**11 iunie ora 8-9:**

1. **Implement Hastad Attack on RSA**

Traila Alexandra (410)+Ursatanu Andreea(406)

1. **Implement a padding oracle + Bleichenbacher attack on RSA**

Cernat Marina (406)+Iolanda Banu (406)

1. **Practical attack on RSA used on smartcards**

Cristian Cojocaru (407)

1. **Linear cryptanalysis of DES with 4 rounds**

Murarasu Renata (407).

**11 iunie ora 9-10:**

1. **Barkan-Biham-Keller attack on A5/1**

Voica Lucian, Mereuta Maria(406)

1. **Petrovici-Fuster-Sabater attack on A5/2**

Cristiana Dumitru, Stancu Adriana (410)

1. **Implement Wang attack on MD4**

Mihai Gheorghe(407)

1. **Break the truncated Linear Congruential Generator**

Victorita Ionela Tache(406) +Vlad Cichirau

**11 iunie ora 10-11:**

1. **Implementare unui model de incredere ierarhic intr-un LAN folosind semnaturi RSA**

Roman Teodora, Taddei Giulia(406)

1. **Implementare SYN Flood Attack intr-un LAN + metode de detectie si respingere ale atacului**

Robu Bianca, Banica Bianca (410)

1. **Spoofing Attack: Implementarea unui atac de tipul MITM intre doua masini din acelasi LAN. Metode de detectie si respingere**

Ceausescu Ciprian, Ionita Matei Marius (406)

1. **Spoofing attack pe WiFi**

Steriopol Andrei(408)+Alexandra Socarici(406)

**11 iunie ora 11-12:**

1. **Fragmentation Attack on WEP**

Ripanu Georgiana, Marin Victor(406)

1. **Offline dictionary attack on the WPA2 4-way handshake protocol**

Ghita Tudor, Ibis Alexandra(410)

1. **Implement + Break Mersenne Twister RNG**

Serban Marius(407)+Nasui Laurentiu(406)

1. **Implement Verifiable Shamir Secret Sharing Scheme ( Feldman's scheme)**

Mihai Iacob, Ianculescu Alexandru George(408)

***Mod de evaluare:***

1. **Continut proiect: 1 punct**
2. **Redactare si evaluare cod sursa: 1 punct**
3. **Mod de prezentare: 1 punct**

Forma scrisa a proiectului (doc, docx, pdf), referintele si codul sursa (*nu executabil*) scris in python sau C (variante) vor fi descarcate pe calculatorul din sala 220 in momentul prezentarii (sau pot fi trimise prin email la aadrian@gmail.com).

**La susţinerea din 11 iuniie:**

* Prezentarea este de maxim 15’ (slide-uri de preferinţă).
* Minim 5 minute vor fi alocate prezentarii aplicatiei.
* Voi aprecia in special:

1. Gradul de asimilare al subiectului
2. Aplicatie (functionalitate, complexitate, cod sursa inteligibil)

Se pot acorda suplimentar pana la 0.5 puncte pentru idei originale (teoretice sau implementari).