Worksheet 2 (due Sunday June 19, 11:59 pm)

Course 01435: Practical Cryptanalysis
June 2016

Andrey Bogdanov
anbog@dtu.dk

Introductory Remarks

All comments from worksheet 0 apply.

Meet-In-The-Middle Attacks

Recommended Reading

R.C. Merkle and M.E. Hellman. On the Security of Multiple Encryption, 1981.

P.C. van Oorschot and M.J. Wiener. A know-Plaintext Attack on Two-Key Triple Encryption, 1990.

Exercises

Exercise 12 (P): DES is only using a key size of 56 bits which makes it vulnerable to bruteforce attacks. It was suggested to use two 56 bits keys and double encryption to increase the keyspace and increase the resistance against those attacks, called *2DES*. The encryption is done in the following way

$$c = E_{k_2}(E_{k_1}(m))$$

- Give the complexity for an exhaustive key search.
- Can you apply a meet-in-the-middle attack to reduce the complexity?
- Would the system be more secure when using $c = E_{k_2}(E_{k_1}(E_{k_1}(m)))$.
- Would the system be more secure when using $c = E_{k_1}(E_{k_2}(E_{k_1}(m)))$.

Exercise 13: DES has a blocksize of 64 bits. When using 2DES with two 56-bit keys:

- What is the expected number of key pairs k_1, k_2 such that $E_{k_1}(m_1) = D_{k_2}(c_1)$?
- What is the expected number of key pairs k_1, k_2 such that $E_{k_1}(m_1) = D_{k_2}(c_1)$ and $E_{k_1}(m_2) = D_{k_2}(c_2)$?

Exercise 14: Another mode 3DES which is still used in practice works uses three 56-bit keys and encrypts a message in the following way

$$c = E_{k_3}(D_{k_2}(E_{k_1}(m)))$$

- Give the complexity for an exhaustive key search.
- Can you still apply a meet-in-the-middle attack?

Exercise 15 (P): In this excercise you should implement a meet-in-the-middle attack on a simple block cipher. The block cipher operates on 16-bit blocks and is based on the Feistel structure (see Figure 1). It uses 8-bit independent round keys k_i and S is the 8-bit AES S-Box. See the C code (`mitm.c`) on CampusNet.

- Implement a meet-in-the-middle attack on this cipher and recover the key.
- Given the following plaintext/ciphertext pairs:

Rounds	Plaintext	Ciphertext
4	`0000`	`4748`
	`1234`	`3cf6`

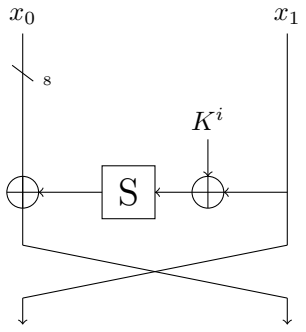

Figure 1: One round of the feistel cipher used in this exercise, where S is the AES S-Box.