



Informatikai Kar

Informatikai biztonság a DEIK-en Dr. Pintér-Husztai Andrea





Kutatócsoportunk területe:

**Kriptográfiai primitívek és protokollok tervezése,
biztonsági elemzése**

Vezető: Prof. Dr. Pethő Attila akadémikus

- Phd hallgatókkal együtt 15-20 fő kutató
- Kollégák oktatási, kutatási tevékenységet folytatnak és K+F+I projekteken vesznek részt



Informatikai Kar

- 1989-ben **Kriptográfia** kurzus programtervező matematikusoknak
- Egyik első kriptográfia kurzus Magyarországon
- Folyamatosan bővültek a kriptográfia területéhez kapcsolódó kurzusok: kriptográfiai protokollok, adatbiztonság stb.

- 2000-es évek végén **Informatikai biztonság alapjai** kurzus: fizikai, ügyviteli, logikai/algorithmusos védelem
- Elmúlt években: IT biztonság, Webes biztonság (OWASP Top 10), Etikus hackelés, Blokklánc technológiák



- 2022-ben megalakult a **Hajós György Adattudományi Szakkollégium**, Adatbiztonság műhely
- Több DETEP-es hallgató
- Számos TDK dolgozat
- OTDK
 1. helyezett: Oláh Norbert, Kovács Szabolcs Zoltán
- **Informatikai Tudományok Doktori Iskola**

Elméleti számítástudomány, adatvédelem és kriptográfia program
7 fő szerzett a témában PhD fokozatot, egy folyamatban

- **Kriptográfiai primitívek**

- Matematikai konstrukciók hash függvényekre és véletlenszám generátorok, FPGA és korlátozott erőforrású IoT eszközökre (Pethő Attila, Herendi Tamás, Major Roland, Padányi Viktória)
- Identitás alapú kriptográfiai algoritmusok, CryptID programcsomag, szabadalom IoT környezetre (Pethő Attila, Vécsi Ádám)
- Automataelmélet alapú kriptográfia (Dömösi Pál, Horváth Géza)



- **Kriptográfiai protokollok tervezése, elemzése**

Pethő Attila, Huszti Andrea, Oláh Norbert, Kovács Szabolcs Zoltán, Jámbor Zsanett

- Anonimitás (e-szavazás, e-vizsgáztatás, e-fizetés), anonim üzenetszórás (VANET),
- Felhasználók hitelesítése (felhő, okosotthon),
- Kiszámíthatósági biztonság és kalkulus alapú technológiák alkalmazása



Informatikai Kar

- Debreceni InfoPark Kooperációs Kutató Központ
Intelligens Közösségi Kártya (egyszerűbben Városkártya)
- 2005-2007
- Lokális és regionális tartalomipar fejlesztése, innovatív
értéknövelt szolgáltatás keretrendszerének kialakítása
adatvagyonok hasznosítására - TARIPAR3 (e-kormányzati
tartalomszolgáltatás mobiltelefonos megoldások
biztonsága) – 2008-2011
- Hiteles és anonim vizsgajavítási rendszer, NetLock Kft. -
2008-2011
- HU-MATHS-IN (Hungarian Service Network for
Mathematics in Industry and Innovations) (kölcsonös
felhasználó hitelesítési rendszer) - 2017-2021



Informatikai Kar

- SETIT - IoT rendszerek biztonságát növelő technológiák (Nemzeti Kiválósági Projekt), álvéletleszám-generátorok, felhasználó hitelesítés, szűrő – 2018-2022
- Tématerületi Kiválósági Program Járműipari projekt, anonim üzenetszórás VANET-re – 2019-2022
- IoT eszközök biztonsági minősítése, Infokommunikációs és Információtechnológiai Nemzeti Laboratórium (NBSZ, Alverad), biztonsági ajánlás IoT ökoszisztémára – 2022-2023
- EDIH (European Digital Innovation Hubs) - 2022-2025
KKV-k digitalizációjának elősegítése



Informatikai Kar

Köszönöm a figyelmet!

