INF 247, spring 2018
Igor Semaev
December 6, 2017

The course is on basic cryptanalytic techniques for symmetric ciphers. The course mostly follows the lecture notes to be distributed before it starts. Prerequisites include basic algebra and probability theory, though necessary notions and results will be explained. Also it is good to have attended INF240 taught at the Department of Informatics, University of Bergen or any other introductory course in cryptography.

1 Cryptanalysis of historical ciphers.

1. General definition of a cryptographic system. Symmetric-key and public-key encryption, classes of cryptanalytic attacks.
2. Substitution cipher, cryptanalysis, unicity distance of a simple substitution cipher.
3. Homophonic cipher, cryptanalysis.
5. Index of coincidence.
6. Transposition cipher, cryptanalysis.
7. Running-key cipher.
8. Hagelin cipher, idea of the cryptanalysis.

2 Stream ciphers.

1. Cryptanalysis at depth.
2. Synchronous and self-synchronizing stream ciphers.
3. Linear feedback shift registers, characteristic polynomial and minimal polynomial of a matrix. Period of an irreducible polynomial.

5. Constructing primitive polynomials modulo 2.


7. Linear complexity profile of a sequence, properties.


10. Time-memory trade off for a filter generator.

11. Solving nonlinear algebraic equation via linearization and extended linearization, algebraic attacks for stream ciphers.


15. Affine approximation attack, complexity.


17. Boolean bent-functions, criterion and examples.


19. Combining LFSRs, minimal period of the output. Linear complexity.

20. Correlation attack against a combiner, complexity. Probability of errors, necessary amount of the key-stream.


22. Piling-up lemma. The best affine approximation for the XOR of Boolean functions in independent variables.


25. 2-adic expansion of rational numbers. Feedback with Carry Shift Registers.


3 Block ciphers.

1. Modern block ciphers, round function and key schedule. Feistel ciphers and Substitution Permutation Networks.

2. Meet in the Middle attack. Time and memory complexity.

3. Linear approximations of \( S \)-boxes. Computing the most biased linear approximations with Walsh-Hadamard transform.

4. Linear Cryptanalysis for round block ciphers. Necessary amount of plaintext/cipher-text blocks.

5. Linear Cryptanalysis of DES.

4 Comments

The attendance to the lectures and group sessions is mandatory, up to four classes may be missed for reasons that include personal and professional commitments and personal/family emergencies. Any student who exceeds the four class limit may not be admitted to the exam. Weekly exercises will be distributed separately upon some necessary theory is studied. There should be three mandatory exercises, the deadline of handing them in is absolute. The students can get up to 30% of the final grade with mandatory exercises: up to 10% for each, the rest 70% comes from the written exam.