

Biomedical Security

Assignment Set 1

1-4 2021

- Due by 12-4 2021.
 - 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 AES, and a software implementation for a military Enigma. The plaintext crypto-text pairs (M, C_{IDEA}) and (M, C_{Enigma}) are given. How much easier/harder is it to find the used secret key K_{IDEA} 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, and consider all possible key-sizes of AES.
 2. Give a short explanation of Differential Cryptanalysis? Is BLOWFISH resilient to a Differential Cryptanalysis attack?
 3. How long would it take on a RTX 3090 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? Explain.
 5. Assume Alice wants to use ONE-TIME-PAD to encrypt a Secret Key that can be of arbitrary length. Alice wants to send the encrypted Secret Key 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. Read the slides 'A Short Introduction to Number Theory'. Note: The slides can be found in the pdf of the first lecture.
 7. 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?