Cryptography

Lab 4 – 7 V

Implement one...

A (Algorithmic track)

Part 1 (3 points) Implement Merkle-Hellman [3] cryptosystem (use gmp-like library to support large numbers). Implement $\langle \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec} \rangle$ functions.

Part 2 (7 points) Implement Shamir's attack [4] on the system.

B (Algorithmic/security track) Implement Merkle-Puzzle cryptosystem `http://www.merkle.com/1974/PuzzlesAsPublished.pdf` (read the story behind: `http://www.merkle.com/1974/`). Run your system for $N = 2^n$, where $n = 24, 32, 40$ and compute and/or estimate space and time requirements. You need to prepare a presentation of the system with $n = 24$ (at least).

C (Security track) Use [1] to implement a linear attack [2] on a given SPN.

Part 1 (5 points) Implement a program which finds the best linear approximations for a given S-box. Are you able to find approximations of S-boxes $S : \{0,1\}^n \to \{0,1\}^m$ for $(m, n) = (8, 8)/(8, 16)/(8, 32)/(16, 64)$?

Part 2 (5 points) You are given an SP-network. Estimate how many pairs of known-plaintext/ciphertext do you need to decrypt another message.

During a class you will be given a set of plaintexts and corresponding cipertexts, your goal will be to decrypt another message.

References

[1] Howard M Heys. A tutorial on linear and differential cryptanalysis. *Cryptologia*, 26(3):189–221, 2002.

[2] Mitsuru Matsui. Linear cryptanalysis method for des cipher. In *Advances in Cryptology—EUROCRYPT'93*, pages 386–397. Springer, 1994.

[3] Ralph Merkle and Martin E Hellman. Hiding information and signatures in trapdoor knapsacks. *Information Theory, IEEE Transactions on*, 24(5):525–530, 1978.

[4] Adi Shamir. A polynomial time algorithm for breaking the basic merkle-hellman cryptosystem. In *Advances in Cryptology*, pages 279–288. Springer, 1983.