalmazása, azok hálózatba kötése, távoli adatbázisok elérhetősége, adatátvitel nyilvános kommunikációs csatornákon, mind növelik az érzékeny információkkal kapcsolatos hibák és visszaélések veszélyét.

Érzékeny információknak azokat tekintjük, amelyek illetéktelen megismerése, elvesztése, illetéktelen módosítása vagy megsemmisítése számottevő veszteséget okoz az információ jogos tulajdonosának.

Egy jól funkcionáló adatvédelmi rendszer három pilléren nyugszik, amelyek a fizikai hozzáférés védelem, a megfelelő felügyeleti rendszabályok alkalmazása, valamint az algoritmikus adatvédelem.

Az algoritmikus adatvédelem módszerei lehetőséget nyújtanak arra, hogy az érzékeny információt megvédjük többek között a illetéktelen megismerése, módosítása, régebbi, felvett üzenetek csalási célú visszajátszása, mások megszemélyesítése, üzenet elküldésének, illetve vételének letagadása ellen. Az algoritmikus adatvédelem a feladatokat rejtjelezés, hitelesítés, hozzáférés védelem módszerekkel oldja meg.

A kriptográfiai alapú védelmi rendszerek magja egy kódoló-dekódoló transzformáció. Blokk kódolás esetén a digitális információforrás kimeneti adatfolyamából N méretű blokkokat készítünk. Egy ilyen $x = (x_1, x_2, \ldots, x_N)$ blokkot, nyílt üzenetnek nevezzük. A kódoló ebből az $y = (y_1, y_2, \ldots, y_N)$ rejtett üzenetet állítja elő:

$$y = E_k(x),$$

ahol E_k a kódoló transzformáció, továbbá $k = (k_1, k_2, \ldots, k_K)$ a kódolás (rejtjelezés) kulcsa, az az információ, amely egyértelműen meghatározza az aktuális transzformációt. A D_k dekódoló (fejtő) transzformáció az E_k kódoló transzformáció inverze, amelynek felhasználásával

$$x = D_k(y)$$

módon kapjuk vissza a nyílt szöveget.

Konvencionális, más néven szimmetrikus kulcsú rejtjelzésről beszélünk, amikor ugyanazt a titkos kulcsot alkalmazzuk a rejtéshez és a fejtéshez. Az ú.n. nyilvános kulcsú, illetve aszimmetrikus rendszerben egy nyilvános és egy titkos kulcsot alkalmazunk, az előbbit a rejtéshez, az utóbbit a fejtéshez.

A kriptográfiai alapú adatvédelem számtalan izgalmas problémaköréből ezen cikk egy szűk szelet, elsősorban elméleti, tervezési indíttatású megközelítésével kapcsolatos. Nevezetesen jelen cikkünk témája szimmetrikus kulcsú blokk kódolók tervezésének alapelveihez, kritériumrendszeréhez kapcsolódik.

Az egyik legismertebb és leggyakrabban használt szimmetrikus kulcsú blokk kódoló a DES (Data Encryption Standard). Ez helyettesítő transzformációt (S-box) és bitpermutációt (P-box) tartalmazó kulcsvezérelt rétegek sokszori egymás utáni alkalmazásával működő kódoló-dekódoló transzformáció. Megjelenésétől kezdve folyamatosan támadják, és próbálják megfejteni, aminek elsődleges oka viszonylag „kicsi" kulcsmérete (56 bit). Ezzel párhuzamosan a DES megerősítésére vonatkozó kísérletek is megfigyelhetők. Mivel a nem-linearitást egyedül a helyettesítő transzformációk jelentik, ezért a megerősítésre tett próbálkozások nagy része az S-box-ok méretének növelésével, illetve az S-box-ok kriptográfiai tulajdonságainak javításával igyekszik eredményt elérni. Ezek a gondolatok vezetnek el az S-box tervezés kritériumainak és módszereinek vizsgálatához [10], [13], [14], [15], [16], [17], [18], [22].

Az évek során számos tervezési kritérium jelent meg a bináris helyettesítő transzformációkkal (S-box-ok, Boole-függvények) kapcsolatosan. A legismertebbek definícióit az Appendix A tartalmazza. Sajnos a különböző kritériumok között vannak olyanok, melyek nem kompatibilisek egymással, azaz egyik teljesülése kizárja a másik teljesülését vagy korlátozza abban az optimum elérhetőségét. Ennek az az oka, hogy a kritériumok halmaza nem valamilyen jól definiált, kompatibilis úton keletkezett és növekszik. A folyamat sokkal inkább ad hoc jellegű: egy új kritéri-

um általában egy új támadás megjelenésével és a támadás elleni védekezés feltételeinek meghatározásával születik. Egyelőre nincs általános szabály, mely megmondaná, hogyan kell optimálisan kiválasztani egy kompatibilis kritériumokból álló részhalmazt, amelynek teljesítése garantáltan kriptográfiailag erős transzformációra vezet. A problémát az is nehezíti, hogy a különböző alkalmazások és környezetek eltérő kritérium-rendszert követelnek meg. Ezért a kritériumok közötti kapcsolatok vizsgálata fontos területe a kutatásnak, s ezzel a kérdéssel foglalkozunk cikkünk 2. pontjában.

Kriptográfiailag erős S-box-ok tervezésére két fő módszer létezik: konstrukció, illetve véletlen választás kritériumok szerinti szűréssel. A véletlen választás vonatkozhat közvetlenül S-box-okra, vagy erős Boole-függvényekre. Utóbbi esetben további feladat a kisorsolt Boole-függvényekből kiválasztani azokat, amelyek együttesen erős S-box-ot alkotnak. A véletlen választáson alapuló tervezés korlátait különböző kombinatorikus leszámlálási módszerekkel és számítógépes kísérletekkel becsülhetjük meg [4], [11]. Ezen megközelítésekkel a 3. pontban foglalkozunk röviden.

A véletlen választás nemcsak az S-box-ok, hanem a P-box-ok tervezésénél is használható módszer. Bár a bitpermutáció szerepe — a diffúzió biztosítása — fontos, tervezése mégsem kritikus kérdés (azaz nem egy „nehéz" feladat). A P-box-szal szemben támasztott lényeges követelmény, hogy biztosítsa az S-box-ok közötti kapcsolatot, azaz minden S-box minden S-box-ból elérhető legyen néhány iterációs lépésen belül. A véletlen választás effektív módszer a fenti tulajdonságot teljesíto P-box-ok keresésére. A 4. pontban mutatunk kapcsolódó eredményt. Ugyanitt adunk egyszerű alsó korlátot egy rejtjelző rétegeinek szükséges számára vonatkozóan.

Egy kész kódolási algoritmus kriptográfiai erejének megítélése igen nehéz feladat. Ehhez a témakörhöz kapcsolódóan statisztikai tesztek ilyen célú alkalmazásáról szólunk röviden az 5. pontban. Célunk elsősorban az elvek szemléltetése. Példát mutatunk a bemenet és a kimenet statisztikai függetlenségének, a bemenet és a kimenet, illetve a kulcs és a kimenet közötti lavinahatás teljesülésének az ellenőrzésére.

2. AZ S-BOX TERVEZÉS KRITÉRIUMAI

Mint a bevezetőben említettük a leggyakoribb konvencionális blokk kódolók kis méretű helyettesítő táblázatok (S-box-ok) együtteséből és bit-permutációból (P-box) felépülő kulcsvezérelt rétegek (round) egymás utáni sokszori alkalmazásával érik el a nyílt bemeneti blokk kriptográfiailag megfelelően erős „véletlenítését".

A helyettesítő transzformációk kriptográfiai erejével kapcsolatos ismertebb kritériumok a következők:

- Balansz tulajdonság.
- Algebrai fokszám.
- Teljesség.
- Nem-linearitás (az affin függvényektől vett minimális távolság).
- Terjedési kritériumok.
  - Lavinahatás kritérium.
  - Szigorú lavinahatás kritérium (Strict Avalanche Criteria – SAC).
  - r-ed rendű SAC.
- Differenciális uniformitás.
  - Perfekt tulajdonság.
  - Differenciális d-uniformitás.
- Lineáris dimenzió.
- Korreláció immunitás.
- Invariancia tulajdonságok.

A kapcsolódó definíciókat Appendix A. tartalmazza. A definíciók könnyebb megértését rövid magyarázatokkal próbáltuk segíteni.

2.1. táblázat

	Korreláció immunis (r-ed rendű)	Perfekt	SAC (r-ed rendű)	Teljes
Algebrai fokszám	$<n-r$	≥ 2	≥ 2 $(\forall r)$ $<n-r$ $(r \leq n-3)$	≥ 2
Nem-linearitás	{1}	$2^{n-1}-2^{n/2-1}$	{2} $\geq 2^{n-2}$	>0
Lineáris dimenzió	Nincs megkötés	0	≥ 1	Nincs megkötés
Walsh-transz-formált	$F(w)=0$ ha $1 \leq wt(w) \leq r$	$\lvert F(w)\rvert = 2^{n/2}$ minden w-re	*	{3}
Invariancia	{4}	Input Output	-Korlátozott Input Inv. -Output Inv.	-Korlátozott Input Inv. -Output Inv.
Balansz tul.				
Teljesség				
SAC (r-ed rendű)				
Perfektség				

(* lásd Appendix A, r-edrendű SAC tulajdonságnál)

A 2.1. táblázatban {szám}-mal jelöltük a következő eredményeinket:

2.1 Tétel ({1}): Egy r-ed rendben korreláció immunis $f : V_2^n \to V_2^1$ Boole-függvény $\delta(f)$ nem-linearitására a következő felső becslés adható:

$$\delta(f) \leq 2^{n-1}\left(1-\left(2^n-\sum_{i=1}^{r}\binom{n}{i}\right)^{-1/2}\right). \quad (2.1)$$

Bizonyítás: Megtalálható [21]-ben.

2.2 Tétel ({2}): Egy SAC tulajdonságot teljesítő $f : V_2^n \to V_2^1$ Boole-függvény $\delta(f)$ nem-linearitására a következő alsó becslés adható:

$$\delta(f) \geq 2^{n-2}. \quad (2.2)$$

Bizonyítás: Megtalálható [21]-ben.

2.3. Tétel ({3}): Nem teljes $f : V_2^n \to V_2^1$ függvény Walsh-transzformáltja a következő alakú:

$$F(w) = \begin{cases} 0, & \text{ha } w^{(2)} \neq 0; \\ 2^{|x^{(2)}|} \cdot F'(w^{(1)}), & \text{ha } w^{(2)} = 0; \end{cases} \quad (2.3)$$

ahol $f(x) = f(x^{(1)}, x^{(2)})$, $x^{(2)}$ azokat az input biteket tartalmazza, melyeknek nincs hatása a kimenetre, továbbá a $w = (w^{(1)}, w^{(2)})$ dekompozíció megfelel az $x = (x^{(1)}, x^{(2)})$ felbontásnak, $|x^{(2)}|$ jelöli $x^{(2)}$ hosszát bitekben, és $F'(w)$ jelöli az $f'(x^{(1)})$ függvény Walsh-transzformáltját.

Bizonyítás: A teljesség, illetve a Walsh-transzformált definíciójából közvetlenül belátható. ■

2.4. Tétel ({4}): A korreláció immunitás nem input invariáns.

Bizonyítás: Egy egyszerű példával bizonyítjuk a fenti állítást. Az $(x) = f(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3 + x_1$ Boole-függvény első rendben korreláció immunis. Ez a 2.2. táblázatból ellenőrizhető.

2.2. táblázat

x_3 w_3	x_2 w_2	x_1 w_1	$f(x)$	$F(w)$
0	0	0	0	4
0	0	1	1	0
0	1	0	0	0
0	1	1	0	4
1	0	0	0	0
1	0	1	0	4
1	1	0	1	−4
1	1	1	0	0

Ellenőrizhető, hogy f Hamming-távolsága a legközelebbi affin függvénytől 2, valamint SAC tulajdonságú.

Legyen a bemeneten alkalmazott invertálható, affin transzformáció mátrixa a következő:

$$A = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

Belátható, hogy az így nyert $f'(x) = f(A \cdot x)$ Boole-függvény Walsh-transzformáltja a $w = (1, 0, 0)$ helyen nem 0 ($F'(1, 0, 0) = 4$), és így nem lehet korreláció immunis. (Megjegyezzük, hogy f' SAC maradt.) ■

A 2.1. táblázat alsó részében halmazjelölésekkel ábrázolt összefüggéseket közvetlen számpéldákkal igazolhatjuk:

Példa:

1. Korreláció immunis és nem teljes függvény:
   Mivel egy nem teljes függvény kimenete nem korrelál azokkal a bemenetekkel, melyektől a kimenet nem függ, ezért ha a maradék bemenetre korlátozott függvény korreláció immunis, akkor az eredeti függvény is az.
2. Teljes és nem korreláció immunis függvény: $f(x) = x_1x_2$.
3. Korreláció immunis és nem SAC függvény: $f(x) = x_1 + x_2$.
4. SAC és nem korreláció immunis függvény: 2.4.tétel f' függvénye.
5. Korreláció immunis és balansz függvény: $f(x) = x_1 + x_2$.
6. Balansz és nem korreláció immunis függvény: $f(x) = x_1x_2 + x_3$.
7. Teljes és balansz függvény: $f(x) = x_1 + x_2$.
8. Teljes és nem balansz függvény: $f(x) = x_1x_2$.
9. Nem teljes és balansz függvény: $f(x) = x_1$.

Az utolsó három példában (7.,8.,9.) a „teljes" szót a „SAC" szóra cserélve további példákat kapunk.

3. VÉLETLEN VÁLASZTÁSON ALAPULÓ S-BOX TERVEZÉS

Kérdés, hogy az S-box-ok véletlen választása, majd bizonyos kritériumok szerinti szűrése elfogadható módja-e a tervezésnek. A kérdés itt lényegében az, hogy mennyi a valószínűsége annak, hogy egy véletlenül választott S-box kielégít egy bizonyos kritériumot vagy azok egy halmazát. Ha ez a valószínűség túl kicsi, akkor nincs remény arra, hogy véletlen választással erős S-box-okat találunk. Ezért egy kutatási irány ezen valószínűségek kiszámítása illetve becslése [4], [11].

Nem-lineáris permutációk

Egy $f : V_2^n \to V_2^n$ transzformáció definíció szerint akkor balansz, ha permutáció. Jól ismert, hogy a permutációk és az összes n bitet n bitbe képző transzformációk aránya

$$\frac{(2^n)!}{2^{2^n}} \quad (3.1)$$

exponenciális sebességgel csökken, ahogy n nő. Ez azonban nem jelent nagy problémát, mert permutációt könnyen lehet sorsolni közvetlen módon. Ezért balansz $V_2^n \to V_2^n$ leképzés véletlen választása kivitelezhető feladat.

Annak valószínűsége, hogy egy véletlenül választott permutáció lineáris:

$$\frac{2^n(2^{n-1})(2^{n-2})(2^{n-4})\ldots(2^n - 2^{n-1})}{n!(2^n)!}, \quad (3.2)$$

amely exponenciális sebességgel csökken, tehát azt könnyen el tudjuk kerülni, hogy affin permutációt válasszunk. Sajnos annak ellenére, hogy maga a permutáció nem affin, az még előfordulhat, hogy valamelyik komponens Boole-függvénye affin. Annak, valószínűsége, hogy egy véletlenül választott permutáció i. komponens Boole-függvénye affin

$$\frac{2(2^n - 1)[(2^{n-1})!]^2}{(2^n)!}. \quad (3.3)$$

(3.3)-at megszorozva n-nel felső becslést kapunk annak a valószínűségére, hogy létezik egy affin komponens. Ez a valószínűség is exponenciálisan csökken, ahogy n nő, $n = 8$ esetén például 10^{-100} nagyságrendű.

Ezek alapján megállapíthatjuk, hogy balansz, nem affin blokk helyettesítés választása nem nehéz feladat.

Teljesség

Teljes függvények számára vonatkozó számítások találhatók [11]-ben. Itt most egy felső becslést adunk meg an-

nak a valószínűségére, hogy egy véletlenül választott balansz függvény nem teljes.

3.1 Tétel: Annak a valószínűsége, hogy egy n bitet s bitbe képző balansz függvények halmazából véletlenül választott függvény nem teljes felülről becsülhető a következő kifejezéssel:

$$n \cdot s \cdot \frac{\binom{2^{n-1}}{2^{n-2}}[(2^{n-1})!]^2}{(2^n)!}. \qquad (3.4)$$

Bizonyítás: Megtalálható [21]-ben.

Például a (3.4) felső becslés $n = s = 6$ esetén $1.2E-9$, míg $n = s = 8$ esetén $1.4E - 37$ eredményt ad. A felső becslés exponenciális sebességgel csökken n-ben és lineárisan nő s-ben, azaz n értéke a meghatározó.

SAC

Nem ismert, hogy egy véletlenül választott permutáció milyen valószínűséggel teljesíti a 0-ad rendű SAC-et. $n - 4$-nél nagyobb rendű SAC kielégítésének valószínűségére azonban vannak ismert eredmények [2], [15].

Erős sejtés, hogy annak valószínűsége, miszerint egy véletlenül választott permutáció teljesíti a SAC-et exponenciálisan csökken az input méretével, ezért itt a véletlen választás nem járható út. Sajnos nagy input méretre az a módszer sem kivitelezhető, hogy egy permutációt n darab megfelelően megválasztott, SAC-et teljesítő komponens Boole-függvényből rakunk össze.

Ezzel szemben olyan invertálható S-box-ot, melynek minden input-output párja között majdnem teljesül a SAC könnyű találni. Ráadásul a jó választás valószínűsége nő, ahogy az input mérete nő. Számítógép segítségével generáltunk véletlen S-box-okat, hogy megbecsüljük a függőségi mátrix maximális és minimális elemének várható értékét és szórását. A függőségi mátrix (i, j) eleme ugyanis pont annak a valószínűsége, hogy a j-edik output bit megváltozik az i. input bit változásának hatására. Egy SAC-et teljesítő S-box függőségi mátrixának tehát minden eleme 0.5. Eredményeinket a 3.1. táblázatban foglaltuk össze.

3.1. táblázat

Méret	Véletlenül választott S-box-ok száma	E(MAX)	D^2(MAX)	E(MIN)	D^2(MIN)
4	10000	0,82	0,0113	0,23	0,0055
6	10000	0,69	0,002	0,32	0,0019
8	5000	0,6	0,0004	0,4	0,0004
10	500	0,56	0,0001	0,44	0,0001
12	100	0,53	2e-0,5	0,47	2e-05

A 3.1. táblázatból látható, hogy a maximum és a minimum átlaga egyre közelebb van a kívánt 0,5-höz, ahogy a méret növekszik. Az is látszik, hogy a szórás nagyon kicsi, és gyorsan csökken a mérettel, ami alátámasztja azt a megfigyelést, hogy olyan S-box, mely valóban teljesíti a SAC-et nehezen található.

A szórás kis értéke azonban azt is jelenti, hogy olyan S-box könnyen található, melynek függőségi mátrixában az elemek közel vannak az átlaghoz. Például 6 próbálkozás után találtuk azt az S-box-ot, melynek függőségi mátrixa a 3.2. táblázatban látható.

3.2. táblázat

0.5	0.51	0.49	0.49	0.5	0.49	0.51	0.51	0.49	0.49	0.5	0.51
0.5	0.48	0.48	0.48	0.5	0.49	0.5	0.48	0.48	0.51	0.49	0.49
0.48	0.5	0.51	0.49	0.49	0.51	0.49	0.5	0.49	0.52	0.51	0.49
0.49	0.51	0.48	0.48	0.49	0.5	0.48	0.51	0.5	0.5	0.51	0.5
0.51	0.5	0.48	0.51	0.48	0.51	0.52	0.49	0.49	0.49	0.52	0.51
0.48	0.50	0.47	0.5	0.51	0.49	0.49	0.49	0.5	0.51	0.51	0.50
0.5	0.48	0.5	0.49	0.5	0.5	0.5	0.48	0.5	0.48	0.5	0.48
0.49	0.48	0.49	0.5	0.51	0.5	0.5	0.49	0.5	0.5	0.52	0.49
0.5	0.47	0.48	0.48	0.50	0.49	0.50	0.51	0.51	0.5	0.5	0.5
0.49	0.5	0.49	0.5	0.5	0.49	0.49	0.49	0.5	0.48	0.49	0.5
0.5	0.51	0.5	0.48	0.49	0.51	0.48	0.5	0.47	0.52	0.51	0.49
0.49	0.5	0.49	0.5	0.5	0.49	0.5	0.49	0.5	0.5	0.47	0.51

Perfekt tulajdonság

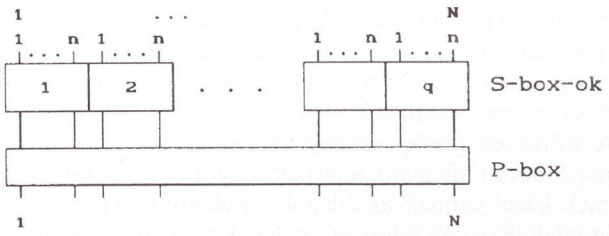
Egy másik nyitott probléma a perfekt Boole-függvények számának pontos meghatározása vagy szigorú becslése. Az mindenesetre sejthető, hogy a perfekt függvények relatíve igen kevesen vannak, így véletlen választással nem lehet őket megtalálni. Sajnos ebben az esetben még a majdnem perfekt Boole-függvények véletlen választása is kivitelezhetetlennek tűnik. A perfektség kritériuma már túl erős a véletlen tervezéshez.

Összefoglalva azt mondhatjuk, hogy balansz, teljes, minden komponensében nem-lineáris és a SAC-et majdnem teljesítő S-box véletlen választással található. De ha megköveteljük a perfektséget, vagy akár csak a definíció szerinti SAC tulajdonságot, akkor konstrukciós módszerekhez kell folyamodnunk.

4. P-BOX TERVEZÉSE ÉS A RÉTEGEK SZÁMA

Az S-box tervezés megalapozott elméletével szemben viszonylag kevés a P-box-okra és a rétegek számának megválasztására vonatkozó eredmény. Egy gyakorlati megközelítés lehet egy bizonyítottan erős rejtjelző struktúrájának megtartása és az S-box-ok, a P-box-ok valamint a kulcsütemező módosítása. Az alábbiakban a P-box-ok véletlen választására vonatkozó eredményeinket ismertetjük, és megadunk néhány egyszerű alsó korlátot a rétegek számára vonatkozóan.

Vegyünk egy N bites SPC-t (Substitution-Permutation Cipher), melynek egy rétege q darab n bites S-box-ból ($q = N/n$) és egy P-box-ból áll.



4.1. ábra. Egy SPC egy rétege

Jól ismert, hogy a rejtjelző kriptográfiai ereje elsősorban az S-box-októl függ. A bit permutáció lineáris és nem változik rétegenként. Szerepe a bemeneten történő bitváltozások hatásának szétszórása, a hatás közvetítése minden egyes bemeneti pozícióról minden egyes kimeneti pozícióra. A P-box-szal szemben támasztott kézenfekvő követelmény, hogy a bemeneten történt változást néhány rétegen belül eljuttassa minden S-box-hoz. A 4.1 Tétel a következő kérdésre ad választ: mennyi annak a valószínűsége, hogy egy véletlenül választott P-box kielégíti a fenti követelményt, azaz hogy ebben az értelemben nem degenerált? Mint látni fogjuk ez a valószínűség szerencsére igen nagy.

4.1 Tétel: Annak a valószínűsége, hogy egy véletlenül választott P-box nem degenerált a következő:

$$P_n(q) = 1 - \sum_{i=1}^{q-1} P_n(i) \cdot \frac{\binom{q-1}{i-1}}{\binom{q \cdot n}{i \cdot n}}, \qquad (4.1)$$

ahol $P_n(1) = 1$.

Bizonyítás: Megtalálható [21]-ben.

Néhány tipikus n és q esetén kiszámoltuk $P_n(q)$ értékét. Az eredményeket a 4.1. táblázat mutatja.

4.1. táblázat

n	q	$P_n(q)$
4	8	0,997
4	16	0,9999
8	4	0,99999
8	8	0,99999

Megjegyezzük, hogy ha egy P-box nem degenerált, akkor a bemeneten történt változás hatása legfeljebb q rétegen belül minden S-box-hoz elér.

Mint már említettük a kódolás egy helyettesítő-permutációs réteg kulcsvezérelt, sokszori egymás utáni alkalmazásával valósul meg. Az alábbiakban ezen rétegek szükséges számára mondunk két viszonylag egyszerű becslést.

Egy bemeneti bit változása legfeljebb n második rétegbeli S-box-ra van hatással. Ezen S-box-ok mindegyike további n S-box-ra lehet hatással a következő rétegben, így a bementei bit változása a harmadik rétegben már n^2 S-box-ot érint. Ezt a gondolatmenetet folytatva könnyen belátható, hogy a rétegek h számára igaznak kell lennie a következő egyenlőtlenségnek:

$$h \geq \log_n q + 1. \qquad (4.2)$$

A változás alsó becslés szerinti gyors szétterjedése megvalósítható szisztematikusan tervezett, szimmetrikus P-boxszal, ami biztosítja, hogy az S-box-ok különböző kimenetei különböző S-box-ok bemeneteihez csatlakozzanak a következo rétegben [6].

A (4.2)-ben megadott alsó korlát szerint $N = 64$, $n = 4$ és $q = 16$ esetén a szükséges rétegek számára $h \geq 3$ adódik.

Egy kicsit erősebb alsó korlátot kapunk, ha a lavinahatás teljesülését is megköveteljük. Feltesszük, hogy az S-box-ok teljesítik ezt a kritériumot.

4.2 Tétel: A lavinahatást teljesítő SPC rétegeinek h számára

$$h \geq (\log_2 N - 1)/(\log_2 n - 1). \qquad (4.3)$$

Bizonyítás: Megtalálható [21]-ben.

A 4.2 Tétel szerint $N = 64$, $n = 4$ és $q = 16$ esetén a szükséges rétegek száma legalább 5. Összehasonlításként megemlítjük, hogy a DES esetén is pont ennyi rétegre van szükség ahhoz, hogy a bemeneti bitek változásának hatása elérjen minden kimeneti bitet (lásd 5. rész).

5. REJTJELZŐ ALGORITMUS STATISZTIKAI TESZTELÉSE

Alapvető tervezési probléma egy kódoló-dekódoló algoritmus kriptográfiai erejének, azaz algoritmikus támadásokkal szembeni védettségének kvantitatív megítélése, pontosabban a bizonyítékok megadása. Hasonlóan, ahogy az elemi helyettesítő transzformációk (S-box-ok) garantáltan erős tervezésére nincsen egységes szabály, a teljes kódoló-dekoló vonatkozásában sincsen olyan végrehajtható tesztrendszer, amely feltétlen garanciát nyújt a támadásokkal szembeni védettségre. Ezért nagyon fontos szerepet töltenek be a statisztikai alapú tesztek, mint első gyengeség-szűrők illetve probléma-indikátorok. Ha egy teszten „nem megy át" egy tesztelt algoritmus, akkor annak pillanatnyi változatát el kell vetni vagy a teszt alapján át kell tervezni. Ha a tesztek sorozatán „átmegy" egy algoritmus, akkor legfeljebb azt mondhatjuk, hogy alapvető statisztikai gyengeséget nem tapasztaltunk, de ez sajnos még nem jelenti azt, hogy nincsen támadható algoritmikus gyengeség benne.

Az Appendix B-ben röviden összefoglaltuk néhány gyakrabban alkalmazott statisztikai teszt alapelvét [7]:

- Frekvencia teszt.
- Széria teszt.
- Futam teszt.
- Lempel-Ziv komplexitás.
- Bináris derivált vizsgálata.

A teszteket kétféle módon is használhatjuk a rejtjelző vizsgálata során. Ha a rejtjelző jól működik, akkor a bemenetére nem véletlenszerű, strukturált blokkokat adva, a kimenetén véletlen blokkoknak kell megjelenni. Ekkor a kimeneten megjelenő rejtjelezett blokkokra alkalmazzuk a teszteket. A másik módszer alapfeltevése, hogy a rejtjelző bemenete és kimenete statisztikailag független. Ekkor a bemenetre adott véletlen p_i blokkok és a kimeneten megjelenő c_i rejtjeles blokkok $s_i = p_i + c_i$ bitenkénti összege véletlen jellegű kell hogy legyen, így az s_i blokkokra alkalmazhatjuk a teszteket.

Érdemes még elvégezni a bemenet-kimenet és kulcskimenet lavinahatás vizsgálatot is. Mivel kimerítő próbára nincs lehetőség, ezért magát a függőségi mátrixot nem tud-

juk vizsgálni. Ismét statisztikai próbákhoz kell folyamodnunk. Ha a rejtjelző teljesíti a SAC-et, akkor bármelyik (i, j) bemeneti-kimeneti (kulcs-kimeneti) bitpárjára igaz, hogy megváltoztatva az i. bemeneti (kulcs) bitet a j-edik kimeneti bit 0,5 valószínűséggel változik meg. Ezt a hipotézisünket χ^2-próbával ellenőrizhetjük. Figyelhetjük azt is, hogy egy bemeneti (vagy kulcs) bit változásának hatására a kimeneten hány bit változik meg. Ha a rejtjelző teljesíti a SAC-et, akkor a j-edik kimeneten történt változások számának eloszlása 0,5 paraméterű binomiális kell legyen. Ezt ismét χ^2-próbával ellenőrizhetjük.

A fent leírt módszerekkel elvégeztük a DES tesztelését, mégpedig négy különböző esetben. Először a DES-t csak 2 rétegig futtattuk, majd 4, 8 és végül a szabványban megadott 16 rétegig. Erre utalnak a DES2, DES4, DES8, DE516 jelölések az 5.1. és az 5.2. táblázatban.

5.1. táblázat

		Próba szint (100-x)	Az esetek ennyi %-a esett a elfogadási intervallumon kívülre			
			DES2	DES4	DES8	DES16
Frekvencia teszt		5%	7.1	6.8	5.6	4.6
		1%	0.9	0.6	0.8	0.2
Szérla teszt		5%	4.0	3.9	5.2	4.1
		1%	0.3	0.5	0.9	0.8
Bináris derivált	P	5%	5.7	5.4	4.2	5.8
		1%	1.2	1.7	0.8	1.3
	R	5%	4.3	4.2	4.2	4.9
		1%	0.8	0.8	0.3	1.3
Lempel-Ziv komplexitás		min	10	10	10	10
		max	16	16	16	15
		átlag	13.09	13.02	13.1	13.07

5.2. táblázat

	Próba szint (100-x)	Az esetek ennyi %-a esett a elfogadási intervallumon kívülre			
		DES2	DES4	DES8	DES16
Bemenet-kimenet függőségi m.	5%	79.68	18.46	5.35	4.35
	1%	76.78	12.72	1.93	1.51
Kulcs-kimenet függőségi mátrix	5%	63.67	15.75	3.69	3.86
	1%	59.96	11.72	0.93	1.89

Az 5.1. táblázat „Frekvencia teszt" sorából, de különösen az 5.2. táblázatból jól látszik, hogy ezek a módszerek valóban használhatóak gyengeségek kimutatására. Az 5.2. táblázat szerint a DES elso négy rétege még nem elegendően erős, hisz a lavinahatást nem teljesíti. Ez a megfigyelés összhangban van a 4. pont rétegek számára vonatkozó állításaival.

Appendix A

Boole-függvény: Boole-függvénynek nevezzük az $f : V_2^n \to V_2^1$, n bitet 1 bitbe leképző függvényt. Az $f : V_2^n \to \{0, 1\}$ Boole-függvény helyett gyakran használjuk az alább definiált $\hat{f} : V_2^n \to \{1, -1\}$ függvényt:

$$\hat{f}(x) = (-1)^{f(x)} = 1 - 2 \cdot f(x). \qquad (A.1)$$

S-box: S-box-nak nevezzük az $f : V_2^n \to V_2^s\}$, n bitet s bitbe leképző függvényt, ahol $s \leq n$. $s = 1$ esetén a Boole-függvény definícióját kapjuk. f-et gyakran fogjuk fel úgy, mint s darab Boole-függvény együttese: $f(x) = (f_1(x), f_2(x), \ldots, f_s(x))$. Az $f_i(x)$ függvényeket komponens Boole-függvényeknek nevezzük.

Walsh-transzformáció: Egy $f : V_2^n \to V_2^1$ Boole-függvény Walsh-transzformáltján a következő $F : V_2^n \to \{\text{egészek}\}$ függvényt értjük:

$$F(w) = \sum_{x \in V_2^n} f(x)(-1)^{x^T w}. \qquad (A.2)$$

Itt tehát a szumma valós összeadást jelöl.

Hasonló módon értelmezhetjük az f Boole-függvényből képzett $\hat{f}$ függvény Walsh-transzformáltját:

$$\hat{F}(w) = \sum_{x \in V_2^n} \hat{f}(x)(-1)^{x^T w} = \sum_{x \in V_2^n} (-1)^{f(x) + x^T w}. \qquad (A.3)$$

A továbbiakban mindig (A.3)-at fogjuk használni az f Boole-függvény Walsh-transzformáltjaként.

1. Balansz tulajdonság

Egy $f : V_2^n \to V_2^1$ függvény balansz, ha tetszőleges $y \in V_2^s$ esetén

$$|\{x, \quad x \in V_2^n : f(x) = y\}| = 2^{n-s}. \qquad (A.4)$$

Ha f Boole-függvény ($s = 1$), ekkor tehát f abban az esetben balansz, ha kimenetén ugyanolyan valószínűséggel jelenik meg 1, mint 0.

Ez a kritérium lényegében azt követeli meg, hogy a transzformáció semmiképp se torzítsa el egy egyenletes eloszlású bemenet gyakoriság-statisztikáját.

2. Algebrai fokszám

Minden $f : V_2^n \to V_2^s$ Boole-függvény egyértelműen megadható algebrai normál alakban (Algebraic Normal Form – ANF):

$$f(x) = a_0 + \sum_{i_1=1}^{n} a_{i_1} x_{i_1} + \sum_{i_1 < i_2}^{n} a_{i_1 i_2} x_{i_1} x_{i_2} + \ldots$$

$$+ a_{i_1 i_2 \ldots i_n} x_{i_1} x_{i_2} \ldots x_{i_n}, \qquad (A.5)$$

ahol az együtthatók binárisak. f algebrai fokszáma megegyezik az algebrai normálalak legmagasabb fokszámú tagjának fokával.

Lényegében az a jó f transzformáció, amelynek ANF alakjában „egyenletesen" sokféle különböző fokszámú tag található. Végzetes, ha nincsen elsőfokúnál nagyobb fokszámú tag, s hasonlóan nem megfelelő, ha csak maximális fokszámú tagok vannak.

3. Teljesség

Egy $f : V_2^n \rightarrow V_2^s$ függvény teljes, ha minden i-re $(1 \leq i \leq n)$ és j-re $(1 \leq j \leq s)$ teljesül, hogy $t_j^{(i)} \neq 0$, ahol $t_j^{(j)}$ az alább definiált $t^{(i)} \in V_2^s$ vektor j-edik komponense:

$$t^{(i)} = \sum_{x \in V_2^n} [f(x) + f(x + e_i)], \qquad (A.6)$$

továbbá $e_i \in V_2^n$, $e_i = (0, 0, \ldots 1, \ldots 0)$ egyetlen egyest tartalmaz az i-edik pozícióban. Az (A.6)-ban szereplő '+' mod 2 összeadást, a '$\sum$' pedig valós összeadást jelöl. Ezen kritérium jelentése az, hogy kerülendő az olyan transzformáció, amelynél vannak hatástalan bemeneti bitek, azaz amelyek változása nem hat a kimeneti bitekre vagy azok egy csoportjára.

4. Nem-linearitás (az affin függvényektől vett távolság)

Egy $f : V_2^n \rightarrow V_2^s$ függvény távolsága az affin függvényektől a következő:

$$N(f) = \min_{w \in V_2^s, w \neq 0} N(w^T f) = \min_{u \in V_2^n, v \neq V_2^1, w \in V_2^s, w \neq 0},$$
$$|\{x,\ x \in V_2 : w^T f \neq u^T x + v\}| \qquad (A.7)$$

ahol $f = (f_1, f_2, \ldots, f_s)$, $f_i : V_2^n \rightarrow V_2^1$, és $w^T f = w_1 f_1 + w_2 f_2 + \ldots + w_s f_s$.

A definíció szemléletesen azt jelenti, hogy egy f függvény nem-linearitása annál nagyobb, minél nagyobb a komponens Boole-függvények tetszőleges lineár kombinációjából képzett $w^T f$ Boole-függvény és az affin Boole-függvények Hamming-távolsága. Mindennemű linearitás kerülendő, mivel az könnyű algoritmikus támadási célpont.Ezért fontos annak kvantitatív megfogalmazása, hogy egy transzformáció milyen „távol" van a lineáristól (affintól).

5. Terjedési kritériumok

5.1. Lavinahatás kritérium

Egy $f : V_2^n \rightarrow V_2^s$ függvény kielégíti a lavina hatás kritériumot, ha minden i-re $(1 \leq i \leq n)$ teljesül, hogy

$$\sum_{x \in V_2^n} wt(f(x) + f(x + e_i)) = s \cdot 2^{n-1}, \qquad (A.8)$$

ahol $wt(.)$ a Hamming-súly függvényt jelöli.

A lavina szó itt azt takarja, hogy egy bemeneti bitben történt változás reményeink szerint a kimeneti vektor bitjeinek átlagosan felében okoz változást. Igazából itt precízebb lenne egyszerű terjedési kritériumról beszélni, mivel a lavinahatás megnevezés inkább a kódoló bemenetéről a kimenetre, sok réteg sokszorozó-permutáló hatásán keresztül létrejött végiggördülő hatásra alkalmasabb.

5.2. Szigorú lavinahatás kritérium (Strict Avalanche Criteria – SAC)

Egy $f : V_2^n \rightarrow V_2^s$ függvény kielégíti a SAC-et, ha minden i-re $(1 \leq i \leq n)$ teljesül, hogy

$$\sum_{x \in V_2^n} [f(x) + f(x + e_i)] = (2^{n-1}, 2^{n-1}, \ldots, 2^{n-1}). \qquad (A.9)$$

Annyiban szigorúbb ez a követelmény, hogy ez implikálja az (egyszerű) lavinahatás teljesülését, de annál szigorúbb, mivel ez megköveteli, hogy minden egyes kimeneti bitben 0,5 valószínűséggel valósuljon meg a bitváltozás, ha egy véletlenül választott bemeneti vektor egy (tetszőleges) elemét megváltoztatjuk.

5.3. r-ed rendű SAC

Egy $f : V_2^n \rightarrow V_2^s$ függvény kielégíti az r-ed rendű SAC-et, ha teljesíti az $(r - 1)$-ed rendű SAC-et, és tetszőleges r bemeneti bit értékét rögzítve az így nyert $f' : V_2^{n-r} \rightarrow V_2^s$ függvény kielégíti a SAC-et. A 0-ad rendű SAC az 5.2. pontban definiált eredeti SAC.

Ez a kritérium a SAC további szigorítását jelenti, amikor is a SAC tulajdonságot akkor is megköveteljük, amikor rögzítjük a bemenet tetszőleges r bitjét tetszőleges értékre, s az így megszorított függvényről követeljük meg a SAC tulajdonságot a fennmaradt szabad input bitek és az output vektor bitjei vonatkozásában.

A 2.1. táblázat '*' -gal jelölt eleme a következő: Egy $f : V_2^n \rightarrow \{1, -1\}$ függvény akkor és csak akkor teljesíti az r-ed rendű SAC-et $(0 \leq r \leq n - 2)$, ha Walsh-transzformáltjára igaz a következő [3]:

$$\sum_{w \in V_2^n} F(w) \cdot F(w + c_s) \cdot (-1)^{w_k} = 0$$

minden $k \in \{1, 2, \ldots, n\}$-re és minden $c_s \in V_2^n$-re $(s = 0, 1, \ldots, r)$ ahol $wt(c_s) = s$ és a c_s vektor k-adik komponense 0, továbbá w_k a w vektor k-adik komponensét jelöli.

6. Differenciális uniformitás

6.1. Perfekt tulajdonság

Egy $f : V_2^n \rightarrow V_2^s$ függvény perfekt, ha az alább definiált $g : V_2^n \rightarrow V_2^s$ differencia függvény minden — rögzített — $\alpha \in V_2^n$, $\alpha \neq 0$ esetén balansz.

$$g(x) = f(x) + f(x + \alpha). \qquad (A.10)$$

Az ún. differenciális kriptanalízis támadási mód, hatékonyan ki tudja aknázni, ha az S-boxok differenciálisan „jelentősebben" nem-balansz tulajdonságúak. Ez azt jelenti, hogy léteznek olyan input differencia-vektorok, hogy ilyen rögzített differenciájú input párokhoz tartozó output differenciák nem egyenletesen veszik fel értékeiket az output térben. Az abszolút egyenletességnek a megkövetelése a perfektségi kritérium.

6.2. Differenciális d-uniformitás

Egy $f : V_2^n \to V_2^s$ függvény differenciálisan d-uniform, ha differencia függvénye „majdnem balansz", azaz

$$\max_{\substack{\alpha \in V_2^n \\ \alpha \neq 0}} \max_{\beta \in V_2^s} |\{x, \quad x \in V_2^n : f(x) + f(x+\alpha) = \beta\}| = d. \tag{A.11}$$

Ezek alapján a perfektség a 2^{n-s}-uniformitással egyezik meg.

Ez a kritérium a perfektségi kritérium enyhítése.

7. Lineáris dimenzió

Egy $f : V_2^n \to V_2^s$ függvény lineáris struktúrája a $\delta \in V_2^n$ vektor, ha

$$f(x) + f(x+\delta) = \text{konstans} \tag{A.12}$$

minden $x \in V_2^n$-re. Belátható, hogy a lineáris struktúrák lineáris alteret alkotnak a V_2^n térben. Ezen altér dimenzióját nevezzük az f függvény lineáris dimenziójának.

A differenciális uniformitás ellentéte a lineáris struktúra, a „szélsőséges" nem-balansz, azaz a konstans differencia. A lineáris struktúrák terének mérete egy hasznos kvantitatív mértéke a transzformáció nem-linearitásának, ugyanis az eredeti f függvény az input lineáris transzformációja útján olyan f' kriptográfiailag ekvivalens függvénybe transzformálható, amelynek ANF alakjában a dimenziótól függő számú elsőfokú tag található.

8. Korreláció immunitás

Egy $f : V_2^n \to V_2^1$ Boole-függvény r-ed rendben korreláció immunis, ha tetszőleges Walsh-transzformáltjára teljesül, hogy

$$F(w) = 0, \text{ minden olyan } w\text{-re, melyre } 1 \leq wt(w) \leq r. \tag{A.13}$$

Ha $F(w) = 0$, akkor belátható, hogy az x bináris input vektorban a w vektor egyesei által kijelölt bitek XOR összege nem korrelált az f kimeneti bitjével.

9. Invariancia tulajdonságok

Egy $f : V_2^n \to V_2^s$ függvény input invariáns egy kritériumra, ha tetszőleges $T_1 : V_2^n \to V_2^n$ invertálható, affin transzformációra $f(x)$ és $f(T_1(x))$ egyszerre teljesítik, illetve nem teljesítik az adott kritériumot, illetve a kritérium azonos kvantitatív eredményt ad.

Egy $f : V_2^n \to V_2^s$ függvény korlátozottan input invariáns, ha input invariáns azzal a megkötéssel, hogy $T_1(x) = P \cdot x^T + b$, ahol $x \in V_2^n$, $b \in V_2^n$, és P egy nxn méretű bit permutációs mátrix.

Hasonlóan, egy $f : V_2^n \to V_2^s$ függvény output invariáns egy kritériumra, ha tetszőleges $T_2 : V_2^s \to V_2^s$ invertálható, affin transzformációra $f(x)$ és $T_2(f(x))$ egyszerre teljesítik, illetve nem teljesítik az adott kritériumot, illetve a kritérium azonos kvantitatív eredményt ad.

Egy leképezés bemenetének, illetve kimenetének lineáris transzformációja útján kapott leképezés az eredetivel kriptográfiai erejét tekintve ekvivalens, tehát ha egy kritérium a kriptográfiai erő mérésének kritériuma kíván lenni attól elváratik, hogy lineáris transzformációkra invariáns maradjon.

Appendix B

Frekvencia teszt

A statisztikai tesztek jelentős része azt próbálja meg eldönteni, hogy egy bináris blokk mennyire véletlen. Egy véletlen blokk minden pozíciójában ugyanolyan valószínűséggel fordul elő az 1, mint a 0, így az egyesek és nullák átlagos számának aránya közel 1 kell legyen elég nagy mintaszám esetén. Ezt ellenorzi a frekvencia teszt azáltal, hogy az egyesek és nullák megfigyelt frekvenciáját χ^2-próbával hasonlítja az egyenletes eloszláshoz.

Széria teszt

A frekvencia teszt nem ellenőrzi a szomszédos pozíciókban előforduló bitminták eloszlását. A 0101...01 blokk például átmegy a frekvencia teszten, hiszen az egyesek és a nullák száma pontosan megegyezik, mégsem tekintjük véletlennek. Ha megfigyeljük a szomszédos pozíciókat, akkor azonnal észrevesszük, hogy a négy lehetséges bitminta közül csak egy, a 01 fordul elő. A széria teszt a szomszédos pozíciókban elhelyezkedő bitek által alkotott bitpárosok megfigyelt frekvenciáját hasonlítja össze az egyenletes eloszlással χ^2-próba segítségével.

Futam teszt

Futamnak nevezzük a blokkban fellépő csupa 1 és csupa 0 sorozatokat. A 001110110000 blokk például 5 futamból áll. Annak a valószínűsége, hogy egy N hosszú véletlen blokkban pontosan k futam van

$$p_k = \binom{N-1}{k-1} \cdot 2^{-(N-1)} \quad (k = 1, 2, \ldots, N). \tag{B.1}$$

A futam teszt a futamok megfigyelt frekvenciáját hasonlítja a fenti eloszláshoz χ^2-próba alkalmazásával.

Egy bináris blokk véletlenségének ellenőrzésére további két módszert említünk meg. Az egyik a blokk Lempel-Ziv komplexitásának [8] kiszámítása, a másik pedig a blokk bináris deriváltjainak vizsgálata [5].

Lempel-Ziv komplexitás

[9]-ben részletes vizsgálat található a véletlen blokkok Lempel-Ziv komplexitásának eloszlásáról. A rejtjelző tesztelése során a blokkok megfigyelt komplexitás-eloszlását a [9]-ben megadotthoz hasonlíthatjuk.

Bináris derivált vizsgálata

Egy bináris sorozat első bináris deriváltját úgy kapjuk, ha megfigyeljük a sorozatban előforduló átlapolódó párokat, és ha a pár két számjegye megegyezik akkor nullát, ha különbözik akkor egyest jegyzünk fel. A második deriváltat hasonló módon nyerjük az első deriváltból stb. Példaként megadunk egy 8 hosszúságú bináris blokkot és annak első három deriváltját:

00111010
0100111
110100
01110

Jelöljük p_i-vel az egyesek hányadát az i-edik deriváltban. A fenti példában például $p_0 = 4/8$, $p_1 = 4/7$,

$p_2 = 3/6$ és $p_3 = 3/5$. Vezessük be továbbá a következő jelöléseket:

$$p_{\max} = \max_i p_i \quad \text{(B.2)}$$

$$p_{\min} = \max_i p_i \quad \text{(B.3)}$$

$$R = p_{\max} - p_{\min} \quad \text{(B.4)}$$

$$P = \frac{1}{k+1} \cdot \sum_{i=0}^{k} p_i \quad \text{(B.5)}$$

Véletlen blokkokra p_0 és P 0,5-höz közeli, R pedig kicsi, még nem véletlen blokkokra p_0 változó, P kicsi, R pedig nagy. [5]-ben leírtak szerint a vizsgálatot az első 7 deriváltra érdemes elvégezni ($k = 7$).

IRODALOM

[1] Contemporary Cryptology: The Science of Information Integrity. ed. by G. J. Simmons, pp. 93-101, IEEE Press, New York, 1991.

[2] T. W. Cusick: „Boolean functions satisfying a higher order strict avalanche criterion", Pre-proceedings, Eurocrypt'93.

[3] R. Forre: „The strict avalanche criterion: Spectral properties of Boolean functions and an extended definition". Advances in Cryptology, *Crypto '88*, pp. 450-468, Springer-Verlag

[4] J. A. Gordon and H. Retkin: „Are big S-boxes best?" *IEEE Workshop on Computer Security*, pp. 257-262, 1981.

[5] H. Gustafson, E. Dawson, B. Caelli: „Comparison of block ciphers."

[6] J. B. Kam and G. I. Davida: „A structured design of substitution-permutation encryption networks", *IEEE Trans. on Computers*, Vol. 28, No. 10., 1979.

[7] D. E. Knuth: „The Art of Computer Programming", Vol. 2. Addison-Wesley, 1973.

[8] A. Lempel and J. Ziv: „On the complexity of finite sequences", *IEEE Trans. on Information Theory*, Vol. IT-22, Jan. 1976. pp. 75-81.

[9] A. K. Leung and S. E. Tavares: „Sequence complexity as a test for cryptographic systems", Advances in Cryptology '84, pp. 468-474.

[10] W. Meier and O. Staffelbach: „Nonlinearity criteria for cryptographic functions", Advances in Cryptology, Eurocrypt '89, pp. 549-562, Springer-Verlag

[11] C. Mitchell: „Enumerating Boolean functions of cryptographic significance", *J. of Cryptology*, Vol. 2., No. 3., pp. 155-169., 1990.

[12] Nemetz T. and Vajda I.: „Algoritmikus adatvédelem", Akadémiai Kiadó, Budapest, 1991.

[13] K. Nyberg: „Perfect nonlinear S-boxes", Advances in Cryptology, Eurocrypt' 91, pp. 378-386, Springer-Verlag

[14] K. Nyberg: „On the construction of highly nonlinear permutations", Advances in Cryptology, Eurocrypt' 92, Preproceedings, pp. 89-94.

[15] B. Preenel, W. van Leekwijk, L. van Linden, R. Govaerts and J. Vandewalle: „Propagation characteristics of Boolean functions", Advances in Cryptology, Eurocrypt '90, pp. 161-173, Springer-Verlag

[16] J. Seberry, X. M. Zhang and Y. Zheng: „Relationships among nonlinearity criteria", Advances in Cryptology, Eurocrypt '94, pp. 389-401, Springer-Verlag"

[17] J. Seberry, X. M. Zhang and Y. Zheng: „Nonlinearly balanced Boolean functions and their propagation Characteristics", Crypto '93, pp. 6.1-6.12, Eurocrypt '94, Springer-Verlag

[18] J. Seberry, X. M. Zhang and Y. Zheng: „On constructions and nonlinearity of correlation immunefunctions", Advances in Cryptology, Eurocrypt '93, Springer-Verlag

[19] I. Vajda and T. Nemetz: „Substitution of characters in q-ary m-sequences", Proceedings AAECC-8, Tokyo, Japan, August 1990, Lecture Notes in Computer Science 508, pp. 96-105, Springer-Verlag

[20] I. Vajda and T. Nemetz: „A cryptographic element based on number system conversion", *Proceedings of the IEEE Int. Symp. on Information Theory*, Budapest, Hungary, June 24-28, 1991. p.127.

[21] I. Vajda and L. Buttyán: „On design criteria for substitution-permutation ciphers", submitted to Cryptologia, Nov. 1994.

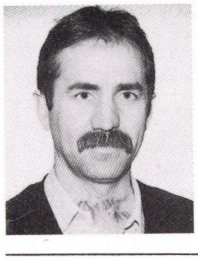
[22] A. F. Webster and S. E. Tavares: „On the design of S-boxes, Advances in Cryptology", Crypto '85, pp. 523-534, Springer-Verlag

ON DESIGN CRITERIA OF CONVENTIONAL BLOCK CIPHERS

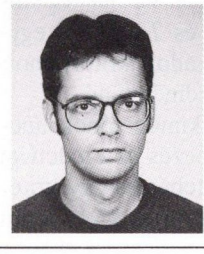
I. VAJDA and L. BUTTYÁN

DEPARTMENT OF COMMUNICATIONS
TECHNICAL UNIVERSITY OF BUDAPEST
H-1111 BUDAPEST, SZTOCZEK U. 2.

Cryptographically strong binary substitution mappings are basic building blocks (S-boxes) in substitution-permutation ciphers. Relationships between different design criteria for strong Boolean functions are investigated. Some associated aspects of random design are also shown. Simple bounds are given for the needed number of rounds. Insight is given into a few basic statistical testing methods at introductory level.



Vajda István 1976-ban szerzett villamosmérnöki oklevelet. 1978-ban egyetemi doktori fokozatot, 1984-ben kandidátusi oklevelet szerzett. Jelenleg a BME Villamosmérnöki Kar Híradástechnikai Tanszékének docense. Fő érdeklődési területe a hibajavító kódolás, a többszörös hozzáférésű csatornák kódolása valamint a kriptográfiai alapú algoritmikus adatvédelem.



Buttyán Levente a BME Villamosmérnöki Kar Informatika Szakának végzős hallgatója. Fő érdeklődési területe az algoritmikus adatvédelem elmélete valamint számítógépes hálózatok adatvédelmi kérdései.

GONDOLATOK AZ ADATÁTVITEL VÉDETTSÉGÉRŐL

PAPP GYÖRGY
MINISZTERELNÖKI HIVATAL
INFORMATIKAI KOORDINÁCIÓS IRODA
1055 BUDAPEST, KOSSUTH TÉR 2–4.

A cikk az adatátvitel biztonsági kérdéseivel foglalkozik. A kommunikáció biztonsága sokkal szerteágazóbb probléma, mint azt gondolnánk. Nemcsak az adatkapcsolattól, a kommunikáció vezérlő eszközöktől és az adattitkosítástól függ, hanem az adatátvitelben résztvevő személyektől és a teljes számítógépes rendszer biztonsági célkitűzéseitől is. Szeretném bemutatni, mi a célja az adatátvitel védelmének, valamint ez milyen kapcsolatban áll a többi számítógépes rendszerelemmel. Mivel a kommunikáció biztonsága terén, ahogy ezt demonstrálom, nincs 100%-os eredmény, a legfontosabb feladatok közé tartozik a biztonsági intézkedések menedzselése és felügyelete. Sajnos ezen a téren igen nagy lemaradás tapasztalható, kevés figyelmet fordítanak erre nemcsak a számítógép rendszert és annak rendszerelemeit előállító cégek, hanem — elsősorban erőforrás hiányában — a rendszert, a hálózatot üzemeltető szervezetek, intézmények és szolgáltató cégek is.

1. AZ ADATÁTVITEL VÉDELMI CÉLKITŰZÉSEI

Amikor adatátvitel, illetve kommunikáció valósul meg, akkor két számítógép vagy számítógépes rendszer között közvetlenül vagy közvetve információcsere jön létre. Az információcsere abban az esetben védett, ha az információcsere szolgáltatást, illetve a szolgáltatás tárgyát, az információt fenyegető veszélyeket sikerül elhárítani. Így az átvitel legfontosabb védelmi célkitűzései közé az információvédelem és a szolgáltatásvédelem sorolható. A szolgáltatásvédelem mellett megjelenik a szolgáltatásban résztvevő eszközrendszerek (fizikai átviteli közeg, pl. kábel, kommunikáció vezérlők, pl. repeater-ek, router-ek, bridge-k, kapcsológépek stb.) mint értéket képviselő vagyontárgyak védelme is.

A kommunikációt fenyegető veszélyek a számítógéphálózatban a következőképpen csoportosíthatók [1]:

- megszemélyesítés;
- visszajátszás, ismétlés;
- az információ módosítása, megsemmisítése;
- hamis információ bevitele;
- az információ felfedése;
- szolgáltatások megtámadása, meghamisítása;
- jogosult felhasználó illetéktelen támadása;
- illetéktelen személy külső támadása;
- rejtekajtó;
- „trójai faló";
- vírusok
- stb.

2. A KOMMUNIKÁCIÓ BIZTONSÁGI SZEMPONTÚ ALAPTERMÉSZETE

Egy számítógépes hálózat alkalmazási szintjén a kommunikáció két hálózati csomópont közötti adat vagy információ átvitelét, illetve cseréjét jelenti. Az információ a legkülönbözőbb típusú lehet. Kezdve a felhasználói adattól, üzenetektől, a különböző erőforrásokhoz való hozzáférés azonosító adatokon át, a fájlok átviteléig minden előfordulhat. A sort hosszan lehetne folytatni, de egy közös dolog jellemzi, mindig a felhasználói alkalmazással áll közvetlen kapcsolatban.

Az információ átviteléhez viszont vezérlési folyamatokra van szükség, amely során a kommunikáló eszközök felismerik, mikor, miért, melyik eszköz szólította meg és ezt megfelelő módon képesek lekezelni. A számítógépes hálózat, az architektúrájától, a kiépítettségétől függetlenül, vezérlést igényel. A különböző értelmezésű vezérlési kapcsolatot megvalósító folyamatot nevezik protokollnak. A protokollokat, melyek az átvitt információhoz hasonlóan a legkülönfélébb struktúrájúak és tartalmúak lehetnek, egyetlen közös dolog jellemzi, a hálózat kommunikációképességét, működését biztosítják. A protokollokra ezenkívül az egymásba ágyazódás is jellemző, amely során egy protokoll valóságos tartalma lehet egy másik protokoll vagy az információ.

Ilyen „leegyszerűsített" megközelítésből a kommunikációt két nagy alkotórészre oszthatjuk:

- a vezérlésére (protokoll) és
- a lényegi tartalmára (információ).

Biztonsági szempontból viszont egy nagyon lényeges tulajdonságot lehet megállapítani. Nevezetesen, közös csatornán jelenik meg mind a vezérlés, mind az információ. Azért fontos ennek hangsúlyozása, mert potenciálisan lehetőség van a két, funkcionálisan elkülönített terület egymás közötti átjárására, ugyanis a vezérlési célú adatokat, amelyek megváltoztathatják egy számítógép-hálózati rendszerelem valamilyen paraméterét, információként is elő lehet állítani, vagy a hálózat vezérléshez szükséges felügyeleti, illetve ellenőrző adatok mások számára információként viselkedhetnek.

Ugyanez a jelenség figyelhető meg a Neumann felépítésű számítógépeknél, tipikusan a személyi számítógépeknél, ahol az alapgondolat az volt, hogy a vezérlési célokat megvalósító programokat ugyanabban a memóriában tárolják, mint a feldolgozásra kerülő adatokat. Ez viszont a közös terület használata révén megteremti potenciálisan az adatok programként történő futtatását és viszont a programok adatokként való értelmezését. Így a „szabad" átjárás tálcán kínált, ami nem kívánt kellemetlen, biztonságot megsértő

hatást válthat ki. Gondoljunk például a számítógépes vírusra. Rengeteg erőfeszítést jelent és energiát köt le az olyan fajta védekezés, amely program és adat ellenőrzést, illetve felügyeletet valósít meg.

Ahhoz viszont, hogy a kommunikáció biztonsággal összefüggő lényeges megállapításait részletekbe menő szinten elemezni lehessen, a teljes számítógépes rendszert átfogó, globális kitekintésre van szükség. A biztonságot nem lehet elszigetelten, a többi kommunikációban résztvevő rendszerelemmel fellépő kölcsönhatásaitól függetlenítve kezelni. A biztonság ezenkívül alaptermészeténél fogva nem rendszerspecifikus elem, az mindig valamilyen érdek képviseletében születik, így azt követelményként kell értelmezni.

3. RENDSZERSZEMLÉLETI KITEKINTÉS, A KOMMUNIKÁCIÓ HELYE

Egy számítógépes rendszer minden esetben valamilyen közösség, csoport, intézmény, szervezet célkitűzéseit támogatja. A célkitűzések a szervezet számára lebontható feladatokban valósulnak meg, amelyeket a munkamegosztás során további részfeladatok követhetnek. Az esetek legnagyobb százalékában a számítógépes rendszer információk és adatok feldolgozását támogatja. Információ a legtágabb értelemben használható, szervezeti célokat segítő fogalomként értelmezhető. Így az információs rendszer számítógépes támogatása valósul meg, amit az egyszerűség érdekében a továbbiakban *informatikai rendszernek* hívok [2]. Az információcsere szintén számítógéppel támogatott módon történhet a számítógépes kommunikáció révén. A számítógépes rendszer, illetve hálózat ezenkívül szolgáltatást valósít meg. Szolgáltatást olyan értelemben, hogy az azt felhasználók rendelkezésére áll és a szervezeti tevékenység feladatrendszerébe illeszkedik.

4. A SZÁMÍTÓGÉPES RENDSZER ALAPFENYEGETETTSÉGE

Az alapfenyegetettség azon veszélyek hatásösszege, amelyek az információk, illetve adatok

- *rendelkezésre állását* (elérhetőségét az arra jogosultak számára),
- *sértetlenségét* (integritását),
- *bizalmasságát* (az illetéktelenek általi megismerhetetlenséget),
- *hitelességét* (a pontosságot és konzisztenciát),

illetve az informatikai rendszer,

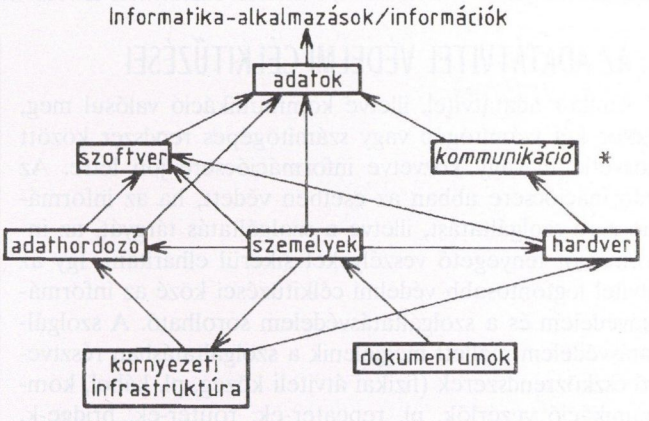
- működőképességét (illetve üzembiztonságát) veszélyeztetik [3] [4].

A veszélyek az informatikai rendszerelemekhez rendelhetők. Mivel az informatika-alkalmazás függ a rendszerelemektől az intézmény tevékenységét támogató informatika-alkalmazás biztonságát a rendszerelemeken keresztül megjelenő károk határozzák meg. Éppen ezért kell megvédeni a rendszerelemeket a veszélyek ellen. Valamennyi olyan rendszerelemet védeni kell, amelyektől az informatikai rendszer működése és valamilyen módon az alkalmazásai függnek, és amelyeket valamely fenyegető tényező negatív módon érinthet. Ehhez a következő rendszerelemcsoportokat célszerű áttekinteni [5], [6], amellyel a kommunikáció helye is megfigyelhető (1. ábra).

Az egyes elemcsoportok között alapvetően komplex függőségi viszony áll fenn abban az értelemben, hogy egy rendszerelem rendelkezésre állása, sértetlensége, bizalmassága, hitelessége és működőképessége más rendszerelemek rendelkezésre állását, sértetlenségét, bizalmasságát, hitelességét és működőképességét feltételezi. Átfogó megközelítésben a 2. ábra szemlélteti azokat a függőségi viszonyokat, amelyek a nyolc rendszerelem-csoport között fennállnak.

Tárgyiasult elemcsoportok	környezeti infrastruktúra
	hardver
	adathordozók
	dokumentumok, iratok
Logikai elemcsoportok	szoftver
	adatok
	kommunikáció ⇐
Személyi elemcsoport	személyzet, felhasználók, ellenőrök

1. ábra. A rendszerelemek nyolc csoportja



2. ábra. Az elemcsoportok függőségi viszonyai

A függőség szemléltetésére egy példa: Az adatok sértetlensége függ az alkalmazói- és a rendszerszoftverek működőképességétől. A szoftver rá van utalva egy sértetlen és rendelkezésre álló hardverre. A környezeti infrastruktúra — mint például az áramszolgáltatás — nélkül egyetlen informatikai rendszer sem üzemképes. Központi szerepet játszanak a személyek, egyebek között felhasználói, kezelői, adminisztrációs-igazgatási, őrzői funkciójukban.

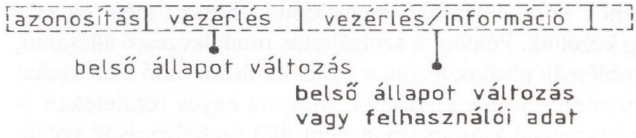
A számítógép-hálózat a kommunikációs rendszeren keresztül azért támadható, mert logikai értelemben a vezérlésbe ágyazott vezérlési és felhasználói információk manipulálható módon egymással és egymás között is kicserélhetők, helyettesíthetők. Természetesen ezek a cserék csak olyan meghatározott értelmezési tartományban valósíthatók meg, amelyek nem eredményezik a rendszer működőképességének megszűnését, a rendszer leállását. A kommunikáció során, a fizikai rétegben megjelenő vezérlés és az információ fizikailag sem különül el egymástól, mert a vezérlés a tényleges információval, a kapcsolat teljes menetében ugyanolyan elemi struktúrában jelenik meg.

Egy felépített konkrét számítógép-hálózatban véges azon állapotok száma, amelyek a hálózati csomópontok közötti kapcsolatok és a csomópontokban kialakított, ún. „normális" üzemeltetéshez szükségesek, ugyanis megszámlálható azoknak a rendszerprogramoknak, az alkalmazá-

soknak, a kezelt adattípusoknak, az engedélyezett felhasználóknak, illetve felhasználói csoportoknak stb. a száma, amelyek és akik a konkrét, üzemelő rendszerben előfordulnak.

Ezzel szemben azon kommunikációs kapcsolatoknak, illetve állapotoknak a száma, amelyek ebben a hálózatban előfordulhatnak, nem korlátos, mert az információ mérete, kiterjedtsége, hosszúsága változó és a hálózat működőképességének időtartama nincs korlátozva. A nem korlátos számosság szerinti kapcsolatból az adott hálózati struktúrában viszont véges számú tesztelés végezhető el, ezért a teszteletlen ágak előfordulási valószínűségi értéke nem nulla.

Ebből az is következik, hogy nem nulla azon események előfordulási valószínűség értéke, amelyek a számítógép-hálózat információcsere szolgáltatásának információs blokkjába olyan vezérlő adatot helyeznek, amely segítségével az egyedi hálózatvezérlő egységek belső paramétereinek, illetve értékeinek módosítására, felfedésére, megsemmisítésére nyílik lehetőség. Ugyanis mind az információ, mind a protokoll adategység felcserélhető vezérlő és manipulációs adattal és így nem korlátos számú ilyen esemény fordulhat elő (3. ábra).

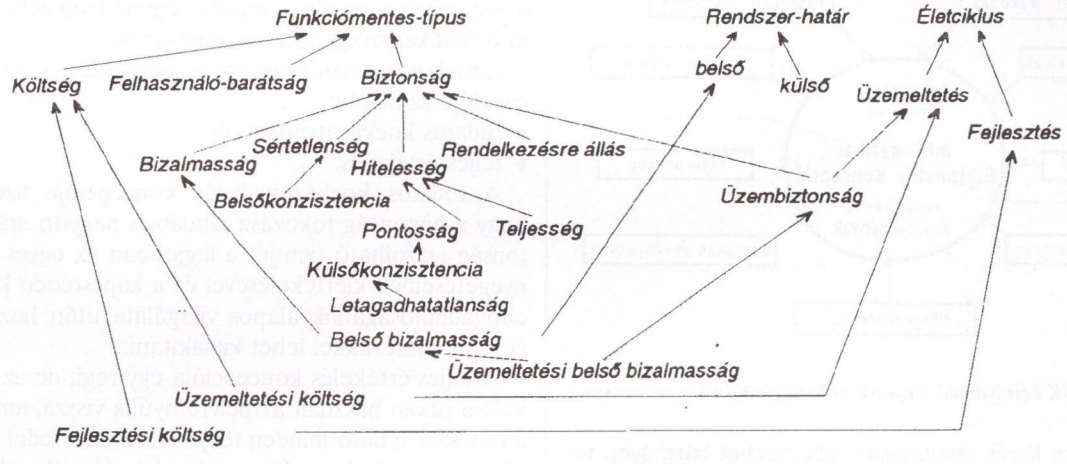


3. ábra. A protokollok egymásba ágyazódásából eredő manipulálhatóság

Ezzel a jelenséggel magyarázható, hogy a hálózatot az információ vagy az erőforrások megsemmisítése, az információ meghamisítása vagy módosítása, az információ vagy az erőforrások ellopása, eltávolítása vagy elvesztése, az információ felfedése, nyilvánosságra hozása, a szolgáltatás megszakítása vagy meghamisítása veszélyek fenyegetik.

5. A BIZTONSÁG, MINT FUNKCIONALITÁS MENTES KÖVETELMÉNY ÉRTELMEZÉSE

A biztonság nem kapcsolható közvetlenül össze működési paraméterekkel, nem írható le egzakt formában, csak az üzemelés, illetve adott folyamat minőségére utaló tulajdonságként értelmezhető, ezért minőségi kategória. Így, hasonlóan a többi minőségi jellemzővel meghatározható fogalommal, a biztonságot funkcionalitás mentes követelménynek (Non-Function Requirement, NFR) értelmezzük [7]. Így a számítástechnikai, mint informatikai rendszer egészét tekintve, funkcionális és funkcionalitás mentes követelmények (Non-Function Requirements, NFR) együttes célkitűzései jelennek meg. Ez alapján a biztonságnak, mint funkcionalitás mentes követelménynek az informatikai rendszerben elfoglalt helyét a célhoz kötöttség határozza meg. A célhoz kötöttség kapcsolatban áll az informatikai rendszer, az egyéb intézményi és intézménykapcsolati célokkal. Számos szempont között az üzleti is megjelenik, így a gazdaságosság, a költség és profit is szerepet kap. A 4. ábra ezt a kapcsolatrendszert mutatja be, amelyben a biztonság elhelyezkedését emelném ki.



4. ábra. Az informatikai rendszer funkcionalitás mentes követelményeinek (Non-Function Requirements — NFR) modellje

A kommunikáció biztonsága során üzemeltetési belső bizalmasság is előtérbe kerül. Ahhoz, hogy a biztonságot, mint funkcionalitás mentes követelményt meghatározzuk, ugyanolyan, de más szinten előforduló funkcionalitás mentes követelményeket kell teljesíteni. Ez a paradox helyzet az egész biztonsági megközelítésre jellemző. Utalni lehet a középkori várak, mint erődítmények szemléletére, vagy a számítástechnikában alkalmazott, az Amerikai Egyesült Államok Nemzetbiztonsági Hivatalának Számítógép Központja által felállított, megbízható központi védelmi bázis (trusted computing base — TCB) fogalmára. Mindegyik védelmi filozófia abból a feltételezésből indul ki, hogy léteznie kell egy olyan szigorúbb védelemmel elkülönített magnak, amelyek őrködik a többi rendszerelem és rendszerfunkció védelme felett.

Ez a megközelítés is azt bizonyítja, hogy a biztonság nem lehet 100%-os eredményű, csak törekedni lehet annak megközelítésére. A kommunikációs rendszerbe történő illetéktelen beavatkozás során feltételezhető, hogy az aktív támadó rendszerspecifikus jellemzők birtokában van. Ugyanis támadása csak akkor lehet sikeres, ha a rendszerspecifikus jellemzők mellett ismeri vagy felderíti a rendszer

gyenge pontjait. Annak a kiegészítő egységnek, amelynek feladata lenne az aktív támadások felfedése, ugyancsak rendelkeznie kell, a támadás lehetséges változatainak tudásával, illetve azon eseménysorozatok ismeretével, amelyek az eredményes támadáshoz szükségesek. Ezzel a gondolatmenettel juthatunk el az ismeretalapú rendszer felé.

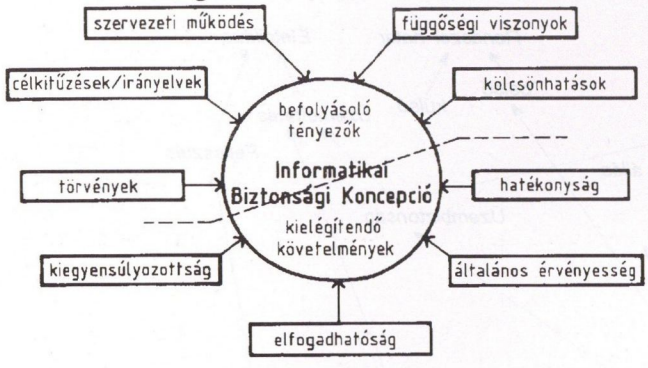
6. EGYÉB INTÉZMÉNYI ÖSSZEFÜGGÉSEK

A megfogalmazott biztonsági célkitűzéseket, elvárásokat egy intézmény biztonságerősítő lépések meghozatalával, azaz védelmi intézkedések megtervezésével és beépítésével érvényesítheti. A védelmi intézkedéseket célszerűen az intézmény informatikai biztonsági koncepcióban (IBK) rögzíti [3]. Ez az adott intézményre vonatkoztatott taktikai lépésként kezelhető, mert az adott helyen a legkedvezőbb megvalósítással foglalkozik.

Az informatikai biztonságerősítő taktikai lépéseket nem lehet elvonatkoztatni az alapvető szervezeti feladatoktól, célkitűzésektől. Minél nagyobb egy szervezet, annál inkább rákényszerül, hogy célkitűzéseit, feladatait egy jól összehangolt munkamenetben kezelje.

Ennek a módszernek az alábbi legjellemzőbb megelőző lépései vannak:

- *Politika*: Abban a tekintetben, hogy meghatározza a szervezési és vezetési irányelveket, célkitűzéseket.
- *Stratégia*: Abban az értelemben, hogy meghatározza a tervezési, a szervezési és irányítási módszereket.
- *Garancia*: Abban az értelemben, hogy meghatározza az irányelvek, célkitűzések érvényesüléséhez és fennmaradáshoz szükséges összetevőket.

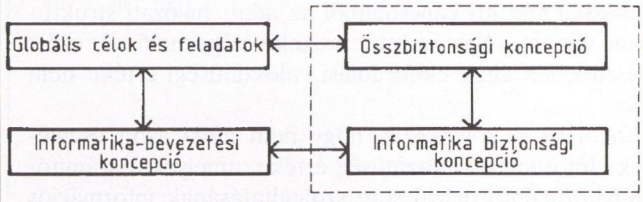


5. ábra. Az IBK befolyásoló tényezői és kielégítendő követelményei

Ez a három lépés általánosan jellemezhet bármilyen tevékenységet, amelyekkel a célok, a megvalósítás és fennmaradás feltételrendszere elkülönülten kezelhető [8].

Az 5. ábra az informatikai biztonsági koncepciót befolyásoló tényezőket, illetve a megvalósítandó követelményeket szemlélteti. Az informatikai biztonsági koncepció során ezek érvényesülésére, illetve érvényesítésére figyelemmel kell lenni [5], ahol gyakorlatilag a biztonsági célkitűzéseket megvalósító politikai, stratégiai lépések és garancia feltételei határozzák meg a tényleges kapcsolatokat.

Az informatika biztonsági koncepciót az adott intézmény összbiztonsági koncepciójába kell integrálni. Ez utóbbiban kell meghatározni a biztonsági stratégiát, azaz a biztonságot érintő általános célkitűzéseket. Az általános biztonsági stratégiából vezethetők le a még elviselhető maradványkockázatok mértékei és a tervezett intézkedések elfogadhatósága. Ha még nem létezik biztonsági stratégia, akkor annak a kiindulópontjául lehet tekinteni az informatika biztonsági koncepcióban szereplő megállapításokat, ezek segítségével megfogalmazni a generális biztonsági célokat és irányelveket. Ugyanakkor az IBK-t egyeztetni kell az informatikai bevezetési koncepcióval is, mint ahogyan — ideális esetben — a biztonsági stratégiának össze kell csengenie az adott szervezet feladataival és céljaival (6. ábra).



6. ábra. Az IBK beágyazódása

7. BIZTONSÁGTERVEZÉSI IRÁNYELVEK

Annak ellenére, hogy a biztonsági kérdések az informatikai szolgáltatások területén már az informatika történelmének korai fázisában megjelentek, hosszú ideig egyedileg kezelték. Például a szolgáltatás rendelkezésre állásának problémáit elválasztották a szolgáltatáshoz való illetéktelen hozzáférések ellenőrzésétől. Még az egyes területeken is az egymással kapcsolatban nem álló szabályozások voltak a jellemzőek (pl. tűz, rendszerbe történő illetéktelen behatolás, adatvesztés stb.). Ez a megközelítés ma már nem tudja az egyre fokozódó biztonságot érvényesíteni, amelyet a szervezetek tevékenységeibe egyre mélyebben beépülő informatikai szolgáltatások igényelnek.

Ennek az új biztonsági megközelítésnek a két kulcskoncepciója az alábbi:

- tudatos kockázatvállalás és
- teljes értékelés.

A tudatos kockázatvállalás koncepciója azon alapul, hogy a biztonság fokozása általában nagyon drága. A biztonság igazolható szintjét a legjobban az egyes esetek fenyegetéseinek kiértékelésével és a kapcsolódó kockázatok elfogadhatóságának alapos vizsgálata után hozott felelős vezetői döntésekkel lehet kialakítani.

A teljes értékelés koncepciója egy régi, de az informatikában ritkán használt alapelvre nyúlik vissza, amely szerint a rendszerre ható minden tényezőt fel kell fedni és elemezni kell. Döntések csupán a teljes kép fényében hozhatók.

A fenti két koncepciót kockázatelemzési és irányítási módszerekkel vezették be a gyakorlatba. Ezek a módszerek segítenek az informatikai rendszerek kívánt biztonsági szintjének meghatározásában és a problématerületek feltárásában. Észre kell venni, hogy minden önálló területen azonban konkrét védelmi intézkedéseket dolgoztak már ki. Így egy ilyen módszer tudatos bevezetése és az egyedi már kialakított technikai megoldások kombinációja sokkal hatékonyabb védelmet tesz majd lehetővé, mint a hagyományos, szétforgácsolódó megközelítés.

Az előbbi megállapítások alapján egy intézmény biztonságerősítő lépéseinek tervszerűségét többek között az alábbiak indokolják:

- alapvető célkitűzések közé tartozik az alaptevékenység minőségének javítása,
- a minőségbiztosítás nem érvényesül, ha a fenyegető veszélyek elhárítása, hatásainak csökkentése nem valósul meg,
- a feladatok és a teljesítésüket támogató rendszerek komplexitása, valamint az intézményi tevékenység során megjelenő törvényesség betartása miatt a minőség javításához szakszerűen elkülönített biztonsági program szükséges,
- a tervezés során szükségessé váló felügyeleti és menedzselési feladatok hiányában észrevétlenek maradhatnak az informatikai rendszert, így az intézményt érő veszteségek, mert az „amit nem látunk az nincs" elve érvényesül,
- a tervezés nélkül az értékek aránytalan védelme valósulhat meg,
- a törvényességi kötelezettség figyelmen kívül hagyásának a veszélye fennáll.

A védelmi intézkedések tervezési módszerei az informatikai biztonsági koncepció gyakorlati megvalósításai, vagyis a tervezési stratégia megválasztása során különbözők lehetnek. A leggyakrabban a kockázatelemzési módszer használatos, ahol a védelemre fordított költséget állítják arányba a védelem hiányából bekövetkezhető károk nagyságával. Ezek csakis becslésekkel valósíthatók meg. Léteznek ezenkívül a kritikus működési jellemzők, valamint az értékek sérülési hatásainak elemzési módszerei is. Míg az előbbi az intézmény számára különösen fontos, releváns tevékenységek rangsorolásával és a sorrend szerinti védelmi intézkedések súlyával dolgozik, addig az utóbbi a várható károk nagyságrendjére koncentrál. Ezek a módszerek az intézmény kiterjedtségétől függően vegyesen is alkalmazhatók [9].

8. ÉRVÉNYESÍTÉSI TERÜLETEK

A biztonságnak az informatikai rendszer teljes életében fenn kell maradnia. Ahhoz, hogy ezt a feltételt hatékonyan teljesíthessük, célszerűnek látszik érvényesítési területeket kijelölni, annak érdekében, hogy a feladatok és hatáskörök elkülöníthetők legyenek egymástól. Az alapvető érvényesítési területek a tervezés, bevezetés, üzemeltetés, ellenőrzés területei.

Az érvényesítési területekre jellemző, hogy nem szükséges módosítani a már lefektetett alapelveket (politika, stratégia, garancia). A területek, a kezelhetőség átláthatósága és a feladat-, hatáskör elkülönítése miatt tovább finomítható *működési, szervezeti és biztonsági területekre*.

A működési terület lényege, hogy ezen belül egy adott főtevékenység vagy a tevékenységek egy csoportja fogalmazódik meg. Ezzel a működési terület teljes egészében lefedi a főtevékenység minden mozzanatát, így a főtevékenység biztonsági elemzése során egyenértékűnek tekinthetők a vizsgálatok eredményei.

A működési terület kiépülése során szervezetekkel, így szervezeti területekkel találkozik. A tevékenység teljes menete a szervezeteken keresztül szabályozott. A szervezetekre a fizikai elkülönültség jellemző, ezért célszerű figyelembe venni.

A harmadik leglényegesebb és tovább már nem osztható logikai egység az ún. biztonsági terület. A biztonsági terület minden esetben valamilyen működési területhez, mint elsődleges biztonsági igényhez vagy szervezeti területhez, mint másodlagos biztonsági követelményhez kapcsolódik.

A biztonsági területet az alábbi tulajdonság jellemzi:

- a biztonsági követelmények egységesek a biztonsági területen belül,
- a biztonsági területek nem bonthatók le további kisebb, azonos biztonsági célkitűzésű területekre.

A biztonsági terület fogalom bevezetésével gyakorlatilag a főtevékenységre jellemző ún. biztonsági lánc építhető fel és ennek teljes elemzésével egyenszilárdságot lehet kialakítani. Gyakran emlegetett mondás, ami ide illik, hogy egy lánc a leggyengébb láncszemnél szakad el. A tevékenységre vonatkozó egyenszilárdság pedig ennek a képzeletbeli láncnak a felépített szakszerű vizsgálatával biztosítható. Azért is lényeges ez a fajta megközelítés, mert túl a könnyebb kezelhetőségen és feladatokra bonthatóságon, előnye, hogy egyszerűbben vehetők figyelembe az informatikai rendszeren kívüli egyéb szempontok.

9. A BIZTONSÁG FELÜGYELETÉNEK ÉS ELLENŐRZÉSÉNAK JELENTŐSÉGE

A biztonság-felügyelet hiányában nőnek az intézmény fennmaradását befolyásoló kockázatok, mert észrevétlenek maradhatnak a rendszer gyengülését meghatározó tényezők, információ szivároghat ki. Olyan támadások léphetnek fel a rendszer ellen, amik alapvetően blokkolhatják a számítógéprendszer működését.

A követhetőség és a menedzselhetőség legfontosabb igénye az informatikai rendszerekkel szembeni minőségbiztosítás fenntartása. Erre az esetre vonatkozik igazán, hogy az informatikai biztonság minőségi kérdés. Természetesen, ha nem tudjuk, hogy mit menedzseljünk, akkor a minőség nem garantálható.

Az alapelv minden esetben az, hogy az informatikai rendszer üzemeltetése során gondoskodni kell a meghozott biztonsági, illetve védelmi intézkedések fennmaradásáról.

A legfontosabb biztonság menedzselési feladatok az alábbiak:

- *hozzáférés szabályozás*, ahol az illetékességi jogok (előállítás, betekintés, módosítás, törlés) kiosztása minden területen és minden szinten;
- *hozzáférés ellenőrzés*, ahol az illetékességi jogok rendszeres ellenőrzését és az illetéktelen hozzáférések felfedését, elhárítását kell elvégezni;
- *integritás ellenőrzés*, ahol az informatikai rendszer elemeinek sértetlen állapotát kell ellenőrizni (legfontosabb az operációs rendszer, az alkalmazási programok és az adatok sértetlenségének ellenőrzése);
- *adatbiztosítás*, ahol a legfontosabb rendszerelemek (programok, alkalmazások, adatok) mentését és biztonságos őrzését kell megoldani. Ez szolgálhatja ki a hibaáthidalási és újraindítási menedzselési funkciókat;
- *hibaáthidalás*, ahol a rendszert ért hibákat kell felfedni és azokat elhárítani. Ide tartozik a vírus felismerés és mentesítés is;
- *újraindítás*, ahol a váratlan esemény vagy katasztrófa helyzet során az üzemből kiesett informatikai rendszert kell újra üzemképes állapotba hozni;

- *konfiguráció menedzselés*, ahol a teljes rendszer felügyelete során kell gondoskodni az új eszközök üzembeállításáról, a régi eszközök kivonásáról és a teljes rendszer technikai és alkalmazói szintű jellemzőinek nyilvántartásáról.

Mindezen bonyolult feladatok akkor végezhetők el hatékonyan, ha olyan támogató segédeszközök, alkalmazások állnak a menedzsment rendelkezésére, amelyek a fenti funkciókat jól kezelik és semmi esetben sem gyengítik a védelmet.

10. ELÉRT NEMZETKÖZI EREDMÉNYEK ÖSSZEFOGLALÁSA

A számítástechnikai rendszerek adatbiztonsági problémáival, érthető módon, legkorábban az Amerikai Egyesült Allamokban kezdtek foglalkozni. Az Amerikai Egyesült Allamok az általános számítástechnikai rendszerekre vonatkoztatva, információ védelmi szempontból a következő területeket különítette el, amelyek napjainkban is érvényes:

- Hírközlés biztonsága (COMSEC): a hírközlés védelmét jelenti elektronikai eszközök segítségével.
- Rejtjelezési biztonság (CRYPTOSEC): az információ rejtjelezését jelenti különböző típusú rejtjelezési eljárások felhasználásával.
- Számítógépes biztonság (COMPUSEC): a számítógépes rendszerek védelmét jelenti elektronikai, szoftver és adminisztratív eszközök felhasználásával.
- Kisugárzás elleni védelem (TEMPEST): a különböző hírközlő és számítógépes berendezések káros, áruló kisugárzásának megakadályozására szolgáló ellentevékenység.
- Atviteli biztonság (TRANSSEC): az adatátvitel védelmét jelenti a lehallgatás és a beavatkozás ellen.
- Fizikai biztonság (PHYSICSEC): az eszközök és információk fizikai őrzés védelmére vonatkozik.
- Személyi biztonság (PERSEC): az információval kapcsolatba kerülő személyek kiválogatásával és rendszeres ellenőrzésével foglalkozó terület.

A számítógéprendszerek biztonsági szempontú tervezéseinél az alább felsorolt modellezési technikák használatosak, amelyek elsősorban bizalmassági és integritás elemzés specifikus modellként váltak ismertté:

- Bell La Padula modell,
- Biba integritás modell,
- Denning féle információ áramlási modell,
- Rushby féle szeparációs modell,
- Take-Grant modell,
- Landwehr's féle biztonsági modell katonai üzenetközvetítő rendszerek számára,
- Clark Wilson modell,
- Bewer-Nash Chinese Wall modell.

11. BIZTONSÁGI KÖVETELMÉNYEK, SZABVÁNYOK

A fejlett országok az előző fejezetekben ismertetett politikai, stratégiai, garanciális tervezési lépéseket követik tevékenységük során. Ugyanez jellemzi az informatikai rendszerekkel kapcsolatban előforduló és az informatikai biztonságerősítő tevékenységeket is. Számos szakirodalom áll rendelkezésre, amelyek ennek a szellemében csoportosítják a legkülönbözőbb informatikai biztonsággal összefüggő feladatokat [10], [11], [12].

A nemzetközi szakirodalom kiemelten foglalkozik a fentieken túl, a számítástechnikai és átvitel-technikai biztonsági feladatokkal. Mivel az informatikai rendszereknek legnagyobb részterülete a számítástechnika, ezért fontos ezen anyagok alapelveinek megismerése.

12. TCSEC (TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA) — (ORANGE BOOK)

Az Amerikai Egyesült Allamok Védelmi Minisztériuma kidolgozott „Megbízható számítástechnikai rendszer biztonságkiértékelési követelménye" címmel egy olyan módszert, amelynek segítségével a számítástechnikai rendszerek különböző biztonsági követelményeket teljesítő szintekre, osztályokba sorolhatók [13], [14]. Az osztályok úgy lettek kialakítva, hogy a legalacsonyabbtól a legmagasabb védettségi szintet lehet elérni, az ajánlott védelemtől kezdve a kötelező védelmen keresztül a bizonyított védelemmel bezáróan.

A védelmi osztályok a következő elnevezéseket kapták:

D osztály: Minimális védelem,
C osztály: Szelektív védelem,
C1: Korlátozott védelem,
C2: Ellenőrzött hozzáférés-védelem,
B osztály: Kötelező védelem,
B1: Cimkézett védelem,
B2: Strukturált védelem,
B3: Szeparált biztonsági egységek,
A osztály: Bizonyított védelem,
A1: Bizonyított tervezés.

13. ITSEC (INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA)

Az Európai Közösség keretében négy fejlett európai ország, Németország, Egyesült Királyság, Franciaország és Hollandia szakértői kidolgozták az „Informatikai rendszerek biztonság kiértékelési követelmények" című ajánlást [15]. Az ajánlás az TCSEC követelményeit maximálisan figyelembe veszi.

Ezentúl megfogalmaz biztonsági célkitűzéseket, elvárásokat, melyek a következők:

- azonosítás és hitelesítés,
- hozzáférés-jogosultság kiosztás,
- hozzáférés-jogosultság ellenőrzés (felelősségre vonhatóság),
- bizonyíték biztosítás (könyvvizsgálat),
- újraindítási képesség (eszköz-újrafelhasználás),
- hibaáthidalás (pontosság),
- funkcionalitás (szolgáltatás megbízhatóság),
- átviteli biztonság (adatcsere).

Az ITSEC arra nem ad választ, hogy a védelmet hogyan, milyen eszközökkel kell megvalósítani az egyes biztonsági célkitűzések, elvárások vonatkozásában, de a követelményszintek során a megvalósítás minőségét és erősségét ellenőrzi. A vizsgálat fogja azután meghatározni, melyik biztonsági osztályba sorolható a termék.

14. ISO 7498-2

A nyílt rendszerek ISO szabványsorozat biztonsági architektúra szerint határozza meg a nyílt rendszerek kapcsolataira jellemző kommunikációs biztonsági „elvárásokat" [1]. A szabvány elsősorban az adatcsere vonatkozásában dolgozza ki részletesen a követelményeket, így megállapítható, hogy az ITSEC és az ISO 7498-2 nagyon jól kiegészíti egymást. Mivel az ITSEC a TCSEC alapjaira épül, az ITSEC és az ISO 7498-2 dokumentumok alapos szakmai ismerete segíthet eligazodni a számítástechnikai és átviteltechnikai követelményein túlmutató informatikai rendszer követelményeinek meghatározásában. Megjegyezzük, hogy az ISO 7498-2 szabványt a CCITT X.800 néven átvette és sokszor ilyen néven is hivatkoznak rá.

Az ISO 7498—2 által meghatározott biztonsági mechanizmusok:

- rejtjelezés,
- digitális aláírás,
- hozzáférés ellenőrzés,
- adat sértetlenség,
- hitelesség csere,
- hamis forgalom,
- forgalom irányítás,
- közjegyzői hitelesítés.

Természetesen a szolgálatok és a mechanizmusok a szabványon belül az OSI rétegei szerint is kibontásra kerülnek.

15. COMMON CRITERIA (A JÖVŐ)

Tekintettel arra, hogy ezek a kidolgozott követelmények, ha nem is sokban, de eltérnek egymástól, a számítástechnikai ipar fellegvárait alkotó nemzetek célszerűnek látták, hogy az egyre növekvő világméretű kiterjedtség és összekapcsoltság érdekében egységes biztonsági követelményrendszert dolgozzanak ki. Common Criteria néven indult meg az a projekt, amelyik ennek a célnak az elérése érdekében született. Az előzetes tervek szerint várhatóan 1995 elejére születik meg a vitára bocsátott nyilvános változat [16].

16. KÖVETKEZTETÉS, ÉRTÉKELÉS

Az adatátvitelt általában a következő veszélyek fenyegetik:

- az információ és/vagy az erőforrások megsemmisítése,
- az információ meghamisítása vagy módosítása,
- az információ és/vagy az erőforrások ellopása, eltávolítása vagy elvesztése,
- az információ felfedése, nyilvánosságra hozása,
- a szolgáltatás megszakítása vagy meghamisítása.

Ezek a veszélyek lehetnek véletlenek vagy szándékosak. A véletlen esemény mögött rendszerhiba, működési rendellenesség vagy emberi hiba áll, míg a szándékos fenyegetés mögött előre megfontolt támadás van. A kommunikáció biztonságát a véletlen és szándékos fenyegetések egyaránt veszélyeztetik. A szándékos fenyegető események passzívak vagy aktívak. A passzív fenyegetés megfigyelést, lehallgatást jelent, az aktív fenyegetés pedig tevékeny támadást, beavatkozást a rendszer működésébe.

Annak ellenére, hogy a szakirodalom a számítástechnikai rendszerek biztonságát a legkülönbözőbb oldalról közelíti meg és számos módszer áll rendelkezésre a számítógépes rendszerek és hálózatok tervezésére, a biztonságfelügyelet és biztonság menedzselés kialakítására kevés módszer ismert. Jelenleg a *naplózást* és ezen *napló eredmények elemzését*, a *könyvvizsgálatot* alkalmazzák legelterjedtebben. A jelenleg alkalmazott módszerek hatékonysága, különösen hazánkban, sajnálatos módon csekély. Gyakran későn kerül felismerésre az illegális beavatkozás ténye, mert a napló nyilvántartások manuális értékeléséből adódó tévedések és a naplózatlan események miatt maradhatnak feltáratlan illegális beavatkozásra utaló rendkívüli események.

A kereskedelmi forgalomban megjelentek a számítógéphálózatok menedzselését elősegítő támogató eszközök, amelyek rendelkeznek bizonyos mértékű biztonság beállítási, mérési jellemzőkkel és jelzési funkciókkal (protokoll analizátor, Kerberos rendszer, firewall stb.), de mindegyikről kimondható, hogy nem valósítja meg és ennek értelmében nem támogatja az egységes védelmi célkitűzéseket.

A megbízható (trusted) számítógéprendszerek hálózati kiépítettségük csak a lokális hálózat szintjén maradt, ahol nem érvényesül egyelőre az elosztott struktúra. Így megállapítható, hogy előrelépést csak az jelentene, ha módszertani kutatási eredmények állnának rendelkezésre a hálózat biztonság-felügyeleti és menedzselési funkciók kialakítására, amelynek segítségével beépíthetővé válik a kommunikációs rendszert leginkább fenyegető illegális beavatkozások eseményeinek detektálási és a bizonyíték biztosításához szükséges nyilvántartási műveletei.

IRODALOM

[1] International Standards Information Processing Systems, *Open System Interconnection Reference Model*; Security Architecture, ISO 7498—2, 1988.

[2] Papp Gy.: „Utmutató az informatikai biztonsági szabályzat elkészítéséhez," tanulmány, *Miniszterelnöki Hivatal, Informatikai Koordinációs Iroda*, 1993. június.

[3] Papp Gy., Berencsi I., Horváth G., Dr. Nagy K., Szekér K.: „Informatikai Biztonsági Módszertani Kézikönyv," *Miniszterelnöki Hivatal, Informatikai Koordinációs Iroda*, ITB 8. sz. ajánlása, 1994.

[4] Papp Gy., Dr. Dudás J., Dr. Hetesy Zs., Horváth G., Dr. Nagy K., Szekér K.: „Kriptográfia a kormányzati informatikában," tanulmány, *Miniszterelnöki Hivatal, Informatikai Koordinációs Iroda*, 1993. december.

[5] Informationtechnik Sicherheitshandbuch — KBSt, Bonn, 1991.

[6] Papp Gy.: „Biztonságos informatikai rendszerek tervezése és működtetése," *Adatvédelem, adatbiztonság, HISEC'93 konferencia*, Budapest, 1993. december 7—9, pp. 35—47.

[7] Lawrence Chung: „Dealing with Security Requirements During the Development of Information Systems." In Colette Rolland, François Bodart, Corine Cauvet (Eds.), *Advanced Information Systems Engineering, Proc., Fifth International Conf. CAiSE '93*, Paris, France, June 8—11, 1993. Berlin: Springer-Verlag, 1993. pp. 234—251.

[8] Papp Gy.: „Adat, információ, informatika — védelem és biztonság," *KRIMINALEXPO-HISEC'94 konferencia*, Budapest, 1994. június 8—11, pp. 35—49.

[9] W. Caelli, D.Longley, M.Shain: „Information Security Handbook," *Macmillan Publishers Ltd*, 1991. ISBN 1-56159-018-5.
[10] W.Caelli, D.Longley, M.Shain: „Information Security for Managers", *Macmillan Publishers Ltd*, 1989.
[11] G.Morrie: Building A Secure Computer System, Van Nostrad Reinhild, 1988.
[12] CCTA Risk Analysis Management Methode User Guide, Version 2.0, CCTA, 1991.
[13] U.S. Department of Defense, Trusted Computer Systems Evaluation Criteria, DOD 5200.28–STD, Dec. 1985.
[14] Papp Gy.: "Survey of the Computer and Network Security Issues from Evaluation Criteria to Open Systems," *Eighth Austrian-Hungarian Informatics Conference, CON'93 — The Challenge of Networking*, Szombathely, Nov. 17–20, 1993. Proceedings pp. 149–158.
[15] Office for Official Publications of the European Communities, Information Technology Security Evaluation Criteria, Provisional Harmonised Criteria, Version 1.2, June 1991. Luxembourg.
[16] International Federation for Information Processing Technical Committee 11 Annual Security Conference, May, 24–27, Curaçao, 1994.

ON THE SECURITY OF DATA COMMUNICATIONS

GY. PAPP

PRIME MINISTER'S OFFICE H-1055 BUDAPEST, KOSSUTH TÉR 2-4.

The paper deals with the challenges of security issues in the data communications. The communication security is a wider problem than we would think of. It depends not only on the data links, on the communication controlling means, and on the data encryption however it depends on the security objectives of the communication partners and of the whole computer system. I would like to show the aim of the communication protection, and how it is related to other computer system elements. As far as the communication security is concerned there is no 100 percent result, as I demonstrate that, one of the most important things is the managing and supervising of security measures. Unfortunately, a great backlog can be experienced in this field, less attention is paid by not only vendors of computers and their system elements but — in the lack of resources — by companies and organizations maintaining the networks or by suppliers.

Papp György 1979-ben a Budapesti Műszaki Egyetem Villamosmérnöki Karán végzett és a Belügyminisztériumban kezdett dolgozni, majd a Nemzetbiztonsági Hivatalhoz került. Kutató-fejlesztő mérnökként elsősorban mikroprocesszoros vezérlő berendezések fejlesztésével, számítástechnikai rendszerek kidolgozásával foglalkozott. 1986-ban oklevelet szerzett a BME Távadatfeldolgozó Szakmérnöki Szakon. 1981 óta végez intenzív kutató munkát a számítógép-hálózatokba történő illegális beavatkozások felfedésének területén. Fő kutatási témája: a Petri hálók elemzése és védelmi modell megteremtése. 1992 óta a Miniszterelnöki Hivatal Informatikai Koordinációs Irodáján vesz részt a kormányzati informatikai rendszer biztonsági feladatainak irányításában. A Neumann János Számítógéptudományi Társaság keretében, nemzeti képviselője a Nemzetközi Számítógépfeldolgozó Szövetség (IFIP) TC11-es, információvédelmi és adatbiztonsági szakbizottságának.

INFORMÁCIÓS ÉS ADATFORGALMI RENDSZEREK KRIPTOGRÁFIAI VÉDELME

DUDÁS JÓZSEF

KFKI SZÁMÍTÁSTECHNIKAI RT.
1121 BUDAPEST
KONKOLY THEGE MIKLÓS U. 29.–33.

A cikk összegzi a kriptográfia fogalmi rendszerét, majd a kriptográfia eszközkészletét tárgyalja. Kitér az adatfeldolgozó rendszerek ellen irányuló támadásokra és a védelmi rendszerekre. Képet ad a kriptográfia matematikai elveiről, hangsúlyosabban foglalkozik a kevésbé ismert kriptoprotokollokkal. A kriptográfiai szolgáltatások közül a rejtjelzésen kívül a hitelesítés, a partner azonosítás, a digitális aláírás, és időpecsét témaköreivel foglalkozik. A hozzáférésvédelmet a jogosultsági rendszerek és a viszonylatfüggő rejtjelzés vonatkozásaiban tárgyalja.

1. BEVEZETÉS

Az elektronikus adatok (információk) védelmével foglalkozó tudomány — a kriptográfia — fejlődése együtt halad az elektronikus adatfeldolgozás eredményeivel. Az „elektronikus iroda" újabb szolgáltatásai mindig felvetik az adatbiztonság és adatvédelem kérdéseit. Számos példa mutatja, hogy hamis biztonságérzetet, téves biztonságtudatot eredményez a nem kellő átgondolással megtervezett adatvédelmi rendszer. Teljes biztonságot csak a kriptográfiai módszerekkel megvalósított magasszintű adatvédelem nyújt. e

2. A KRIPTOGRÁFIA FOGALMI RENDSZERE

A *kriptográfia* hagyományos értelmezésben adatok, üzenetek rejtjelzésével (kódolás, sifrírozás) foglalkozó tudomány. Napjainkra a kriptográfia témaköre jelentősen bővült és az adattitkosításhoz felhasznált matematikai bázishoz hasonló eszközökkel és módszerekkel a kriptográfia az adatvédelem és adatbiztonság egyéb területein is számos szolgáltatást kínál.

A kriptográfiai szolgáltatások a biztonság, a bizonyosság vagy a hitelesség kérdéskörében általában erősebbek, mint a hagyományos eljárások, de olyan szolgáltatások is vannak, melyek hagyományos eszközökkel nem realizálhatók. Az elektronikusan tárolt vagy továbbított adatok esetében például a digitális aláírás néhány országban már kodifikált eljárás, több országban a kodifikálás előkészítése folyamatban van.

A *rejtjelzés* sajátos matematikai eszközökkel azt biztosítja, hogy a védendő információk — stratégiai fontosságú adatok, pénzügyi, üzleti titkok, dokumentációk vagy a személyiségi jogokat érintő adatok stb. — csak abban a körben legyenek értelmezhetők, (megfejthetők) melyben a kijelölt személyek azokkal jogosultak foglalkozni és a védett információk az illetéktelenek elől elzárva maradjanak. A rejtjelzett adatok illetéktelenek birtokában értéktelen és érthetetlen adathalmazt jelentenek. A rejtjelzés megfejtése éppen a matematikai apparátus erőssége miatt reménytelen vállalkozás, általában nagyon nagy költséggel járó eszközbázist és még párhuzamos feldolgozás esetén is beláthatatlanul hosszú időt igényel.

A rejtjelzés matematikai szerkezete általában két komponensből áll: a *rejtjelző algoritmus* és a rejtjelzéshez felhasznált *rejtjelkulcsok*. Az algoritmus olyan matematikai eljárások sorozata, melyek egy nyílt adatsorból egyértelmű (egyértékű) rejtjelzett adatsort állítanak elő egy adott kulcs vagy kulcskészlet felhasználásával.

A felhasznált kulcsok számossága (a kulcs szabadsági foka) nagyszámú, egymástól jelentősen különböző rejtjelzett változat létrehozását teszi lehetővé. Valamely rejtjelzett állomány megfejtéséhez a rejtjelzéshez felhasznált kulcsok ismerete szükséges. Az adatok különböző kulccsal kialakított rejtjelzése, valamint a kulcsok meghatározott körben való ismertetése számos variációt tesz lehetővé az adatokkal foglalkozók illetékességének behatárolására.

Azt a megoldást, hogy a kulcsok a rejtjelzett adatokkal illetékesen foglalkozók rendelkezésére álljanak a *kulcskialakítási rendszer* biztosítja. Ez azt jelenti, hogy a rejtjelzett állomány megfejtéséhez szükséges kulcsok ismerete vagy a kulcsokat tartalmazó hardver eszközök birtoklása az adatvédelem jellegének megfelelően csak egy jól meghatározott körben biztosított.

Az egymás között kapcsolatot létesítő kriptográfiai egységek, *kriptográfiai hálózat*, központi kulcsellátás alapján kapják meg azokat a kulcsokat, melyekkel az azonos hálózaton belül tetszőleges kriptográfiai kapcsolat fenntartására képesek. A kulcskialakítási rendszerek különböző célú rejtjelzési megoldásokat tesznek lehetővé, sőt egy adott kriptográfiai célhoz legjobban illeszkedő kulcskialakítási mód is rendelhető.

A felhasznált kulcsokat a rejtjelző és megoldó oldalon egyaránt el kell tudni érni. Az a megállapítás, hogy a rejtjelzett adatok megfejtéséhez a rejtjelzéshez felhasznált kulcsok ismerete szükséges fordítva is igaz, a kulcsok ismeretében a rejtjelzett adatok megfejthetők. Természetes a kulcsok védelme, hiszen azok ismeretében az egész rejtjelző rendszer támadható.

Magasszintű adatvédelmet vagy adatbiztonságot, így a felhasznált kriptográfiai eszközök körét a konkrét feladatnak megfelelően, „testreszabottan" kell kialakítani. Az adatvédelem szintjét kockázat elemzéssel kell meghatározni. Fel kell mérni, hogy a védendő adatok mekkora értéket képeznek és azt is figyelembe kell venni, hogy az adatokat milyen hosszú ideig kell védelem alatt tartani. Kommunikációs adatok esetében a védelem csak a kommunikáció időtartamára vonatkozik, míg a tárolt adatok esetében a védelmi idő — az elavulási időtől függően — több év, évtized is lehet.

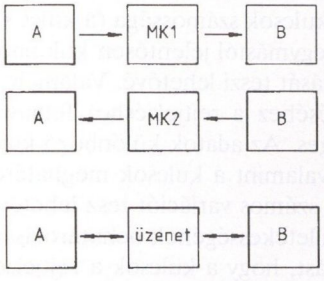
Személyiségi jogokat érintő vagy stratégiailag fontos adatok értékét nem mindig lehet számszerűsíteni — az adatok fontosságát többnyire jogi eszközökkel határozzák meg. A védelmi szintet ennek megfelelően az elérhető legmagasabb fokon kell meghatározni (természetesen az adatstruktúrának és adatforgalomnak megfelelően).

Üzleti vagy pénzügyi titkok védelmi szintjének meghatározásakor támpontot jelent, hogy a rendszer elleni támadás költségei arányban legyenek azzal a haszonnal, melyet az illetéktelenül megszerzett adatok birtoklása és felhasználása jelenthet a támadónak.

3. A KRIPTOGRÁFIA ESZKÖZKÉSZLETE

Maga az adatrejtjelzés egyfajta védekezési eszköz, komoly védelmet jelent, de önmagában meglehetősen „sérülékeny", ha nem párosul egyéb, kiegészítő védelmi elemekkel is.

Egy teljes kriptográfiai rendszer három komponensből épül fel (1. ábra).



1. ábra.

A három komponens együttesen határozza meg a kriptográfiai rendszer erősségét. Lehet bármilyen erős algoritmus valamely rendszerben, ha azt egy jó kulcsképzés nem támogatja, vagy a körülötte kialakított védelmi rendszer gyenge, a teljes kriptográfiai rendszer sérülékennyé, könnyen támadhatóvá válik.

Az *algoritmikus rendszer* a rejtjelzés, hitelesítés, partnerazonosítás és egyéb kriptográfiai szolgáltatások matematikai algoritmusait tartalmazza.

A *kulcsrendszer* lényegesebb elemei:

- *Kulcsmanagement* központi kulcsellátás (a rendszer — hálózat) induló kulcsainak képzése, eljuttatása és betöltése a rendszer elemeibe (állomásaiba), valamint ezek időszakos (féléves, éves) cseréje.
- *Kulcskialakítás* konvenciók összessége, mely biztosítja, hogy a rejtjelző és a megoldó oldalak is összetartozó kulcshalmazzal dolgozzanak. *Szimmetrikus kulcskialakítás* (üzeneti kulcs, cserekulcs, hierarchia kulcs) esetében a rejtjelzéshez és a megoldáshoz használt kulcsok megegyeznek. *Aszimmetrikus kulcskialakítás* (PKS — Public Key System — nyilvános kulcs) a rejtjelző és a megoldó oldalon más kulcsokat használ.
- *Kulcsképzés* a rejtjelzést közvetlenül megelőző folyamat, mely a kulcskialakítási rendszernek megfelelően a rendszertől pillanatnyi kulcsot kér vagy azzal kulcsot fogadtat el.

A *védelmi rendszer* a teljes kriptográfiai rendszer önvédelmét a támadások vagy hibázások elleni felkészítettségét, a kulcselosztás folyamatait stb. jelenti. A védelmi rendszer szoftver, és hardver elemeket éppúgy tartalmaz, mint üzemeltetési vagy rezsimutasítások sorozatát, amelyek a technológia betartásának előírásai.

Az *integrált kriptográfia rendszer* a három komponens együtteséből áll. Az egyes komponensek helyeként egymásba olvadnak, egymással bonyolult összefüggésben vannak, elhatárolásuk gyakran ki sem mutatható. Egy kriptográfiai adatvédelmi eszköz vagy rendszer komponenseiben nem minősíthető, a minősítés csak az integrált védelmi rendszer teljességének áttekintése alapján lehetséges.

Szokásos az adatvédelmi területen a rejtjelzés vagy algoritmus erősségéről beszélni, ami nem egészen egzakt, hiszen nehezen mérhető vagy definiálható fogalom. Az algoritmuselméleti kutatások számos, jobbnál jobb rejtjelző algoritmust dolgoztak ki, a kutatások ma is folynak, de keveset mond az erősség az integrált adatvédelmi környezet meghatározása nélkül.

Bármilyen jó rejtjelző algoritmus is erősen támadható, ha például rosszul tervezett adatvédelmi közegben

- a nyílt és rejtjelzett anyagok együtt is előfordulnak,
- ugyanarról a nyílt anyagról több rejtjelzett változat is együtt van a rendszerben,
- a rejtjelzett anyag és a rejtjelzéshez felhasznált kulcs egy helyen fordul elő.

A *kriptográfiai szivárgási pontok*, melyek nemcsak a rendszerből, hanem kezelési hibákból vagy emberi mulasztásokból is adódhatnak a „legerősebb" matematikai rendszereket is tönkretehetik.

Az a matematikai apparátus, melyet a korszerű kriptográfia használ, a rejtjelzésnél lényegesen tágabb területet fog át és komplex adatvédelmi rendszerek kialakítását eredményezi. Az integrált adatvédelmi környezet az alkalmazott matematikai eszközök mellett technológiai előírásokat, rezsim utasításokat, funkció meghatározásokat, jogosultság kijelöléseket, ellenőrzési pontokat és szinteket, valamint több egyéb eseti előírást is jelent. Ezek együttesen határozzák meg és teszik egyenszilárdságúvá a kriptográfiai védelmi rendszert.

A kriptográfiai rendszerek tervezésekor a kockázatelemzésben nemcsak a védendő értékkel kell foglalkozni, hanem figyelembe kell venni a rendszer ellen feltételezhető támadásokat, melyek külső vagy belső eredetűek lehetnek, gyakori azonban a kombinált formában, konspiratív módon jelentkező támadás is.

A *külső támadások* ellen kriptográfiai eszközökkel lehet védekezni, sőt azok bekövetkezését meg is lehet akadályozni. Ezt a védelmet a hatékony rejtjelzés és a jól kialakított, kellőképpen védett kulcsrendszer biztosítja.

A *belső támadások* elvileg sem akadályozhatók meg. A támadás vagy az arra irányuló kísérlet minél előbbi felfedezésére van csak lehetőség annak érdekében, hogy intézkedéseket lehessen tenni a támadás megismétlésének megakadályozására (pl. a teljes kulcsrendszer azonnali cseréjével). A támadás felismerhetőségét valósítják meg a kriptográfiai naplózó rendszerek.

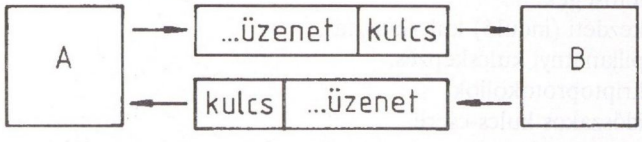
Egy jól felépített kriptográfiai rendszer valamennyi — üzemeltetéssel kapcsolatos — eseményről naplót vezet. A napló nem törölhető, tartalma nem manipulálható, csak az arra felhatalmazott kezelő számára érhető el. A naplóból kiolvashatók az üzemeltetés normális folyamatai, de a

rendszer elleni támadások is felderíthetők.

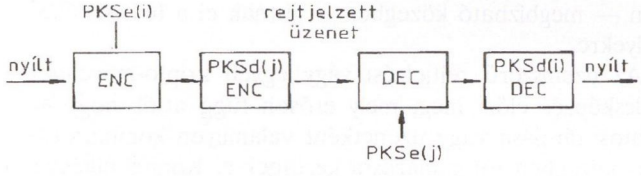
A tárolt adatok — dokumentációk, levelezések, adatbázisok stb. — esetében az illetéktelen hozzáférésen kívül az adatok meghamisítása, kivonása, idegen adatok bevitele jelenti a fő veszélyforrásokat. Az esetek többségében bebizonyosodott, hogy az ún. hozzáférés védelem nem nyújt kellő biztonságot, és olyan kriptográfiai módszereket is alkalmazni kell, mint a tárolt adatok hierarchikus rejtjelzése vagy a hitelesítés, melyekkel az adatállomány manipulálhatatlansága biztosítható vagy azok sértetlensége ellenőrizhető.

A telekommunikációs adatforgalmi közegben maga az átviteli csatorna jelent védelmi gondot. Két jellegzetes támadási forma a lehallgatás és a megszemélyesítés.

A *lehallgatás* szituációban a támadó illetéktelenül rákapcsolódik az átviteli vonalra, az ott folyó adat- és kulcsforgalmat figyeli. Az üzenetek gyűjtésével, különleges szituációk észlelésével olyan információkat igyekszik felderíteni, melyek kihasználásával az egész kripto-rendszer ellen támadhat (2. ábra).



2. ábra.



3. ábra

A *megszemélyesítés* nagyobb technikai apparátust igényel. Többnyire a megfigyelt rejtjelzéshez felhasznált szoftver és hardver elemek birtoklására van szükség, a rendszert önmagával vagy ahhoz nagyon hasonló eszközbázissal támadják. A támadó beépül a kommunikációs összeköttetésbe, az üzeneteket elnyeli, és az ellenállomások helyett mindkét irányban válaszol (3. ábra).

A támadás különös veszélyei:

- a támadó az egymással kommunikáló állomásokat csak az üzenetek sorozatos megismétlésére kényszeríti és ugyanarról az üzenetről esetleg több különbözően rejtjelzett variációt szerez meg,
- a támadó valamelyik állomásról általa ismert tartalmú választ kényszerít ki és ezzel megszerzi a nyílt válasz változatát.

A támadásokkal kapcsolatban elmondható, mint azt az említett példák is szemléltetik, hogy nagyobb az esély a rendszer gyenge pontjainak, *kriptográfiai szivárgásainak,* kihasználása a rendszer felderítésére vagy feltörése érdekében, mint egy bonyolult rejtjelző algoritmussal rejtjelzett állomány faktorizációs megfejtésére.

Az olyan hálózatokban, melyek kevert (rejtjeles és nyílt) adatokkal is kommunikálnak, a kriptográfiai szivárgási pontok kellő eséllyel kiküszöbölhetők, ha rendszerbe a védendő adatok már a keletkezésükkor rejtjelzetten kerülnek be, és a tárolás, valamint a kommunikációs továbbítás is ebben a formában történik.

Hasonló alapelvként állapítható meg az is, hogy a védelmi rendszerek kialakítása akkor jó, hogy egy esetleges támadás folyamatában — ha már valamilyen mélységig eljutott a támadó — a további megismeréshez mindig újabb (eddig még nem használt) eszközök bevetése is szükséges legyen.

A védelmi rendszer stratégiai alapelve rávilágít a kriptográfiai rendszerek realizálási problémájára is. Igazán erős védelmi rendszerekben kriptográfiai eszköz — nem is csekély mértékben — hardver erőforrást is követel. A csak szoftver úton megvalósított kriptográfiai rendszerek védelmi képessége általában gyenge, támadásukhoz maga az eszköz is elég, melyben működnek.

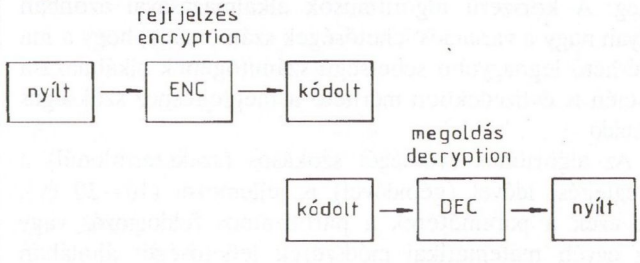
A jól kialakított kriptográfiai rendszerekben a védelem nemcsak a külső vagy belső támadások megakadályozására, vagy az ellenük történő felkészülésre vonatkozik, hanem biztosítékot ad a felhasználónak arról is, hogy az általa használt eszközbázis üzemeltetése független és támadhatatlan a tervezőtől, gyártótól, forgalmazótól, szerviztől, hasonló eszközt birtokló további felhasználóktól, sőt a saját vagy idegen kulcskészítő központtól is.

4. A KRIPTOGRÁFIA MATEMATIKAI APPARÁTUSA ÉS ELVEI

4.1. Algoritmus

A rejtjelző algoritmusok alatt olyan matematikai apparátust kell érteni, mely egy tetszőleges, „nyílt" adathalmazból úgy állít elő egy transzformált, „kódolt" adathalmazt, hogy abból az eredeti nyílt adathalmaz visszanyerhető — visszafejthető legyen.

A rejtjelzés ugyanazt a nyílt adatsort mindig ugyanabba a rejtjelzett adatsorba transzformálja, ha a felhasznált kulcs (kulcskészlet) is azonos volt. A kulcs tartalmának megváltozása a rejtjelzett adatsor tartalmát is megváltoztatja. Az algoritmusok feladata az, hogy a kulcs egyetlen bitjének megváltozása a teljes rejtjelzett üzenetet megváltozását vonja maga után. Az erős algoritmusok általában azt is biztosítják, hogy két — egymástól egyetlen bitben — különböző kulcs felhasználásával végrehajtott rejtjelzés hatására, ugyanarról a nyílt adatsorról két olyan rejtjelzett változat készül, melyekben átlagosan a bitek fele különbözik. A bitek különbözősége egyenletes matematikai eloszlású és független attól, hogy a kulcs melyik bitje változott meg.



4. ábra.

A rejtjelző algoritmusok követelmény rendszere a kriptográfia néhány ezer évre tehető történeti fejlődése során

többé kevésbé tisztázódott. Kialakultak azok a matematikai elvek és módszerek, melyek alapján közel azonos kriptográfiai erősségű algoritmusok készítése ma már „rutin feladatnak" számít.

Elmondható, hogy alapkövetelmény az, hogy a rejtjelzés változtassa meg az adathalmaz statisztikai szerkezetét — a rejtjelzett anyag gyakorlatilag véletlen statisztikai szerkezetet mutasson.

A különböző algoritmikus üzemmódok az átviteli csatorna jellegzetességeihez is igazodnak. A rejtjelzett anyag egy bitjének megváltozása (hibabehatás) az egész üzenetet is tönkreteheti — lavina hatás —, vagy csak az üzenet meghatározott szakaszára (néhány Byte) terjed ki.

Az algoritmus a kriptográfiai védelem alapvető eszköze, de önmagában kevésnek bizonyul. A teljes kriptográfiai rendszert úgy kell kialakítani, hogy az algoritmus feltételezett megszerzése („zsákmányolása") esetén se kerüljenek veszélybe a rejtjelzett adatok — csak az algoritmus ismerete kevés legyen a sikeres megfejtéshez.

Jellemző példa erre a *DES* (Data Encryption Standard), mely a 70-es évek elején az Egyesült Államokban szabványosított rejtjelző rendszer lett. Az algoritmus teljesen publikus, korrekt forrásnyelvi leírása számos cikkben úgy jelent meg különböző programozási nyelveken, hogy azt egy gyakorlott programozó néhány órai munkával realizálni is tudja. A DES mint rejtjelző rendszer azonban kellő védelmet jelent a rejtjelzett adatok biztonságára nem egy esetben még minősített titkok vagy üzleti (bank) titkok esetében is.

Hasonló a helyzet a nyilvános kulcsú rendszerekben alkalmazott *RSA* algoritmussal is. Az algoritmus (meghökkentően egyszerű) publikus, mindenki számára elérhető. Az RSA algoritmussal kialakított rejtjelzés — akár a rejtjelzés, akár a hitelesítés vagy partnerazonosítás tekintetében — a ma ismert egyik legerősebb rendszer.

4.2. Kulcsmanagement

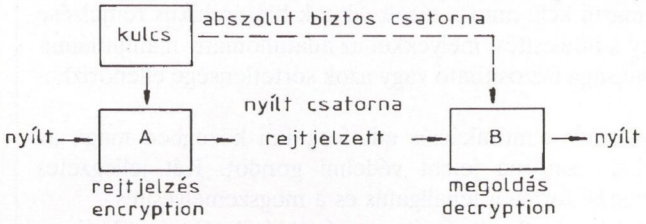
A mai korszerűnek tekinthető kriptográfiai rendszerekben az algoritmus szervesen összeépül egy kulcskészlettel, melynek ismerte nélkül a kódolt üzenet megfejtése — a rejtjelzés feltörése — reménytelen vállalkozás.

A kulcskészlet vagy annak egyes elemei úgy épülnek be a rejtjelzett anyagba, hogy a kulcsok egyetlen bitjének megváltoztatása is a teljes rejtjelzett üzenet megváltozását vonja maga után.

A kulcs vagy kulcsok ismerete nélkül a rejtjelzett üzenet csak faktorizáció (próbálkozások sorozata) útján oldható meg. A korszerű algoritmusok alkalmazásával azonban olyan nagy a variációs lehetőségek számossága, hogy a ma elérhető legnagyobb sebességű számítógépek alkalmazása esetén is évtizedekben mérhető a megfejtéshez szükséges gépidő.

Az algoritmus erősségét szokásos (szakszerűtlenül) a megfejtési idővel (gépidővel) is jellemezni (10–20 év), de ezek a paraméterek a párhuzamos feldolgozás vagy az egyéb matematikai módszerek lehetőségét általában figyelmen kívül hagyják — a megfejtési idő gyakorlatilag nem jelent semmit.

Elvileg létezik feltörhetetlen rejtjelzés (1937 Vigener), mely azon alapszik, hogy a rejtjelzéshez legalább annyi fizikai véletlen Byte-ot kell kulcskét felhasználni, mint amennyiből az üzenet áll. A gondot lényegében az jelenti, hogy a kulcselemeket a térben és időben máshol működő megoldóhoz is el kell juttatni. A problémára Shannon paradoxona mutat rá: a rejtjelzett üzenet tetszőleges nyílt csatornán átküldve is támadhatatlan, ha a kulcsok forgalmazása egy „abszolút biztos" csatornán történik (5. ábra).



5. ábra.

Az abszolút biztos csatorna minél jobb közelítése a kulcskialakítási rendszerek feladata. A rendelkezésre álló lehetőségek:

- kezdeti (induló) kulcskiosztás,
- pillanatnyi kulcsképzés,
- kriptoprotokollok,
- időszakos kulcs-csere.

A *kezdeti kulcskiosztás* valamilyen központi helyen KMC (Key Management Center) kezdődik, és az egy rendszerhez összehangoltan képzett kulcsok valóban védett csatornán — megbízható közegben — jutnak el a felhasználási helyekre.

Az üzemszerű rejtjelzést vagy egyéb kripto-műveletet kulcsképzés előzi meg, mely erősen függ attól, hogy az adatok tárolása vagy üzenetként valamilyen kommunikációs közegben forgalmazásra kerülnek-e. Kommunikációs közegben az egymással forgalmazó állomások egyeztetett kulcsképzését a kriptoprotokollok valósítják meg.

Bizonyos értelemben az abszolút biztos csatorna közelítését jelenti az időszakonként elvégzendő kulcs-csere is. A kezdeti (induló) kulcsokat leváltják (frissítik). A cserélendő kulcsokat szintén központilag a KMC-ben generálják.

Az abszolút biztos csatorna jelentős absztrakció. Napjainkban egyre jobb megközelítések vagy helyettesítések születnek, de ma még igaznak bizonyul az a nézet, hogy az abszolút biztos csatorna — csaknem valamennyi környezetben — a matematikai módszereket kiegészítő rezsim utasítások sorozatával biztosítható. A technológiai előírások sajnálatos módon a technológiai fegyelem betartásának vagy az emberi tévesztésnek, esetleg kísértésnek (konspirációs támadás) függvényei is lehetnek.

Az emberi tényezők minimálisra szorítása érdekében általában elterjedtek az osztott védelmi rendszerek, melyekben az abszolút biztos csatornát úgy valósítják meg, hogy az a kezelő személyzettől a rendszerhez tartozó fizikai és logikai eszközök együttes birtoklását követelik meg és a rendszerrel kapcsolatos valamennyi tevékenység dokumentált formában követhető.

Az osztott védelmi rendszer a kulcsrendszer kialakításának — kulcsmanagement — is rendező alapelve. A különböző típusú és funkciójú kulcsok időben és fizikai helyszínben máshol keletkeznek, és a teljes rendszer működtetése vagy kihasználása csak azok együttes birtoklásával lehetséges.

4.3. Standard kulcsok (hálózat azonosítás)

A rejtjelző rendszer legmagasabb egysége maga a kriptográfiai hálózat. A hálózat sok (néhány száz) munkaállomást (végpontot) fog össze úgy, hogy az egyes végpontok egymás között tetszőleges kombinációban rejtjelzetten kommunikáció-képesek úgy, hogy a többi állomástól és főleg más hálózatoktól védettek.

A hálózatot a központi kulcsellátó rendszer látja el az alapvető (standard) kulcsokkal és módot nyújt arra is, hogy ezek a kulcsok meghatározott időszakonként cserélhetők legyenek.

A standard kulcsok feladata, hogy egy hálózaton belül az egyes végpontok tetszőleges viszonylatban úgy értsék meg egymást, hogy a hálózaton belül körlevél (broadcast) üzenet fogadására is képesek legyenek, pontosan olyan kriptográfiai szinten, mellyel egyébként normál forgalmazásban egymás között pont—pont közötti kapcsolatban is forgalmaznak.

4.4. Irányfüggő kulcsok (végpont azonosítás)

A kriptográfiai hálózat valamennyi állomása (végpont) saját identifikációval is rendelkezik, olyan speciális egyedi kulcselemet tartalmaz, melyek alapján más állomásról (végpontról) hívható, illetve valamennyi más állomással kizárólagos kapcsolat felvételére képes. A forgalmazást (üzenet váltást) csak a kiválasztott partner érti meg úgy, hogy az üzenet a hálózat többi végpontja számára sem érthető.

4.5. Kulcsrejtjelző kulcs (KEK — Key Encryption Key)

Az üzenet rejtjelzéséhez felhasznált tényleges kulcs természetesen nem jelenhet meg az átviteli csatornán. A kulcs rejtjelzése (legalább olyan matematikai erősségű, mint maga az üzenet rejtjelzése) általában a teljes hálózatra érvényes kulcsrejtjelző kulcs (KEK — Key Encryption Key) felhasználásával lehetséges.

4.6. Adatrejtjelző kulcs (DEK — Data Encryption Key)

Mint az korábban is említésre került az önmagában használt algoritmikus védelem kevésnek bizonyul. A korszerűnek nevezhető algoritmusok — és ez az elv meglehetősen hosszú múlttal rendelkezik — mindig valamilyen kulcselem felhasználásával operálnak. Az adatrejtjelző kulcs mérete (szabadsági foka) determinálja azokat a lehetőségeket, melyek az algoritmussal együtt a rejtjelzés minőségét (erősségét) meghatározzák.

Az adat rejtjelző kulcs mérete csak az algoritmussal együtt jelenthet értékelhető mérőszámot. A reklám jellegű méretadatok indifferens információkat szolgáltatnak, hiszen ahogy azt az irodalmi adatok is mutatják nagy szabadságfokú kulcsokkal is produkáltak feltörhető algoritmusokat.

Az amerikai szabványú DES 56 bit (7 Byte) kulcs felhasználásával operál, a hasonló elven működő algoritmusok általában 10—16 Byte méretű kulcsokkal dolgoznak. A nyilvános kulcsú rejtjelző rendszerekben a minimális kulcsmérete 80—120 karakter (Byte).

A korszerű rejtjelző rendszerek az adatrejtjelzésre szolgáló kulcsot (DEK) valódi fizikai véletlen számokból, esetleg pszeudó véletlen számsorozatból képezik. A kulcsrejtjelző kulcs felhasználásával transzformált üzeneti kulcs az átviteli csatornára is kikerülhet, a rejtjelzés biztonságát nem veszélyezteti.

A rejtjelző rendszerekben az adatrejtjelzésre szolgáló kulcsot — ami végül is egy fizikai véletlen számsorozat (DEK) — módosítják (modulálják) a hálózat-, viszonylat- vagy hierarchia-függés, esetleg más rugalmasan kialakított paraméterek függvényében.

4.7. Pillanatnyi kulcsok (MK — Message Key)

A konkrét rejtjelzés — üzenetküldés vagy üzenetváltás — történhet a hálózatra vagy a végpontokra jellemző kulcselemek felhasználásával is, de ha erre lehetőség van mindig konkrét — csak arra az egy üzenetre érvényes kulccsal történik.

A pillanatnyi (üzeneti) kulcsok a kriptográfiai erősséget növelik és jelentős védelmet nyújtanak az üzenetek gyűjtésével manipuláló támadások ellen.

4.8. Kriptoprotokoll

Azokat a módszereket, eljárásokat és eszközöket, melyek azt biztosítják, hogy a rejtjelzési oldalon alkalmazott kulcsok a megfejtő oldalon is rendelkezésre álljanak összefoglaló néven a kriptoprotokoll fogalma fejezi ki. A kriptoprotokoll szervesen összeépül az egyéb számítógépes erőforrásokkal és főleg telekommunikációs környezetben azoktól szinte elválaszthatatlan.

Tágabb értelemben a központi kulcs generálás (KMC — Key Management Center), valamint a kripto-rendszerek installálása (kezdeti kulcsokkal való feltöltése) is a kriptoprotokoll fogalomkörébe tartozik ugyanúgy, mint a standard kulcsok időszakos (igénytől, támadástól vagy forgalomtól függő féléves, éves) teljes vagy részleges cseréje.

A kriptoprotokoll a Shannon által definiált abszolút biztos csatornát valósítja meg, pontosabban azt valamilyen megoldási móddal, technológiai folyamattal vagy rezsimutasítások sorozatával közelíti.

Az abszolút biztos csatorna elvontsága ellenére is meglehetősen definit fogalom és konkrét formában jelentkezik a különböző kommunikációs közegekben. A tárolt adatok (levelező rendszerek, archiválás, adatbázisok stb.) más támogatást, kulcselérési és védelmi fokozatot kívánnak a kulcsátjuttatás miatt a kriptoprotokolltól, mint ahogy azok az esetek többségében on-line kapcsolattal felépülő kommunikációs környezetben jelentkeznek.

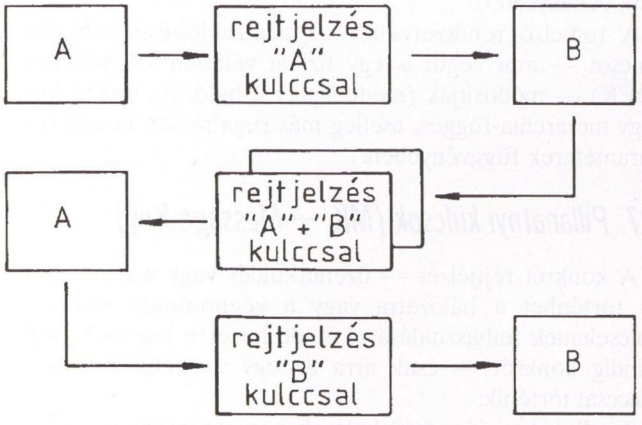
A különböző környezetek sokszor egymásnak ellentmondó feltételek egyidejű teljesülését is megkövetelik. Egy optimális (minden célnak megfelelő) kriptoprotokoll definiálása azzal is bonyolódik, hogy a kriptográfiailag zárt rendszerek nyílt számítógépes környezetben (Open System) működnek és a kriptoprotokolloknak a rendszer védelme mellett azok nyíltságát is biztosítani kell.

A kriptoprotokoll feladata végül is a Shannon-féle paradoxon feloldása. Az abszolút biztos csatorna matematikai

modellezése több, a gyakorlatban is használható megoldást is eredményez.

4.9. Háromutas kulcsforgalom

Ennek a gyakorlatban nehezen realizálható megoldásnak, inkább csak elvi jelentősége van, ami a probléma lényegére mutat (6. ábra).



6. ábra.

1. "A" saját kulcsaival rejtjelezve üzenetet küld "B"-nek.
2. "B" az üzenet megfejtésére sem tesz kísérletet, hanem azt saját kulcsaival ismét rejtjelzi és így küldi vissza "A"-nak.
3. "A" a saját kulcsaival megfejti az üzenetet ("B" rejtjelzése miatt ez számára már érthetetlen) és a már csak "B"-vel rejtjelzett üzenetet küldi vissza "B"-nek, aki ezt saját kulcsaival képes megfejteni.

Az eljárás egyszerű matematikai módszerrel modellezi a Shannon-féle abszolút biztos csatornát.

Megjegyzés: a három irányú kulcsforgalom csak olyan rejtjelző eljárásokat alkalmazhat, melyben az "A" és "B" szerinti rejtjelzés felcserélhető (kommutatív). Az eljárás a megszemélyesíthető támadásra érzékeny.

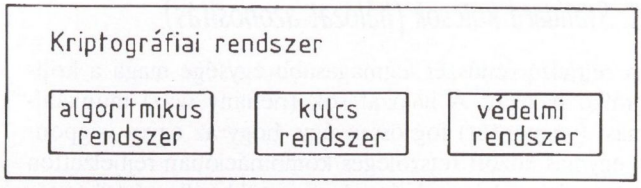
4.10. Kétirányú kulcsforgalom (cserekulcs)

Napjainkban is használt, nagy biztonságot jelentő (nehezen támadható) megoldás, mely kizárólag a kulcsforgalomra koncentrál. A rendszer feltételezi, hogy a partnerállomások rendelkeznek azonosan installált kulcsrejtjelző kulccsal (KEK) vagy azzal egyenértékű közös információval, mellyel a küldött, illetve kapott kulcsokat egybehangzóan tudják rejtjelezni és megoldani (7. ábra).

1. A tényleges (rejtjelzett) üzenet előtt "A" (rejtjelzett) kulcsot (MK1) küld "B"-nek, egyúttal felszólítja "B"-t válaszkulcs küldésére.
2. "B" megfejti a kapott (MK1) kulcsot és az installált konvenciónak megfelelően (MK2) rejtjelzett válaszkulcsot küld vissza "A"-nak.

A kulcscsere lezajlódott, mindkét fél rendelkezik olyan közös és csak számukra ismert információval, melynek alapján a rejtjeles forgalom elkezdődhet.

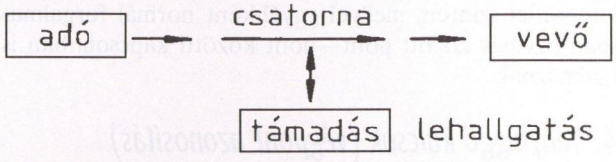
Megjegyzés: a kriptoprotokoll kellően erős (ellenőrző összeggel és irányfordítással is rendelkező) kommunikációs protokoll támogatását feltételezi.



7. ábra

4.11. Egyirányú kulcsforgalom (üzeneti kulcs)

Napjainkban elterjedten használt kulcsforgalom, mely egyszerűsége miatt könnyen alkalmazható. Az üzeneti kulcsos rejtjelzést a használatos telekommunikációs protokollok zöme támogatja (8. ábra).



8. ábra.

Az egymással kapcsolatban levő állomások a rejtjelzett üzenetek küldése előtt az üzenet megfejtéséhez tartozó (installált konvencióknak megfelelően) rejtjelzett kulcsot is átküldik a partnerállomásnak, melynek alapján (és a hasonlóan installált kulcselemek birtokában) azok az üzenetet megértik.

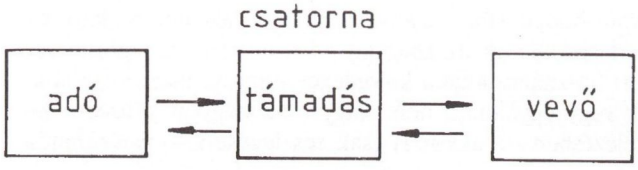
4.12. Nyilvános kulcsú rendszerek (PKS)

A 80-as évek közepétől egyre jobban elterjedő nyilvános kulcsú rendszerek a Shannon-féle paradoxon érdekes matematikai megkerülését adják.

Minden állomás az installációs konvenciónak megfelelően egy titkos kulccsal (PKSd) és annak nyilvános párjával (PKSe) rendelkezik. A hívható állomások nyilvános kulccsal bárki számára elérhetőek.

A nyilvános kulcsra alapozó rejtjelző algoritmusok automatikusan biztosítják a partnerazonosítást.

- Ha az üzenet rejtjelzése a nyilvános kulccsal (PKSe) történik, a feladó biztos lehet abban, hogy az üzenetet csak az az állomás képes megfejteni, amelyik a kulcs titkos párjával (PKSd) rendelkezik (címzett azonosítás).
- Ha az üzenet rejtjelzése az állomás titkos kulcsával történik, azt mindenki megfejtheti, aki a kulcs nyilvános párját ismeri. Az így megfejtett üzenet abszolút bizonyosságot ad arról, hogy azt ki küldte (feladó azonosítás). Ezt az elvet használja a digitális aláírás.
- A nyilvános kulcsú algoritmusok zöme a többszintű rejtjelzést is megengedi. Kialakítható olyan kapcsolat is, mely a címzett nyilvános kulcsával és a küldő titkos kulcsával is rejtjelzi az üzenetet. A fogadó oldalon a fogadó saját titkos kulcsával és a küldő nyilvános kulcsával történik a megfejtés. Az így létrehozott rejtjelzés elektronikus partnerazonosítást valósít meg (9. ábra).



9. ábra.

4.13. Tárolt adatok kulcsrendszerei

Tárolt adatok esetén a rejtjelző és megoldó folyamatok időben elválnak egymástól. A kommunikációban használt pillanatnyi kulcsok jelentősége az „on line" kapcsolat hiánya miatt csökken, viszont biztosítani kell azt, hogy a tárolt adatok különböző kulcsokkal készített rejtjelzett változatai ne forduljanak elő. Egy adatbázis rekord vagy egy szövegállomány mindig ugyanazzal a rejtjelzéssel kerüljön forgalomba — az elérés helyétől és idejétől függetlenül.

A Shannon-féle abszolút biztos csatorna közelítésére a központi kulcselosztás és a *jogosultság* kérdései jutnak nagyobb szerephez. A központi kulcselosztásban különböző (véletlen eredetű) hozzáférési kulcsokat és szinteket kell kialakítani *hierarchikus kulcs*. Valamilyen hozzáférési szinten rejtjelzett üzenetet a felhasználóknak csak azon köre képes „megérteni", aki a szint elolvasására (megfejtésére) jogosult.

A hierarchikus kulcsok alkalmazása erősen kétségbe vonja a hagyományos hozzáférési rendszerek jelentőségét. A hierarchia szinttel rejtjelzett állományokhoz bárki hozzáférhet, hiszen csak az értheti meg, aki annak elérésére jogosult.

A szállítható adathordozón (pl. floppy) történő tárolás esetén az egyirányú kulcs vagy a nyilvános kulcs is alkalmazásra kerülhet, de a tárolt adatok védelmére a hierarchia kulcsok vagy központilag előállított *fix kulcsok* esetleg *input kulcsok* alkalmazása terjedt el általánosan. Az adathordozók rejtjelzésére főleg a gyors elérésű diszkek esetében a nagysebességű algoritmusok használata szokásos.

5. KRIPTOGRÁFIAI SZOLGÁLTATÁSOK

Az utóbbi időszakban egyre jobban előtérbe kerülnek a rejtjelzésen túlmenő kriptográfiai szolgáltatások is. Egzakt matematikai módszerek léteznek az adatvédelem különböző területein, melyek a hagyományos „bizonylati rendszerek" megbízhatóságát felülmúlják, bizonyos esetekben teljesen új kriptográfiai szolgáltatásokat is nyújtanak, melyeknek a hagyományos eljárásokban nincs megfelelő megoldásuk.

5.1. Hitelesítés (autentikáció)

A tárolt adatok vagy kommunikációs üzenetek tartalmára vonatkozó védelmi eljárás. Az adatokat védi hamisítás, manipulálás, üzenet kivonás vagy járulékos üzenet beiktatás ellen. A hitelesítés a hagyományos kontroll-szummás ellenőrzés helyett lényegesen magasabb matematikai biztosítékot ad arra, hogy az adathalmaz vagy üzenet valóban hiteles és a keletkezése óta nem változott. Az eljárás olyan ellenőrző összeget (4—8 Byte-os karaktersorozat) generál, mely csak az adott kriptográfiai rendszerben készíthető el és csak ott ellenőrizhető. Készítéshez általában felhasználják azokat a kulcselemeket, melyeket a rejtjelző algoritmusok is használnak.

5.2. Partner azonosítás (identifikáció)

Az eljárás főleg kommunikációs környezetben vagy elektronikus levelező rendszerekben az üzenet tartalmától függetlenül a küldő vagy a fogadó oldalnak (mindkettőnek) matematikai biztosítékot ad arról, hogy az üzenetet a címzett és csak a címzett értheti meg, vagy ha az üzenetet megértette, teljes bizonyosságot nyer arról, hogy az üzenetet ki küldte. Az eljárásban gyakori a viszonylatfüggő kulcskialakítás, melyben a kölcsönös azonosítás után következik az üzenetváltás.

5.3. Digitális aláírás, időpecsét

Az eljárás az autentikálás és az identifikálás kombinált alkalmazása, mely az üzenet hitelességén és forrásán kívül a hitelesítést végző személy azonosítását is lehetővé teszi. A digitális aláírás általában önálló üzenetben vagy file-ban (esetenként „záradékban") tartalmazza az aláírandó anyag megnevezését, hitelesítő kódsorozatát, az aláírás idejét, az aláíró nevét, valamint a záradék rész hitelesítő kódját is. Az aláírás file-ba szerkesztett időpont az üzenetek megismételése ellen véd a digitális aláírásban. Csak az azonosítható időponthoz tartozó üzenetet tekinti hitelesnek.

A digitális aláírásban alkalmazott rejtjelzés abban különleges, hogy az aláírás megfejtése csak az aláírót egyértelműen azonosító kulcs felhasználásával lehetséges. A rejtjelzéshez használt kulcs titkos, a megfejtéshez felhasznált kulcs publikus is lehet. A digitális aláírás az aszimmetrikus kulcs alkalmazásával a nyilvános kulcsú rendszerekben terjedt el.

A megfejtett aláírás file-ból kibontott hitelesítő kód alapján az aláíró személy és az anyag hitelessége, a készítés időpontja is ellenőrizhető.

5.4. Jogosultság hozzáférésvédelem

A jelszavas hozzáférésvédelem — annak ellenére, hogy alkalmazása napjainkban nagyon elterjedt — számítógépes környezetben kevés védelmet nyújt és könnyen támadható. A leggyakrabbi számítógépes támadások általában a hozzáférésvédelem feltörésére irányulnak. A legismertebb módszerek a klaviatúra csapda, mely memória rezidens programként, beépül a számítógépbe és file-ba gyűjti a leütött billentyűkódokat a leütések időpontját vagy a különböző „supervizor programok" (nagyrészük költségmentesen jogtiszta), melyek teljes jogkörű hozzáférést biztosítanak a hálózati rendszerekben.

A matematikai apparátuson alapuló jogosultságvédelem — mely jól helyettesíti password-ös hozzáférésvédelmet — a kriptográfia egyéb területein is alkalmazott hierarchia szintre alapozott rejtjelzéssel oldja meg az illetéktelen hozzáférés elleni védelmet. Az adathoz — rejtjeles formában — minden felhasználó hozzáférhet, de nem érti meg, ha a szintre nincs jogosultsága. Az eljárás erősíthető, ha egy rendszerben az adatokat ott rejtjelzik (célirányosan), ahol azok keletkeznek és csak ott fejtik vissza őket, ahol közvetlen felhasználásra kerülnek.

6. AZ ADATVÉDELEM SZINTJEI

Az adatvédelemben alkalmazott kriptográfiai szolgáltatások alapján szokásos alacsony, illetve magasszintű adatvédelmi fokozatokról is beszélni. A különböző adatvédelmi szintek nem az adatvédelmek erősségét minősítik, hanem arra vonatkoznak, hogy a rendszerek milyen mértékben használják a kriptográfia matematikai apparátusát és a védelmet technológiai előírásokkal (rezsimutasításokkal) mennyire kell megerősíteni. A magasszintű adatvédelmek kevésbé érzékenyek az emberi mulasztásokra vagy tévedésekre, és a rendszer elleni támadások lehetőségeit is csökkentik vagy nagymértékben nehezítik.

Alacsony szintű adatvédelemnek tekinthető a

- hozzáférés védelem,
- szoftver védelem,
- céleszközös (fekete doboz) védelem.

A hozzáférés védelem legalacsonyabb szintje a passwordös (jelszavas) védelem. A hardver kulcsos védelem (soros vagy párhuzamos porton alkalmazott extra hardver) inkább a szoftver készítőit (szerzői jog) védi, mint a felhasználót. A smart-, OTP (One Time Programing) kártyás védelem, mint az alacsony szintű adatvédelem egyik legerősebb eszköze arra utal, hogy az igazán erős adatvédelmek extra hardver megoldások nélkül nem realizálhatók.

A szoftver védelem, jóllehet már „igazi" kriptográfiai eszköz — általában rejtjelzés — figyelmen kívül hagyja azt a tényt, hogy egy jól védett rendszer támadásához nagyobb eszközbázist kell felhasználni, mint amellyel annak védelme realizálódott. (A szoftver rejtjelzés feltöréséhez elegendő az az eszköz — az a gép —, mely a rejtjelzést készítette.)

A céleszközös (crypto-modem, crypto-fax, crypto-X25, crypto-bridge stb. — általában *fekete doboz*) rejtjelzések azért sorolhatók az alacsony védelmi szint kategóriájába, mert használatukkal a különleges kriptográfiai szolgáltatások vagy egyáltalán nem, vagy csak nagyon költséges kivitelezésben — akkor is csak részlegesen — valósíthatók meg.

A magasszintű adatvédelem (*kripto-védelem*) kizárólag hardver eszközökben realizálható és olyan lehetőségeket kínál, melyek a kriptográfia hagyományos értelmezését (rejtjelzés, kódolás) jelentős mértékben kiterjesztik.

A magasszintű adatvédelem eszközei:

- rejtjelzés,
- autentikáció (hitelesítés),
- identifikáció (partner azonosítás),
- digitális aláírás,
- időpecsét,
- jogosultság,
- eseménynapló.

A magasszintű védelem lényeges eleme az eseménynapló. A napló a jogosultsági rendszerhez hasonlóan védve és megmásíthatatlanul szintén önálló hardver eszközben készül. Automatikusan rögzíti a rendszer működésében lényegesnek tartott „eseményeket". A napló a nem megakadályozható visszaélések felderítésére és szankcionálására nyújt lehetőséget.

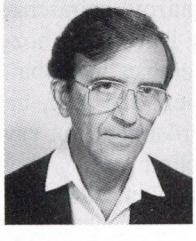
A naplóban olyan tetszőleges felhasználói bejegyzéseket is el lehet rejteni, melyek a rendszer működése szempontjából lényegesek, de védelmük az egyéb adatoknál fontosabb vagy a felhasználói körben nem publikus. A hardver védelmű napló kezelése (írása, olvasása) jogosultsághoz kötött.

CRYPTOGRAPHICAL PROTECTION OF INFORMATION PROCESSING AND DATA COMMUNICATION SYSTEMS

J. DUDÁS

KFKI, COMPUTER SYSTEMS CORP.
H-1121 BUDAPEST, KONKOLY THEGE MIKLÓS U. 29.–33.

The paper summarizes the basic concepts of cryptography and discusses its resources. Different types of threats against data processing systems are investigated and the protection systems are also discussed. A survey of mathematical principles of cryptography is provided and the the less-known crypto-protocol is also described. In addition to encryption the paper discusses other cryptographical techniques: authentication, partner identification, digital signature and time-seal. Finally the access-protection is described from the aspects of permission structures and relation-dependent encryption.



Dudás József a Budapesti Műszaki Egyetem Híradástechnika Szakán 1965-ben szerzett villamosmérnöki diplomát. Több mint 10 évig a Magyar Rádióban aktív hangmérnökként dolgozott. 1976-ban a Budapesti Műszaki Egyetemen digitális elektronikai szakmérnöki diplomát szerzett és a Műszeripari Kutató Intézetben speciális elektronikai berendezések hardver és szoftver tervezését végezte. 1981-ben a Távközlési Kutató Intézetben került kapcsolatba a kriptográfiával. Digitális jelfeldolgozással is foglalkozik, melyből 1984-ben a „Momentán Fourier Transzformáció" című disszertációval doktori fokozatot szerzett. 1989 óta a KFKI Számítástechnikai Csoportjához tartozó ITEA Kft-ben a „CryptoPCard" elnevezésű adatvédelmi és adatrejtjelző rendszerrel és annak applikációival, valamint az MFT-t alapuló beszédrejtjelzéssel és beszélőfelismeréssel foglalkozik.

INFORMATIKAI BIZTONSÁG, KOMMUNIKÁCIÓ BIZTONSÁG

SZEKÉR KÁLMÁN

PROTAN INFORMATIKAI BIZTONSÁGI TANÁCSADÓ RT.
1554 BUDAPEST, PF. 41.

A kommunikáció biztonsága teljeskörűen csak a biztonság fogalmának szélesebb kontextusában értelmezhető. Ezt a teljesebb képet szolgálja egyrészt a biztonság fogalmának általánosságban — rendszerszinten, az információ, illetve a számítógépes feldolgozás szintjén — történő bemutatása, másrészt a kommunikáció biztonság sajátos vonásainak, célkitűzéseinek és a meghatározó ISO OSI 7498-2 szabványnak rövid áttekintése.

BEVEZETÉS

A biztonságos adatátvitel, kommunikáció problémakörének teljeskörű kezelése csak egy szélesebb kontextus, a biztonság általános, rendszerszintű megközelítése figyelembe vételével képzelhető el. Célszerű ezért a biztonság általános fogalmából kiindulva, az információ és az informatikai biztonság fogalmának érintésével eljutni a kommunikáció biztonságának kérdéseihez, sajátos problematikájához, követelményeihez.

1. RENDSZERSZINTŰ BIZTONSÁG

Általános értelemben véve a *rendszer biztonsága* az adott rendszernek alapermészete által meghatározott cél elérésére alkalmas állapotban való megmaradása képességét, a rendszer biztonságának védelme a rendszernek az ebben az állapotban való megtartását jelenti. Fontos kiemelni, hogy a célelérés követelménye magában kell foglalja a cél elérésének hatékony voltát.

Rendszer biztonságának védelme általános értelemben a fenyegető rendszerösszeomlások megelőzésére, lokalizálására, következményeik felszámolására irányuló tevékenység. Ez általában — az előrejelezhetőség, a beavatkozási lehetőségek korlátozott volta miatt — indirekt módon, olyan rendszertulajdonságok — állóképesség, túlélőképesség, alkalmazkodóképesség — fejlesztése révén valósul meg, amelyek a rendszer sebezhetőségének csökkentésében játszanak szerepet [1]. Rendszerek biztonságának három alapvető, egymástól elkülönítve azonban nem kezelhető területe az objektumbiztonság, az információ biztonság és a személyi-strukturális biztonság.

2. INFORMÁCIÓ BIZTONSÁG

Információ biztonsága vonatkozásában ennek a megkívánt állapotnak leírására a *funkcionalitás, rendelkezésre állás, bizalmasság, sértetlenség és hitelesség* kategóriái szolgálnak. Másképpen, az információkezelő, feldolgozó rendszerek biztonsági követelményei a fenti öt biztonsági alapállapotra vonatkozó követelményeken keresztül határozhatók meg. A következőkben az öt biztonsági alapállapot rövid áttekintését adjuk. Részletes bemutatásuk túlnő jelen írás keretein. Részletesebb ismeretek forrásául szolgálhat mind a nemzetközi, mind a hazai szakirodalom (pl. [2], [3], [4]).

A *funkcionalitás* biztosításának eredménye, hogy az információ kezelése, feldolgozása, az eredmények előállítása során megfelelő (összetételű) adatok kerülnek összegyűjtésre, tárolásra, feldolgozásra, az alkalmazott eljárások, algoritmusok megfelelnek az előírásoknak, a feldolgozás normális esetben a kívánt időhatárok között, megfelelő kapacitással történik, a folyamatba építhető ellenőrzési mechanizmusok kialakításra kerülnek.

Ebbe a témakörbe sorolható pl. a pénzügyi feldolgozást végző programok helyes működése, a bizonylatok kezelésének megfelelő rendje, a megfelelő szervezés, amely lehetővé teszi, hogy a szükséges adatok a megfelelő időben rendelkezésre álljanak, a logikai ellenőrzési funkciók, a túlzott kockázatú esetek jelzése stb.

A *rendelkezésre állás* biztosítása azt szolgálja, hogy az adatok és a szolgáltatások minden körülmények között — illetve a szükséges mértékben — az arra jogosultak számára hozzáférhetők legyenek.

Sok tényező játszhat közre abban, hogy a szükséges információ tökéletesen kialakított funkcionalitás ellenére sem áll rendelkezésre egyes esetekben. Ide tartozik az adatok sérülése, megsemmisülése (pl. a papírok elégése, egy „mindentudó" munkatárs balesete), feldolgozási vagy egyéb funkciók kiesése (pl. betegség, berendezések meghibásodása, kommunikáció kiesése) stb.

A *bizalmasság* állapotának fenntartása azt szolgálja, hogy minden adat és szolgáltatás csak az arra jogosultak számára, és jogosultságuk mértékében legyen hozzáférhető. Ez mindenekelőtt felveti az információ monopolizálhatóságának kérdését. Ennek keretében vizsgálni kell azt, hogy az adott információ ténylegesen eltitkolható-e. Másképpen, vizsgálni kell, hogy

- az adott információt lehetséges-e más módon kikövetkeztetni, előállítani (egyéb adatok, eljárások ismeretében);
- az információnak a munkavégzéshez szükséges megismerési köre ésszerűen szűkre szabható-e;
- az információ eltitkolása nem sért-e fontosabb értékekhez fűződő érdekeket.

A bizalmasság védelme érdekében pontosan meg kell határozni a titok fenntartásának időhorizontját, és foglalkozni kell azzal, hogy a titok fenntartásának feltételei, eszközrendszere folyamatosan fenntarthatók-e, beleértve különböző rendkívüli események kezelésének (pl. szerviz, helyettesítés, katasztrófa-elhárítás) eseteit is. A téma részletesebb kifejtését (ld. [5]).

A bizalmasság védelmét a jogi, üzleti követelményeken túl az általános értelemben vett biztonsági megfontolások is megkövetelik, amennyiben a védelem eszközrendszerének jelentős hányada alapul valamilyen titok fenntartásán.

Az *integritás vagy sértetlenség* védelme szolgálja azt, hogy az adatok a feldolgozás, tárolás során pontosan és csak a szándékozott és a jogosultságnak megfelelő módon és mértékben változzanak. Ez részben a hozzáférhetőség megfelelő szabályozásán, részben a hozzáférések utólagos vizsgálhatóságának és a felelősségrevonhatóságnak a fenntartásán, részben a jogosulatlan és véletlen módosulások hatékony kiszűrésén és helyreállításán alapul. Fontos kiemelni azt, hogy nem elég helyreállítani tudni egy meghamisított bejegyzést, azt időben, még a káros hatás érvényre jutása előtt fel kell tudni fedezni.

A *hitelesség* biztosítása eredményeképpen valamely — papíron vagy elektronikusan megjelenő — adat felhasználója biztosan, esetenként bizonyíthatóan tudhatja, hogy az adat valóban a felhasználó számára azonosított forrásból ered, és az adattartalom valóban megegyezik az adatforrás által szándékolttal.

3. INFORMATIKAI RENDSZEREK BIZTONSÁGA

Informatikai biztonságról számítógépes információfeldolgozó rendszerek kapcsán beszélhetünk. Az informatikai biztonság így az információ biztonság speciális esete, azaz a biztonsági követelmények meghatározása a fenti öt biztonsági alapállapot szerint történik. A számítógépes környezet azonban több olyan sajátossággal bír, amely biztonsági vonatkozásban speciális problémát jelent. Ezek közé tartozik:

- *Az adatok megjelenési formája az ember számára közvetlenül értelmezhetetlen.* Ennek fontos következménye, hogy nem ellenőrizhető egyszerű módon, hogy egy-egy adathordozó milyen adatokat is tartalmaz. További következmény, hogy az adatok rendelkezésre állásának biztosításához hozzátartozik a megjelenítő, hozzáférést biztosító eszközök rendelkezésre állásának biztosítása is.
- *Az adatfeldolgozás bonyolultsága, sebessége nem teszi lehetővé a történések „kézi" módszerekkel való ellenőrzését.* Így pl. a számítógépes feldolgozási folyamatok „könyvvizsgálatára", a biztonsági mechanizmusok működésének „hitelesítésére" speciális eszközöket kell alkalmazni.
- *Az adatok adathordozótól független megjelenése, másolhatósága* azt eredményezi, hogy egyrészt számítástechnikai környezetben nem lehet adatállomány „eredetiségéről" beszélni, másrészt digitális dokumentumok hitelesítése a szokásos módon (ahol a papír „köti össze" az aláírást a hitelesítendő szöveggel) nem valósítható meg.
- *A hozzáférési lehetőségek kiterjedt volta* a jelenlegi számítógépes rendszerek túlnyomó részénél a szokásos fizikai védelmi eszközök kiegészítését teszi szükségessé, ugyanakkor a számítógép önvédelme (algoritmikus védelem) sok esetben nem áll megfelelő szinten rendelkezésre.
- *A felhasználói tevékenység anonimitása*, az a tény, hogy az egyes akciók gyakran nem hagynak személyhez köthető „nyomot" maguk után, azzal jár, hogy a védelmi eszközök között fontos szerepet betöltő vizsgálhatóság, felelősségre vonhatóság biztosítása külön erőfeszítést igényel.

Számítógépek, számítógép-rendszerek biztonságával kiterjedt szakirodalom és fontos nemzetközi szabványok foglalkoznak. A legfontosabbak között meg kell említsük az amerikai egyesült államokbeli TCSEC (ismertebb nevén Orange book [6]) című dokumentumot, amelyhez számos kiegészítő dokumentum csatlakozik, amelyek együttesen Szivárvány könyvek (Rainbow series) néven ismertek. A TCSEC európai megfelelője az ITSEC dokumentum [7], amely az eredeti dokumentum továbbfejlesztett, és az európai országok szintjén harmonizált változata. Ezek a dokumentumok elsősorban azt a célt szolgálják, hogy az egyes számítógép-rendszerek biztonsági szintje, védelmi funkcionalitása mérhető, osztályozható legyen. Ilyen módon lehetőség van mind az egyes termékek egységes minősítésére (az ismert C2, B1 stb. besorolás), mind a felhasználói igények minősítési kategóriákban való megfogalmazására.

4. HÁLÓZATOK FENYEGETETTSÉGE

Hálózatok, kommunikációs lehetőségek megjelenésével a fentiekben érzékeltetett problémakör tovább szélesedik. Ennek okai a következők:

- A hálózat bonyolult volta miatt a biztonsági vonatkozásokat nehezebb átlátni és egységesen kezelni. A hálózat egyes részeinek fenntartása mind műszaki, mind egyéb szempontok szerint (pl. hozzáférési jogok kezelése) egymástól elkülönült szervezetek által történik, központilag nehezen kézben tartható.
- A hálózat kiterjedése dinamikusan változik, esetenként központilag nehezen kontrollálható. Számos megtörtént behatolás támasztja alá azt, hogy biztonsági szempontból egységes hálózatként kell kezelni mindazokat a rendszereket, melyek hálózati kapcsolatban állnak a vizsgált rendszerrel. Ebben a megközelítésben pedig nyilvánvaló, hogy a rendszer mérete nem csak dinamikusan változik, hanem sok esetben ismeretlen és teljességgel átláthatatlan és befolyásolhatatlan is.
- A hálózat kiterjedtsége miatt sok a lehetséges támadási pont. Ha a hálózat valamelyik eleme külső hálózatra csatlakozik, akkor a támadás lehetséges helyeinek száma nagyságrendileg megnőhet és kezelhetetlenné válhat. Mivel a hálózatban az információ számos csomóponton és csatornán át jut el rendeltetési helyére, a behatolónak számos lehetősége van a támadás helyének kiválasztására.
- A hálózat felhasználóinak a száma nagy, így sok a potenciális támadó. Különösen igaz ez abban az esetben, ha a hálózat nyilvános hálózatra csatlakozik, vagy kapcsolt telefonvonalon hívható. Nyilvános hálózaton nagy a célzatlan támadás veszélye, amikor a támadó nem egy bizonyos rendszer támadására törekszik, hanem egyszerűen csak igyekszik behatolni oda, ahova lehet. Az ilyen célzatlan támadások is nagy kárt okozhatnak, és idővel célzottá is válhatnak.
- A kommunikációs csatornák fizikailag a csomópontok-

nál általában lényegesen kevésbé védettek, sok esetben teljesen védtelenek. Ez számos behatolási módra ad lehetőséget, a forgalom megfigyelésétől az üzenetek módosításáig.

5. HÁLÓZATOK BIZTONSÁGA

Számítógépes hálózatok kialakítása, tágabb értelemben adatátviteli lehetőségek létrehozása, működtetése kapcsán a biztonság követelményeit a következőkben foglalhatjuk össze:

1. *Az adatátvitel folyamán, illetve következtében az adatok biztonsága nem csökkenhet.*
   Az adatátvitel folyamata gyakran úgy tekinthető, hogy az adatok egy biztonságos környezetből egy másik biztonságos környezetbe, egy gyakorlatilag védtelennek tekinthető közegen keresztül jutnak el. A védtelen közegben az adatok biztonságát a rendelkezésre állás, a bizalmasság, a sértetlenség és a hitelesség tekintetében is veszély fenyegeti. Ezeknek a fenyegetéseknek kivédésére szolgáló eszközöket egyre elterjedtebben alkalmazzák. Ezt jelzi az is, hogy az adatátvitel terén bekövetkezett nemzetközi szabványosítási tevékenység immár az alkalmazható védelmi eszközökre is kiterjed. A vonatkozó legfontosabb szabvány rövid ismertetésére a következő szakaszban térünk ki.
2. *Az adatátvitel eredményeként az adatok nem kerülhetnek kevésbé biztonságos környezetbe.*
   Nehezebben kezelhető, és sajnos kevésbé figyelembe vett követelmény, hogy az adatok átvitelére nem kerülhet sor, ha az adatok végcéljaként meghatározott környezetben az előírt biztonság nem áll fenn. (Az átvitel során az adatok ideiglenes megjelenése pl. a hálózat egyes aktív elemein, csomópontjain, továbbá ezek következményei az előző kérdéskörbe tartoznak.)
   Az amerikai egyesült államokbeli informatikai biztonsági szabályozás külön kötetben foglalkozik a korábban említett TCSEC hálózati környezetre vonatkozó interpretációjával [8]. A szabályozás külön megszabja, hogy milyen esetekben lehetséges kétirányú, és milyen esetekben csak egyirányú (a kevésbé biztonságos rendszertől a biztonságosabb felé irányuló) adatátvitel. Meghatározza, hogy egy adatátviteli csatorna mikor alkalmas többszintű (pl. vegyesen szigorúan titkos, titkos és nyílt) adatok, és mikor csak egyetlen minősítési szint átvitelére. Útmutatást ad, hogy önmagukban adott biztonsági szintet elérő rendszerek milyen feltételek mellett kapcsolhatók össze, és a létrejövő együttes rendszer milyen új minősítési szintet érhet el.
3. *Az összeköttetés nem csökkentheti az egyes számítógépek, számítógép-rendszerek biztonságát.*
   Számítógép-rendszerek kommunikációs lehetőségeinek kialakításakor legtöbbször nem elegendő, ha csak az „elsődleges értékek", az adatok biztonságára terjednek ki megfontolásaink. Azt is figyelemmel kell kísérjük, hogy a kommunikációs csatornák léte mennyiben növeli az egyes rendszerek fenyegetettségét, támadhatóságát. Sajnos gyakori példaként említhető a bejelentkezéshez használatos jelszavak bizalmasságának sérülése. A legtöbb operációs rendszerben, alkalmazói rendszerben a jelszavak átvitele nyílt formában történik. A jelenleg „divatba jött" publikus hálózatmonitorozó programokkal távoli bejelentkezések esetén viszonylag kis fáradsággal és szakértelemmel az adatforgalomból bárki kiszűrhet jelszavakat. Ez pedig alapjaiban támadja a legtöbb számítógépes védelmi rendszert.
   Másik példa új támadási lehetőség megjelenésére a legtöbb platformon megtalálható azon szolgáltatás, amely egyes hálózati csomópontokon érvényesen bejelentkezett felhasználóknak megkönnyíti, illetve automatikussá teszi más csomópontokra való bejelentkezését (VMS proxy login, Unix trusted hosts stb.). Ilyen módon a hálózat egyetlen gépére behatolva a támadó gyakorlatilag egy egész sor rendszer védelmi vonalán juthat túl.
   További példaként szolgálhat egy-egy kevéssé ismert biztonsági rés (pl. Unix sendmail csapóajtó, VMS SETEUI hiba stb.), amelyet az eredetileg szűk felhasználói kör nem ismer, nem tud „kiaknázni", azonban a hozzáférési lehetőségek kiterjesztésével mind a potenciális szakértelem, mind a kísérletezési lehetőség veszélyes méreteket ölthet.

6. AZ OSI BIZTONSÁGI ARCHITEKTÚRA

Az adatátvitel terén meghatározó dokumentum a nyílt rendszerek összekapcsolására vonatkozó OSI (Open Systems Interconnection [9]) nemzetközi szabvány, amelynek részeként külön dokumentum — OSI 7498-2 [10] — foglalkozik a javasolt biztonsági architektúrával. A dokumentum általános leírását nyújtja az OSI modell keretében megvalósítható biztonsági szolgáltatásoknak és az azokhoz kapcsolódó biztonsági mechanizmusoknak (különválasztva a mit és hogyan kérdéseit). Meghatározza továbbá azokat a pozíciókat, amelyekben a szolgáltatások és mechanizmusok a réteges szerkezetű OSI modellben megvalósíthatók.

Az adatátvitel során fellépő fenyegető tényezőket a következőkben összegezhetjük:

- *Üzenetek, üzenetfolyam sérülése:* a hálózaton átvitt üzenetekbe adatok, mezők, csomagok beszúrhatók, az üzenetek duplikálhatók, tartalmuk módosítható, egyes eredeti üzenetek visszajátszhatók, így érve el a kívánt hatást.
- *Bizalmasság elvesztése:* az adatátvitel során az adatátviteli csatornákon vagy az egyes csomópontokban az üzenetek tartalma illetéktelenek által hozzáférhetővé válhat.
- *Megszemélyesítés:* a hálózat egyes elemei, vagy arra csatlakozó idegen elemek önmagukat egy másik csomópontnak adhatják ki, így megtévesztő üzeneteket küldhetnek, vagy a címzett helyett üzeneteket fogadhatnak.
- *Adat küldésének, megkapásának letagadása:* az adatküldés eseményei gyakran nem hagynak olyan nyomot a rendszerben, amely hitelt érdemlően bizonyíthatná megtörténtüket. Mivel az üzeneteket általában nem kíséri pl. papír bizonylat, lehetőség van „kellemetlen" üzenetek letagadására.
- *Üzenetek eltérítése:* a routerek átprogramozásával az üzenetek más címre (is) továbbíthatók, így bizalmasságuk sérülhet, esetleg a címzett meg sem kapja azokat.
- *Forgalom megfigyelése:* az adatátviteli csatornák forgalmának megfigyelésével információk gyűjthetők a rendszerről.
- *Funkcionalitás sérülése:* előfordulhat a normális működés ellehetetlenülése, pl. egyes programok vagy hardver

elemek kiesése, hibás működése, vagy az adatátviteli kapacitás behatolók által történő nagyfokú lekötése miatt.

Az OSI biztonsági architektúrában meghatározott alapvető biztonsági szolgáltatások a következők:

- *Hitelesítés:* az adateredet hitelesítés igazolja, hogy az adat eredeti forrása valóban az, amelyik forrásként meg van adva. Ez az igazolás azonban nem véd az adatelem megduplázása vagy módosítása ellen. Az ún. társentitás hitelesítés azt igazolja, hogy az aktuális kommunikáló fél valóban a megadott entitás, így megfelelő módon alkalmazva kizárja a megszemélyesítés vagy a visszajátszás lehetőségét.
- *Hozzáférés-ellenőrzés:* feladata az OSI-n keresztül elérhető erőforrások jogtalan használata elleni védelem biztosítása. A hozzáférés-ellenőrzés által védett erőforrások lehetnek OSI vagy nem OSI erőforrások, melyeket OSI protokollokon keresztül érnek el. A védelem vonatkozhat az erőforrás összes hozzáférésére vagy egy erőforrás különböző hozzáférési típusaira.
- *Adat titkosság:* kiterjed az egyes üzenetek és a teljes forgalom bizalmasságának védelmére. Az üzenetek bizalmassága megvalósulhat egy-egy kapcsolat (a kapcsolat teljes tartama alatt küldött üzenetek), egy-egy üzenet, vagy üzenetek egyes részei vonatkozásában. Az összeköttetés titkossága szolgáltatás mind a címzési és egyéb adminisztratív adatok, mind a forgalom időbeli jellemzői elfedésére vonatkozik.
- *Adat sértetlenség:* kiterjed mind az egyes üzenetek, mind az üzenetfolyam sértetlenségének védelmére. Megvalósulhat egyes üzenetek, illetve üzenetmezők szintjén, vagy egy teljes kapcsolatfelvétel (összeköttetés) tartamára. Magába foglalhatja a sérült üzenet helyreállítását is.
- *Letagadhatatlanság:* biztosítása harmadik fél számára is bizonyíthatóvá teszi, hogy adott üzenet adott forrásból származik, hogy az elküldés, illetve a kézbesítés valóban megtörtént.

A fenti szolgáltatások megvalósítására biztonsági mechanizmusokat kell alkalmazni, amelyek [10] felosztásában a következők lehetnek: rejtjelezés, digitális aláírás mechanizmusok, hozzáférés ellenőrzési mechanizmusok, adatépség mechanizmusok, hitelesítés-csere mechanizmusok, forgalom helykitöltési mechanizmusok, forgalomirányítás ellenőrzési mechanizmusok, valamint közjegyzői hitelesítési mechanizmusok.

A biztonsági szolgáltatások és mechanizmusok kapcsolódását mutatja az 1. táblázat.

A táblázat érzékelteti, hogy a rejtjelezés, illetve az ahhoz kapcsolható egyéb mechanizmusok (digitális aláírás, adatépség védelme) mennyire központi szerepet töltenek be az adatátviteli biztonsági szolgáltatások megvalósításában. Látszik azonban az is, hogy ez a szerep nem kizárólagos és igen sokrétű. A mechanizmusok kiválasztása és működtetése ugyanis összhangban kell hogy álljon a megvalósítandó kommunikációbiztonsági szolgáltatásokkal, továbbmenve, az informatikai biztonság teljes eszközrendszerével.

1. táblázat. Biztonsági szolgáltatások és mechanizmusok

	Mechanizmusok							
Szolgáltatás	Rejtjelezés	Digitális aláírás	Hozzáférés ellenőrzés	Adatépség	Hitelesítés csere	Forgalom helykitöltés	Forgalom-irányítás ellenőrzés	Közjegyzői hitelesítés
Társentitás hitelesítés	I	I	–	–	I	–	–	–
Adateredet hitelesítés	I	I	–	–	–	–	–	–
Hozzáférés ellenőrzés	–	–	I	–	–	–	–	–
Összeköttetés szintű titkosság	I	–	–	–	–	–	I	–
Összeköttetés nélküli titkosság	I	–	–	–	–	–	I	–
Kiválasztott mező titkosság	I	–	–	–	–	–	–	–
Forgalom titkosság	I	–	–	–	–	I	I	–
Összeköttetés szintű sértetlenség	I	–	–	I	–	–	–	–
Összeköttetés nélküli sértetlenség	I	I	–	I	–	–	–	–
Forrás letagadhatatlanság	–	I	–	I	–	–	–	I
Kézbesítés letagadhatatlanság	–	I	–	I	–	–	–	I

Megjegyzés: I – A mechanizmus (magában vagy más mechanizmusokkal kombinálva) alkalmas az adott szolgáltatás megvalósítására.

7. ZÁRÓ MEGJEGYZÉSEK

Meg kell tehát állapítani, hogy kommunikációs rendszerek biztonságának erősítése, megvalósítása nem korlátozódik az adatoknak az adatátvitel folyamán történő védelmére. A kommunikáció biztonsága sem megvalósításában, sem pedig hatásaiban nem választható el az összekapcsolt rendszerek biztonságától, szélesebb értelemben pedig a szervezeti szintű biztonság kérdéseitől.

Fontosnak tartjuk annak kiemelését, hogy mind a nemzetközi szakirodalom, mind a tapasztalatok azt mutatják, hogy gyakran feloldhatatlan ellentét áll fenn a hálózat rugalmassága és univerzalitása, a hozzáférés könnyűsége, valamint a számítógép-rendszer biztonsága között. A hálózat biztonságának kielégítő megvalósításakor sok esetben azzal a dilemmával találjuk szembe magunkat, hogy az illegális behatoló dolgának megnehezítésével együtt nehezítjük a legális felhasználók életét is. Ezzel kapcsolatban figyelembe kell venni azt a tényt is, hogy a jogosult felhasználóknak okozott nehézségek nemcsak a biztonsági rendszer költségeit növelik, hanem bizonyos mértékig a biztonság ellen is hatnak, amennyiben a felhasználók a biztonsági intézkedések nehézkessége miatt nem tartják be azokat, vagy megkerülésükre törekszenek.

Ilyen körülmények között fokozott jelentősége van annak, hogy a hálózattal és általában a számítógépes rendszerrel szemben támasztott követelmények megfogalmazásakor a funkcionalitásbeli és a biztonsággal kapcsolatos igényeket egymással összefüggésben vizsgáljuk, figyelembe véve a kölcsönös következményeket. A tapasztalat azt mutatja, hogy esetenként célszerűbb lemondani olyan funkciókról, amelyeknek megvalósítása a biztonságot nagymértékben csökkenti, vagy a védelmet elfogadhatatlanul megdrágítja.

Ha azonban ez nem lehetséges, akkor explicit módon csökkenteni kell a biztonsági követelményeket. Igy legalább mindenki tudhatja, mit vállal.

IRODALOM

[1] Nagy Károly: „Biztonságvédelmi funkciók kiteljesedése", *Detektor*, 1994/1.

[2] Jackson, C. B.: „The Need for Security, Datapro Reports on Information Security", 1991.

[3] Caelli, W., Longley, D. and Shain, M.: „Information Security Handbook", Macmillan Press Ltd, 1991.

[4] Informatikai biztonsági módszertani kézikönyv, 8. sz. ajánlás, MeH Informatikai Koordinációs Iroda, 1994.

[5] Nagy Károly: „Adatvédelem, informatikai biztonság", HISEC '93 konferencia.

[6] DoD Trusted Computer System Evaluation Criteria (TCSEC), DOD 5200.28-STD, December 1985.

[7] Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, May 1992., EC DGXIII.

[8] NCSC Trusted Network Interpretation of the TCSEC, NCSC-TG-005, July 1987.

[9] Information processing systems. Open Systems Interconnections Basic Reference Model. General requirements — ISO 7498: 1984.

[10] Information processing systems. Open Systems Interconnections Basic Reference Model — Part 2: Security Architecture — ISO 7498-2: 1989 (E).

INFORMATION SECURITY AND COMMUNICATION SECURITY

K. SZEKÉR

PROTAN INFORMATION SECURITY CONSULTING SERVICES CORPORATION
H-1554 BUDAPEST, P.O.BOX 41., HUNGARY

Communication security is part of the general concept of security. To set up a broader picture on the one hand the concept of security is given in general — in the level of system, information and IT security —, on the other hand the special aspects of communication security are shown together with a short overview of the important OSI 7498-2 standard.

Szekér Kálmán 1986-ban a BME Villamosmérnöki Karán szerzett diplomát. A KFKI falai között, először az MSZKI, majd a Xeus Rendszerépítő Iroda munkatársaként elsősorban Unix platformon rendszerprogramozóként és szakértőként tevékenykedett. Jelenleg a PROTAN Informatikai Biztonsági Tanácsadó Rt. vezető projekt menedzsereként kormányzati és banki informatikai rendszerek biztonságával kapcsolatos átvilágítási feladatokban, tanulmányok készítésében, oktatásban vesz részt.

BANKINFORMATIKUS KÉPZÉS A MŰEGYETEMEN

A hazai bankok informatikai szakemberképzése és utánpótlása — saját helyzetértékelésük szerint — jelenleg nem megoldott. Az igény kielégítéséhez részben banki/pénzügyi szakemberek informatikusi továbbképzésére, részben informatikusok bankspecifikus szakképzésére van szükség. Ezen túlmenően a bankinformatika nem egyszerűen a banki és számítástechnikai szakmák tudásanyagának közös oktatáást jelenti, hanem egy új minőséget is reprezentál az alkalmazott informatika e területén.

Az igény a felhasználónál támad: a korszerű működéshez szükséges technikai — elsősorban számítástechnikai — infrastruktúra megteremtésekor a bankok elsősorban a nagyértékű gépi, illetve szoftver háttér megteremtésére figyeltek, s így elmaradt az optimális működtetéshez szükséges beruházások talán legfontosabbika, a humán erőforrás megteremtése. (Mértékadó vélemények szerint az átállás, az átmenet nehézségei nem kis részben ennek is betudhatók). A méregdrága rendszereknek azonban üzemelniük kell, ezért nagy erőfeszítésekkel mindig sikerült olyan szakembereket találni, akik jól-rosszul alkalmasak voltak (vagy lettek) a működtetésre. A továbbiakban azonban ez nem járható út: ahogy minden nagy szakértelmet igénylő részfeladat esetében, itt is szisztematikus és alapos képzésre van szükség.

Ezt a célt szolgálja a bankinformatikusi tudást megalapozó képzés megjelenése a Műegyetemen. 1994 szeptemberétől a nappali tagozatos műszaki informatika szakos hallgatók már választhatják a másfél éves „Bankinformatika" tantárgy-csomagot, s nem is haboztak: jelentkeztek. A fejlődés irányát felmérve ráéreztek, hogy munkaerőpiaci helyzetüket ugyancsak megerősítik, ha számítástechnikai ismereteik mellett a legfontosabb felhasználói világok valamelyikéből is naprakész tudást szereznek. Mindennél többet mond az óriási érdeklődés. A negyedévesek számára szabadon választható tárgyra *félszáz* műszaki informatikus hallgató jelentkezett (az évfolyam túlnyomó része), s az egyébként nem érintett ötödévesek közül is tizennégyen tartották szükségesnek, hogy elérjék: ők is hivatalosan járhassanak az órákra.

A képzés igazi „nagykorúsítását" azonban az 1995 februárjában induló térítéses *posztgraduális bankinformatikai képzés* jelenti, amely azonban már nem a mérnökképzés része (mégha a kétfajta képzési forma tartalma egyébként jelentősen át is fedi egymást).

A teljes *posztgraduális szakképzési program* (tanfolyami formában) két *egyéves képzésre* tagolódik, amelyet egy *féléves szakdolgozat* elkészítési időszak zár le. (Az egyéves képzés elkülönítését — a piaci igények felmérése után — azért javasolták a szervezők, hogy lehetőség legyen csupán egy-egy évre is csatlakozni a programhoz, kisebb értékű diploma fejében).

Az első félév alaptárgyi vizsgákkal, a második alapszigorlattal zárul, amelyről — a tanulmányok megszakítása esetén — bizonyítvány adható. A negyedik félév zárószigorlattal fejeződik be, amelyről szintén bizonyítvány állítható ki. A teljes értékű oklevél kiadásának feltétele a szakdolgozat benyújtása és elfogadása.

A program előzetes elképzéseit az egyetem Társadalmi Informatika Osztályának néhány munkatársa vezető bankszakemberekkel közösen állított össze. A nagy számban visszaérkező egyetértő-jóváhagyó, illetve javaslatokkal kiegészítő válasz után elkészültek a részletes tematikák és óratervek. Eszerint a a Bankinformatika képzés tantárgyai a következők:

Alaptárgyak:

- Banküzemtan
- A bankinformatika számítástechnikai alapjai
- Banki információs rendszerek működtetése
- Bankbiztonság és adatvédelem
- Banki információs rendszerek technológiája
- Tőkekihelyezés, finanszírozás, projektkövetés informatikája
- Tudásszervezés és kommunikáció a bankban
- A banki információs rendszerek fejlesztési módszertana

„A típusú" (kötelezően választható) alternatív tárgyak:

- Döntési informatika a bankban
- Bankjog
- Ergonómia és munkavédelmi menedzsment
- Nagyszámítógépes adatbáziskezelés
- Változásmenedzsment
- Banki szolgáltatások fajtái és marketingjük
- Érvelés és tárgyalástechnika
- Telematikai rendszerek és szolgáltatások

„B típusú" (fakultatív) alternatív tárgyak:

- Számítástechnikai alapismeretek és szemléletek
- Szervezet-szociológia
- Információs társadalom
- Üzleti hálózatok
- Üzleti etika
- Sajátos finanszírozási értékrendek és megoldások (a „zöld" bank)
- Teljeskörű minőségmenedzsment – TQM
- English for Banking I-II. (kezdő és haladó banki angol)

Az oktatás nagy terjedelmű anyagot fog át nagyon igényesen, s ezt — ehhez képest — nem hosszú idő alatt adja át. Azonnal „hadra fogható" tudást ad, amelynek alkalmazásától a célterületen minőségi ugrás remélhető. A képzés színvonalát rangos szakmai gárda fémjelzi: a két nagy induló témacsoport „gazdája" például Bácskai Tamás és Angyal Zoltán.

A törzsanyag tárgyai mind a főiskolai képzésben, mind az egyetemi szintű képzésben komplex jellegűek, amelyek tematikájának, tananyagának részletes kidolgozására a gesztor kar (a Műegyetem Természet- és Társadalomtudományi Kara) pályázatot hirdet.

A nagy várakozással fogadott képzés első évének tapasztalataira — amennyiben mód nyílik rá — a Híradástechnika hasábjain visszatérünk. ■

AZ EUROHÍVÓ DIGITÁLIS SZEMÉLYHÍVÓ SZOLGÁLTATÁS

Az EUROHÍVÓ személyhívó szolgáltás komplett üzenetközvetítési megoldást kínál a magyar piac számára. Hosszú és személyre szóló nagysebességű, alfanumerikus üzenetek továbbítására alkalmas („Fax a zsebben").

Az EUROHÍVÓ személyhívó szolgáltatás főbb jellemzői:

- Hosszú üzenetek továbbítása. A személyhívó memóriájában 7800 karaktert tud tárolni.
- Mobil kommunikáció elérhető áron.
- Személyes üzenetközvetítés.
- Csoport-hívás (egyszerre több személy is elérhető).
- „Alpha Mail" (gyorsított üzenethagyás). A hívást a hívott előfizető saját postafiókja fogadja, azt automatikusan rögzíti, majd továbbítja az első szabad operátorhoz. Az operátor beviszi a rendszerbe az üzenetet, amely percek alatt kisugárzásra kerül. Így nincs szükség személyes érintkezésre a hívó fél és az operátor között, ezáltal idő takarítható meg.
- Rendszeres,aktuális információ szolgáltatás (hírek, időjárás) az EUROHÍVÓ minden előfizetője részére.

Az EUROHÍVÓ szolgáltatás potenciális ügyfelei:

Mindazok, akiknek fontos,hogy bárhol, bármikor elérhetők legyenek, így:

- Azok, akiknek sikere attól függ, hogy időben jussanak el hozzájuk gyors és megbízható információk (pl. újságírók, értékesítéssel vagy tőzsdei munkával foglalkozók).
- Az olyan vállalatok, amelyeknek olcsó és megbízható megoldásra van szükségük, a mindíg úton lévő dolgozóik elérésére (pl. szállító vállalatok). Mivel a készülékről hívás nem kezdeményezhető, így nem merül fel nem kívánatos telefon költség a vállalat részére.
- Kis- és egyéni vállalkozók, akik számára fontos, hogy bármikor személyes üzenetvevő és közvetítő szolgáltatással rendelkezzenek, amely kiváltja a saját iroda költségeit.
- Bárki, aki szeretne elérhető lenni, de nem kíván minden bejövő hívást rögtön megválaszolni.

Az EUROHÍVÓ szolgáltatás működése:

Az EUROHÍVÓ szolgáltatás az ERMES (European Radio Massage System) rendszer alapján működik, amely az európai standard-et jelenti a személyhívó szolgáltatások terén. A rendszerhez eddig 21 ország csatlakozott. Az ERMES digitális rendszer lehetővé teszi majd a jövőben az országok közötti mozgást (roaming) is használói számára.

Egy EUROHÍVÓ előfizető részére érkező üzenetet az operátor rögzíti a személyhívó rendszerben, amely rendszer fix rádió hullámokon sugározza ki az üzenetet az éterbe. Az EUROHÍVÓ személyhívó gyakorlatilag egy hordozható rádió-vevőkészülék,amely saját, előre meghatározott címmel (hívószámmal) rendelkezik. A vevőkészülék csak a saját címére érkező üzeneteket rögzíti és jelzi. Azt, hogy a vevőkészülék milyen módon (hangjelzéssel vagy diszkrét mozgással) jelezze az üzenet vételét a felhasználó tudja meghatározni.

Üzenet küldésekor a hívó fél a következő 10 számjegyű hívószámot tárcsázza: 06-503-XXXXX. Az utolsó öt számjegy azonosítja a hívott előfizetőt. A beérkező üzenet az alábbi két mód egyikén kerül feldolgozásra:

- Operátor. A hívó felet egy operátor üdvözli, aki rögzíti az üzenetet a rendszerben,amely automatikusan és pillanatok alatt kisugárzásra kerül.
- Alpha posta (Hang-üzenet). A hívó felet a hívott előfizető saját hangposta fiókjához továbbítja a rendszer. Az automatán hagyott üzenetet az első szabad operátor viszi be a rendszerbe, amely pillanatok alatt közvetítésre kerül.

Jelenleg a japán NEC cég gyárt ERMES rendszerű személyhívó vevőkészüléket. Ezek memóriája 7800 karaktert vagy 40 üzenetegységet képes tárolni.Az üzeneteket a rendszer ún. üzenet- egységek formájában továbbítja.Minden egyes üzenet-egység max. 350 karakterből állhat. (Ennél hosszabb üzenet több egységben küldhető ki.) Minden vevőkészülék az elsődleges hívószámon felül rendelkezik egy ún. második címmel is. Erre a második címre naponta többször az EUROHÍVÓ szolgáltató rendszeres, aktuális híreket sugároz.

Az EUROHÍVÓ szolgáltatás típusai:

- Alapszolgáltatások.
- Információs szolgáltatások.
- Személyes üzenetközvetítés.
- Különleges szolgáltatások.

Alapszolgáltatások:

Az alapszolgáltatás korlátlan számú üzenetküldést tartalmaz meghatározott havi díj ellenében. Külön térítés nélkül az alapszolgáltatás része a napi hírek és az időjárásjelentés közvetítése.

Információs szolgáltatások:

Minden készülék rendelkezik egy ún. másodlagos címmel, amely minden felhasználónak azonos. Ezen a második címen naponta többször is híreket és időjárás-jelentést sugárzunk.

Személyes üzenetközvetítés:

Az EUROHÍVÓ számos titkárnői szolgáltatást tud nyújtani. Ezek kökzé tartozik a személyes üdvözlés.

Különleges szolgáltatások:

- Alpha posta.
- Csoport hívás. Több egyéni előfizetőből (max. 16) rendszercsoportot képez. A csoport ugyanabban a pillanatban elérhető egy üzenettel. Több 16 fős kis csoportból előállítható bármely nagyságú csoport.
- Üzenetek kinyomtatása. Az előfizető kérheti az utolsó két hét üzeneteinek papírra nyomtatását.
- Hosszútávú üzenet tárolás. Az előfizető kérheti, hogy üzeneteit az EUROHÍVÓ szolgáltató három hétig tárolja a rendszerben. A tárolt üzenetek kérésre kinyomtathatók vagy újra sugározhatók.

Az EUROHÍVÓ és a mobil telefonok:

Az EUROHÍVÓ személyhívó szolgáltatás kiegészítője a celluláris telefonoknak, mivel eltérő mobil kommunikációs igényeket elégít ki. A személyhívás nem helyettesítheti a kétirányú kommunikációt. Kutatások szerint azonban az üzleti kommunikáció kb. 70%-a egyirányú. Erre az esetre kínál az EUROHÍVÓ egy költségkímélő megoldást.

Az EUROHÍVÓ országos személyhívó hálózat kialakítása:

Az EURO-HÍVÓ Rt. személyhívó hálózata Budapest besugárzásával indul.A hálózat központi állomása Budapesten a Váci út 37. szám alatt van. A központi állomás és a 10–20 km átmérőjű hatótávolsággal rendelkező, fix frekvencián működő, azonos információt folyamatosan kisugárzó bázisállomások közötti (egyirányú) kapcsolatot VSAT rendszerű műholdas összeköttetés biztosítja. A központi állomásra és a VSAT HUB állomásra vezetékes, bérelt vonalon jut el az információ.A bázisállomások nagy adatsebessége (6250 bps) a 169.675 MHz-es frekvencia négyszintű kódolásával érhető el.

A bázisállomások feladata:

A bázisállomások két feladatot látnak el. Az egyik feladat a műhold által sugárzott információ vétele, melyre 1,2 m-es átmérőjű parabola antenna szolgál.

A másik feladat a beérkező jel feldolgozása és kisugárzása a 169.675 MHz-es frekvencián a személyhívó vevők felé. A több bázisállomásból álló, nagykiterjedésű személyhívó rendszerek helyes működésének feltétele a bázisállomások szinkronizálásának biztosítása.

Az EURO-HÍVÓ Rt. személyhívó hálózatának szinkronizációja a GPS (Global Positioning System) rendszeren alapul. Az EURO-HÍVÓ Rt. hálózata két helyen alkalmaz GPS vevőkészüléket, melyek szolgáltatják a pontos időalapot a rendszer szinkronizációjához. GPS egység kerül felszerelésre a személyhívó vezérlő központban, illetve a digitális szakasz átjátszó egységnél (HUB).

A bázisállomásokon GLENAYRE (USA) gyártmányú, ERMES rendszerű GL-T5410 típusú adóberendezést alkalmaznak. A bázisállomási adók főbb jellemzői:

- Működési frekvenciasáv: 138-175 MHz
- Moduláció: 4-PAM/FM
- ERP: 250 W
- Adatsebesség: 6250 bps
- Csatornaosztás: 25 kHz (min. 5 kHz)

A személyhívó vevő a NEC (Nippon Electric Corporation) terméke. A PA 3E6-1B típusú személyhívó vevő megfelel az ERMES előírásainak.

A személyhívó vevő főbb jellemzői:

Kód:	ERMES
Vételi frekvencia:	169,425 – 169,800 MHz
Moduláció:	4-PAM/FM
Méretek:	91mm x 57mm x 19,3mm
Tömeg:	94 g
Adatátviteli sebesség:	6250 bps
Hangjelzés:	2
Képernyő:	LCD 80 karakter (4x20) 5x7 pontos mátrix karakterek Automatikus képernyő világítás
Üzenethossz:	max.7800 karakter
Memóriakapacitás:	max. 7800 karakter vagy 40 üzenet
Működési hőmérséklet:	−10°C – +55°C
Feszültség:	1 db 1,5 V-os elem AAA méretű elem
Az elem élettartama:	900-950 óra alkáli elemmel

WILK NÓRA

ITEA®

Adat - és információvédelem

Nálunk megtalálja a legkorszerűbb, leghatékonyabb, legárnyaltabb adatvédelmi eljárások és szolgáltatások választékát, amelyeket a

CryptoPCard®V2.0

ADATVÉDELMI RENDSZER

kriptográfiai, rejtjelző képességeire alapoztunk.

RENDSZERFUNKCIÓK:

- tömörítés
- kriptográfia, adatrejtjelezés,
- felhasználó azonosítás,
- partnerhitelesítés,
- üzenethitelesítés,
- digitális aláírás,
- időpecsét,
- hierarchikus hozzáférésvédelem,
- adatvédelmi funkciók aktivizálásának naplózása,
- kulcsgenerálás, -frissítés,
- archiválás.

JAVASOLJUK:

Különleges adatvédelmet igénylő intézmények;
Állami hivatalok;
Bankok, pénzintézetek;
Biztosító társaságok;
Adatnyilvántartók, adatbankok;
Cégek vezetői információs rendszerei;
Egészségügy;
Bíróság, ügyvédi-, közjegyzői irodák részére,
stb.

REJTJELZÉSI JELLEMZŐK:

- magyar fejlesztésű és gyártású hardver és szoftver;
- kulcsgenerálási eljárás opciók:
  - nyilvános kulcs (RSA),
  - csere kulcs (CHG),
  - véletlen (RDN),
  - hierarchikus,
  - input,
  - fix,
  - levelező,
  - disk rejtjelző,
- rejtjelzési algoritmus opciók:
  - CPC
  - FADS
  - DES
  - RSA
  - felhasználói;
- rejtjelzett külső eszközben tárolt kulcs elemek és algoritmus;
- eseménynaplózás védett memóriába (nem hamisítható);
- a gyártó által folyamatosan biztosított kulcscsere lehetőség;
- menüvezérelt és/vagy programozott eltérés;
- egyszerű kezelhetőség (nem igényel számítógépes ismeretet);
- rejtjelzési sebesség: 128 kbit/s.

ITEA®

InformációTechnikai és Elektronikus Adatvédelmi Kft.

a KFKI Számítástechnikai csoport tagja

Cím: 1121 Budapest XII, Konkoly Thege M. út 29-33.
Tel.: 169-7574,169-499/2488
Telefax: 155-1894
Levélcím: 1525 Budapest, Pf. 49.

KÖNYVISMERTETÉS

HÍRADÁSTECHNIKA
Szerkesztette: Géher Károly

Merész vállalkozást teljesített a BME huszonkét oktatója. A híradástechnika jelenleg fontos összes területének bevezető ismertetését mindössze 319 oldalon összefoglaló könyvet tart kezében az olvasó. A könyv megjelenését a Budapesti Műszaki Egyetem Villamosmérnöki és Informatikai Karán 1991-ben bevezetett új tanterv tette szükségessé. Eszerint a hallgatók öt félévig ugyanazt a tananyagot tanulják, képzésük csak a hatodik félévtől kezdve specializálódik. A villamosmérnöki ismeretek alapját képező egyik szaktárgyat, a híradástechnikát az ötödik félévben hallgatják. A Híradástechnika c. tárgy tananyagát tartalmazza ez a könyv, mely eredetileg a hallgatók részére készült jegyzet lett volna. A Műszaki Könyvkiadó érdeme, hogy a híradástechnika iránti szélesebb körű érdeklődést felismerve a jegyzet helyett könyv kiadására vállalkozott.

A könyv szerkezete könnyen áttekinthető, a gyors ismeretszerzést messzemenően támogatja. A fejezetek a könnyebb áttekinthetőség kedvéért a résztémákat felölelő alfejezetekre tagolódnak. Különösen értékesek a fejezetek elején található rövid összefoglalók, melyek a fejezetek anyagát mindennapi világképünkben elhelyezik. A fejezetek törzsanyaga a részterületek legfontosabb megállapításainak, tételeinek és összefüggéseinek tömör, bizonyítás nélküli összefoglalása. A fejezetek végén feladatok, ellenőrző kérdések és az alapvető irodalmi hivatkozások felsorolása segíti az anyag megértését. A huszonnégy fejezetet a távközlési törvényt tartalmazó függelék és tárgymutató egészíti ki.

A bevezetés a híradástechnika fogalmát, történetének rövid összefoglalását és a könyv felépítését ismerteti. Ezt követi a jelek leírásával foglalkozó fejezet, melyben a determinisztikus és a sztochasztikus leírás elemeit találhatjuk meg. Jelenleg különösen fontos a mintavételezéssel és a diszkrét források kódolásával foglalkozó harmadik fejezet, melyben a mintavételezési tétellel és következményeivel foglalkoznak a szerzők, és a kódoláselmélet alapjait ismertetik. A negyedik fejezet az akusztikai alapokat: a hangot, a hallást és az elektroakusztika elemeit tárgyalja. Fénytechnikai alapokkal foglalkozik az ötödik fejezet. A hatodik fejezet ismét kiemelkedő fontosságú tárgykört, a hírközlő csatornákkal kapcsolatos alapfogalmakat tartalmazza, a másodlagos effektusok, analóg csatorna esetén a torzítások, a zaj és a visszhang, digitális csatorna esetés a hibák tárgyalásával együtt. A hetedik fejezet a hibakorlátozó kódolással foglalkozik. Rendszertechnikai szempontból logikailag helyesen következnek ezután a nyolcadik fejezetben a vezetett hullámú összeköttetések, majd a kilencedik fejezetben a sugárzott hullámok, a rádiócsatorna. A tizedik fejezet a természetes és mesterséges eredetű zajok és híradástechnikai hatásuk leírásával foglalkozik. Az eddig leírt ismereteket felhasználja és ezért került a tizenegyedik fejezetbe az analóg modulációs, majd a tizenkettedik fejezetbe a digitális modulációs eljárások leírása. A tizenharmadik fejezet a csatorna megosztását: a frekvencia-, az idő- és a kódosztást és az ezekkel rokon területeket tárgyalja. Az eddigi fejezetek alapozó ismereteket nyújtanak, innen következik az alkalmazások ismertetése. A tizennegyedik fejezet a nyilvános, kapcsolt távbeszélő hálózatok témakörét tekinti át. Mivel Magyarországon a híradástechnika legégetőbb problémája még mindig a telefon, ez és a következő két fejezet, melyek a forgalomelmélettel és a pont-pont közötti összeköttetésekkel foglalkoznak, tekinthetők a könyv súlyponti témaköreinek. A mobil hírközléssel foglalkozó tizenhetedik fejezetben olyan összeköttetésekről van szó, melyben legalább az egyik végpont mozog. Ez új problémákat vet fel, többek között a rádiócsatorna leírására és az összeköttetések szervezésére vonatkozóan. Többféle információforrás jeleinek egyidejű, azonos csatornán történő továbbításának kérdéseivel foglalkozik az integrált szolgáltatású hálózatok (ISDN) című fejezet. A klasszikusnak számító hang- és kép-műsorszórást a tizenkilencedik és huszadik fejezet ismerteti, majd az adatszórással és a műsorszétosztással találkozunk a huszonegyedik fejezetben. Itt találjuk meg a kábeles televízió-rendszerek felépítésének alapvető jellegzetességeinek leírását. Különleges alkalmazásokat találunk az utolsó három fejezetben: a rádiólokációt és a mikrohullámú aktív távérzékelést, a rádiócsillagászatot, a mikrohullámú passzív távérzékelést és a rádiónavigációt, valamint a különleges fogyasztói elektronikai alkalmazásokat, mint például a lézerlemezt és a videokamerát.

A könyv megírásának technikája is különleges volt: valószínűleg Magyarországon az első olyan könyv, amely számítógép-hálózaton készült. A könyvet három tanszék huszonkét oktatója írta. A számítógép-hálózat lehetővé tette, hogy a megírás közben egymás munkáját is eredményesen kísérhessék figyelemmel. A könyv kiváló, tematikusan egymásra épülő és a teljességet megközelítő szerkezete a főszerkesztő, Géher Károly professzor nagy szakmai tudását és kiváló pedagógiai érzékét dicséri.

A villamosmérnök és informatikus hallgatókon kívül eredményesen forgathatják a könyvet a híradástechnika területén dolgozó szakemberek is.

LADVÁNSZKY JÁNOS

TOVÁBBKÉPZÉS MENEDZSEREKNEK

Az Angliában alapított ADR (London) Ltd cég angolnyelvű szaktanfolyamokat kínál. A résztvevők többek között kommunikáció technika, tervezés, döntéshozatal, projekt menedzsment, informatikai rendszerek és menedzser továbbképzés témakörében sajátíthatnak el hasznos tudnivalókat. Az előadók nagy tapasztalattal rendelkezző, üzleti területen, valamint felsőfokú oktatási intézményekben is tevékenykedő szakemberek.

Az ADR (London) Ltd tavaly decemberben kezdte meg magyarországi szeminárium sorozatát *Változások kezelése* címmel. A szeminárium az információs technológia és telekommunikáció szerepét, az adaptív szervezeti struktúrák fontosságát, versenyhelyzet kiélesedését, a menedzsment pozícióját elemezte a jelenlegi nemzetközi politikai, szociális és gazdasági viszonyok között.

Részletesebb információkat a 00 44 171 589 8349 (tel.) vagy 00 44 171 730 3267 (fax) kérhet.

BÉRES ANTÓNIA

NEMZETI INFORMATIKAI STRATÉGIA KEZDEMÉNYEZÉSE

A MTESZ Kamarájának szervezésében 1995. február 21-én egésznapos konferenciára került sor a Nemzeti Informatikai Stratégia kialakításának kérdéseiről. A konferencián számos kiemelkedő szakértő világította meg az informatika szerepét a gazdaság, az államigazgatás, a társadalom és a mindennapi élet különféle szféráiban.

A konferenciát Havass Miklós a MTESZ elnöke és Pál László ipari és kereskedelmi miniszter nyitotta meg. Egyetértettek abban, hogy a magyar társadalom valamennyi szférájában a következő évtizedekben jelentős átalakulást fog eredményezni az informatika térhódítása. Ezt az átalakulást tervszerűen kell elősegíteni. A társadalom modernizáció nem képzelhető el informatikai program nélkül.

Néhány érdekelt szervezet és vállalkozás szakértői *Nemzeti Informatikai Stratégia, kezdeményezés* címmel tanulmányt készítettek, amely áttekinti

- a globális trendeket,
- az Európai Közösség informatikai stratégiáját,
- a informatika magyarországi helyzetét,
- az informatikai ipart Magyarországon.

és ennek alapján megfogalmaz

- célkitűzéseket és feladatokat,

meghatároz

- projekt javaslatokat.

A tanulmány legfontosabb megállapításait Szlankó János a KFKI igazgatója ismertette.

Ezután Bihari János az OMFB Tanács elnöke *Az ipari rekonstrukció és az informatika*, Kolossy Tamás SZÜV elnök *Társadalom és informatika*, Szabó Katalin BK egyetemi tanár *Gazdaság és informatika*, Horvát János *Média és informatika* címmel tartott előadást. Az előadásokat korreferátumok követték.

A stratégiát összefoglaló tanulmány fontos kérdésként tárgyalja az informatikai rendszerek létrehozásához és működtetéséhez szükséges távközlési hálózat kérdéseit. Világosan látszik, hogy az informatikai rendszerek kialakításához és tervezéséhez a távközlési hálózatok problémái is hozzátartoznak. Így, ha az informatikai stratégia alapján sikerül fejlesztési programot kidolgozni és megvalósítani, akkor a távközlési szakemberek számára is jelentős és érdekes feladatok adódnak.

A konferencia előadásait a MTESZ külön kiadványban teszi közzé. ■

A MTESZ INFORMÁCIÓS RENDSZERE

A MTESZ az elmúlt évben megkezdte egy olyan számítástechnikai bázis kialakítását, mely tagegyesületei s általában a műszaki értelmiség számára hozzáférést biztosít a hazai és külföldi információs szolgáltatások széles köréhez.

A MTESZ tíz vidéki Technika Házában, valamint egy budapesti — a Fő utcai — központban a projekt első fázisaként ún. *Információs Pultok* kerültek kiépítésre. Ezek többek között információkeresésben és elektronikus levelezésben nyújtanak segítséget. Az Információs Pultok a hazai adatbázisok mellett — az Internet hálózat lehetőségeit kihasználva — külföldi információforrásokhoz is kapcsolatot teremthetnek. ■

MESSE MÜNCHEN INTERNATIONAL

A világ vezető innovatív és alkalmazott optoelektronikai vására – a piacrajutás kulcsa

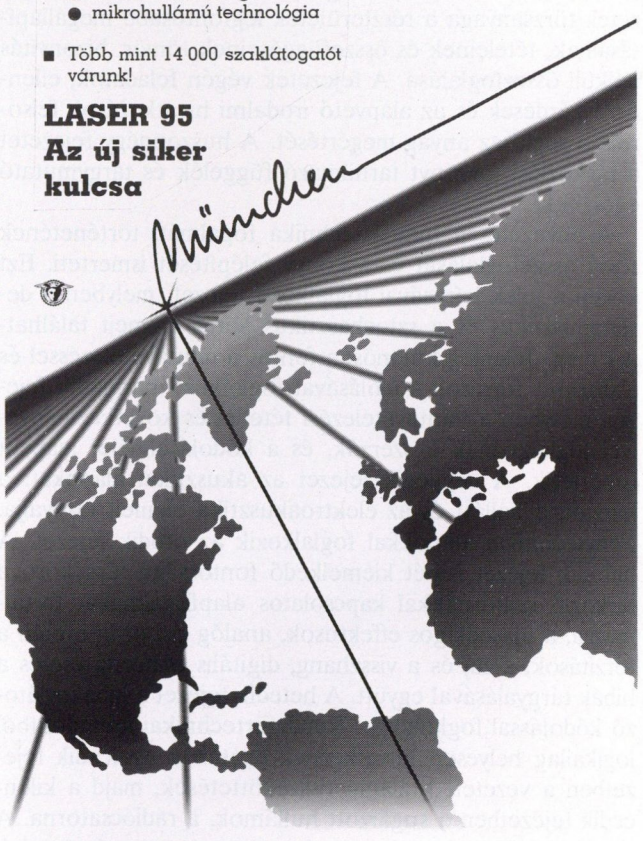
München, 1995. június 19–23.

Ön sem engedheti meg magának, hogy szakmája területén ne naprakész információval rendelkezzen! Mindenről egy helyen, a LASER 95-ön tájékozódhat!

- Több mint 580 kiállító
- több mint 24 000 nm-en bemutatja az aktuális trendet az alábbi szakterületeken:
  - a lézertechnológia és lézerrendszerek alkalmazása a termelésben, kommunikációban, környezetvédelemben, a gyógyításban és a különféle tudományágakban
  - az optikai mérés és tesztelés moduljai és rendszerei
  - optika
  - optoelektronika
  - száloptika
  - holográfia
  - ipari anyagmegmunkálás
  - szenzor-technológia
  - mikrohullámú technológia
- Több mint 14 000 szaklátogatót várunk!

12. Nemzetközi Vásár és Kongresszus

LASER 95
Az új siker kulcsa



LASER 95

Információ: Promo Kft. – 1064 Budapest, Rózsa u. 55.
Tel.: 342- 6748, 342-1148 Fax: 342-5589, 342-0973
Belépőjegyek forintért előzetes rendelés alapján itt vásárolhatók!
Szervező: Messe München GmbH, Messegelände
D-80325 München Tel.: (00-49/89) 5107-410 Fax: (00-49/89) 5107-176

MŰSZAKI INFORMÁCIÓS KÖNYVTÁR 1883 BUDAPEST

MOBIL TÁVKÖZLÉS

nemzetközi szeminárium
Budapest, 1995. október 2-3.
A Hiradástechnikai Tudományos Egyesület
és a
HÍRADÁSTECHNIKA folyóirat
rendezésében.

A szeminárium célja a mobil távközlés problémáinak elsõsorban az analóg és a digitális rádiótelefon rendszerek kérdéseinek széleskörû áttekintése, a mûszaki megoldások tárgyalása és azok értékelése. Az alapvetõ rendszertechnikai fogalmakból kiindulva ismertetésre kerülnek a tervezés a telepítés és az üzemeltetés legfontosabb kérdései.Különös figyelmet kapnak a jövõben alkalmazásra kerülõ rendszerek A szeminárium elõadásait ismert nyugati cégek képviselõi és a hazai piacon jelentõs eredményeket felmutató szolgáltatók szakértõi tartják .A szemináriumon való részvételt különösen ajánljuk olyan mérnököknek,akik új mobil távközlési szolgáltatások megvalósításán dolgoznak.

A szeminárium témakörei

Rendszertechnika
Hálózat tervezés
Szolgáltatások és tarifák
Jövõbeni rendszerek
Rádiós alkalmazások
Mobil terminálok
Adatátvitel
Bázis állomások, kapcsoló központok

A szemináriummal egyidõben kerül megrendezésre a mobil távközlési hálózatok *tervezéséhez* használt eszközöket és az *üzemeltetésre* szolgáló berendezéseket bemutató kiállítás..

A szeminárium nyelve angol, szinkron tolmácsolást biztosítunk.A szeminárium elõadásai és a kiállított tárgyak ismertetõi a JOURNAL ON COMMUNICATIONS
külön számában jelennek meg, amelyet a szeminárium résztvevõi a regisztrációnál kézhez kapnak.

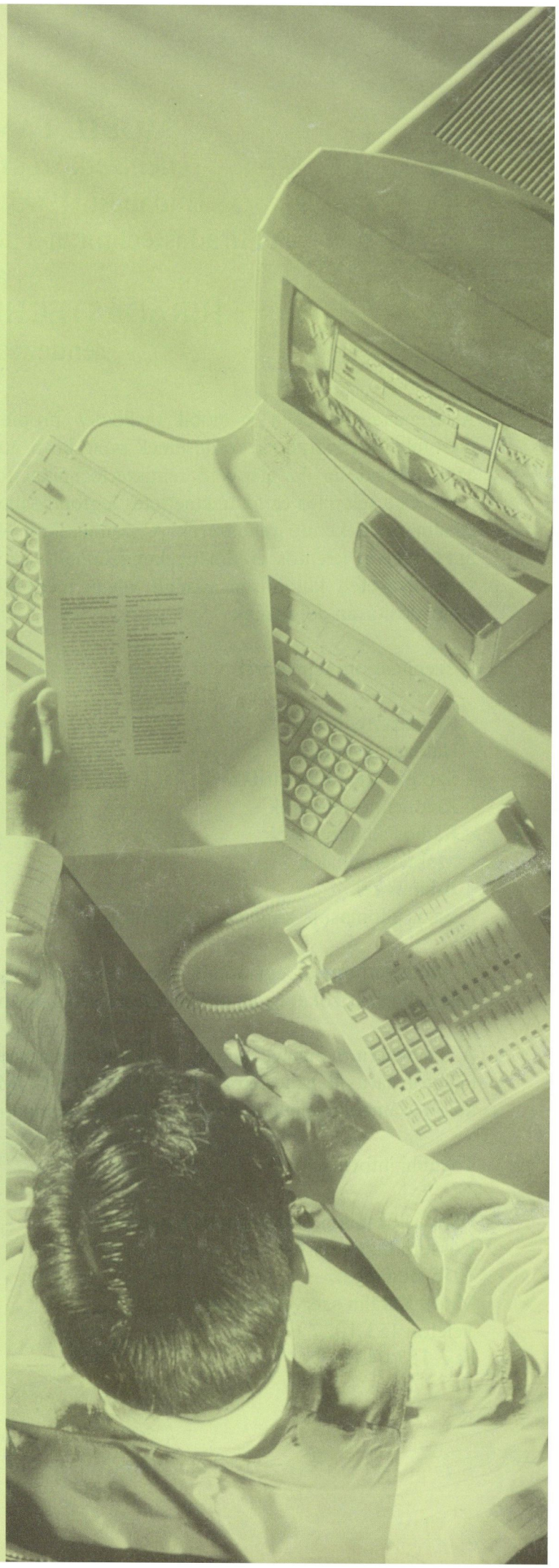
További információk

Híradástechnikai Tudományos Egyesület
Kossuth Lajos tér 6-8
1055 Budapest
Mitók Katalin szervezõ titkár
Telefon 153 1027
Fax 153 0451

SIEMENS

Az Ön szakértő partnere

1995 JUL 03

az alközponti hálózatok terén: telefonrendszeren alapuló komplett kommunikációs hálózatok tervezése, kivitelezése és szervizelése.
A hálózati rendszerek területén: vállaljuk helyi és nagykiterjedésű hálózatok létesítését (LAN, WAN, MAN), valamint strukturált kábelezést.

Bemutatókkal és szaktanácsadással várjuk Önt az IFABO '95 szakkiállításon az A pavilon 305/a standján.