Biomedical Security

Assignment Set 1

6-9 2018

- Due by 13-9 2018.
- Send your answers in a pdf by e-mail to erwin@liacs.nl
- Use as filename: **<your student number>_<your name>_iBS_Assignment_set_01.pdf**

1. Assume you have a software implementation for DES, and a software implementation for a military Enigma. The plaintext crypto-text pairs (M, C_{DES}) and (M, C_{Enigma}) are given. How much easier/harder is it to find the used secret key K_{DES} than it is to find the used secret key K_{Enigma}? To answer this question verify the number of settings for a military Enigma mentioned in the slides.

2. Give a short explanation of Differential Cryptanalysis? Is DES resilient to a Differential Cryptanalysis attack?

3. How long would it take on a Titan V GPU to find the secret key when you execute a known plaintext attack on DES?

4. Why can you not use the secret key of the ONE-TIME PAD twice?

5. Assume Alice wants to use ONE-TIME-PAD to encrypt a message that can be of arbitrary length. Alice wants to send the encrypted message to Bob and Bob should be able to decrypt it. Describe a scheme that would enable this. Give a (short) critical review of your solution.

6. Give pseudocode for an algorithm that finds and stores all the primes smaller than a given integer N > 0. N should be a parameter of your algorithm. What is the time and space complexity of your algorithm?