***Proiecte***

1.Fragmentation Attack on WEP

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

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

4. Petrovici-Fuster-Sabater attack on A5/2

5.Implement + Break Mersenne Twister RNG

6. Break the truncated Linear Congruential Generator

7.Implement a padding oracle + Bleichenbacher attack on RSA

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

9. Implement Hastad Attack on RSA

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

11. Practical attack on RSA used on smartcardes

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

13. Spoofing Attack: Implementarea unui atac de tipul MIM (Meet In the Middle) intre doua masini din acelasi LAN. Metode de detectie si respingere

14. Differential cryptanalysis of DES with 4 rounds

15. Linear cryptanalysis of DES with 4 rounds

1.Fragmentation Attack on WEP

<https://www.aircrack-ng.org/doku.php?id=fragmentation>

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

<https://security.stackexchange.com/questions/66008/how-exactly-does-4-way-handshake-cracking-work>

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

<http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2006/CS/CS-2006-07.pdf>

4. Petrovici-Fuster-Sabater attack on A5/2

<https://eprint.iacr.org/2000/052.pdf>

5.Implement + Break Mersenne Twister RNG

http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/ARTICLES/mt.pdf

<http://cryptopals.com/sets/3/challenges/23>

6. Break the truncated Linear Congruential Generator

<https://www.math.cmu.edu/~af1p/Texfiles/RECONTRUNC.pdf>

7.Implement a padding oracle + Bleichenbacher attack on RSA

<http://archiv.infsec.ethz.ch/education/fs08/secsem/bleichenbacher98.pdf>

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

(in fisierul 1\_PKI.pdf)

9. Implement Hastad Attack on RSA

<https://crypto.stanford.edu/~dabo/papers/RSA-survey.pdf>

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

<http://www.cs.huji.ac.il/~ns/SS.pdf>

<https://crypto.stackexchange.com/questions/6637/understanding-feldmans-vss-with-a-simple-example>

11. Practical attack on RSA used on smartcardes

<https://crocs.fi.muni.cz/_media/public/papers/nemec_roca_ccs17_preprint.pdf>

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

13. Spoofing Attack: Implementarea unui atac de tipul MIM (Meet In the Middle) intre doua masini din acelasi LAN. Metode de detectie si respingere

14. Differential cryptanalysis of DES with 4 rounds

<http://www.cs.bc.edu/~straubin/crypto2017/heys.pdf>

15. Linear cryptanalysis of DES with 4 rounds

<http://www.cs.bc.edu/~straubin/crypto2017/heys.pdf>