Programming Project 2

Course 01435: Practical Cryptanalysis
June 2016

Andrey Bogdanov
anbog@dtu.dk

1 Remarks

- hand in via campusnet before Wednesday, June 22, 11:59 pm (no print out necessary)
- work alone or in groups of up to 4 people
- free choice of programming language
- the code should be well-structured and contain a sufficient amount of comments such that it can be understand be an external programmer
- some written documentation of the code is necessary and you have to be able to explain every single detail when asked
- it is your responsiblity to be able to demonstrate your programme at the colloquium (make sure that a computer is available your programme runs on etc)

Programming Project (P)

In this excercise your task is to implement a meet-in-the-middle attack on double-DES.

Encryption Scheme DES is rather vulnerable against bruteforce attacks as it only has an effective key size of 56 bits. As a fix to this problem it was suggested to use double encryption with a 112-bit key (see Figure 1). In this excercise you will evaluate the security of this construction.

Programming Task For this task you will use a reduced size for the keys. The two keys k_1 and k_2 are 20-bit keys padded with 0 to get a 56-bit key.

- Find an implementation of DES in the programming language of your choice.

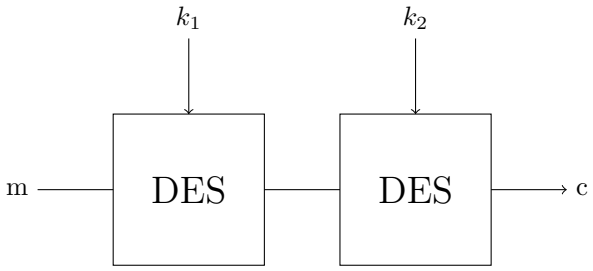

Figure 1: Double DES

- Choose two random 20-bit keys k_1, k_2 and pad them with zeroes to get a key for double-DES.
- Encrypt a plaintext of your choice using double-DES and your key (consisting of two chunks 20 bits each).

Key Recovery Your task is now to recover the secret keys k_1 and k_2 from your plaintext/ciphertext pair using a meet-in-the-middle attack.

- Implement a meet-in-middle attack on this scheme to retrieve k_1 and k_2.
- How long does it take to recover the key?
- What is the effective key length of this scheme?
- Give the memory/time complexity for the attack.