Basics of cryptography (CE057)

March 28, 2023

Assignment 3

Name: [Your name]
Student Number: [XXXXXXXXX]

Due date: 28 April 2023, 23:59 (GMT+3:30)
In this assignment you are going to answer questions related to the Data Encryption Standard (DES) and Triple-DES.

- By turning in this assignment, I declare that all of this is my own work.
- This is an individual assignment. Please mention your name and student number in submission. You have to hand in a **SINGLE** document (PDF) with your answers and your source code (if any). **Also, be aware that any form of plagiarism will not be condoned.**
- Your code must be written in C, Java, Python or Golang, although we encourage you to use Python for simplicity.
- Pose your questions on the Telegram group, so that your fellow students can also read them.
- **Explain and motivate all your answers!**

Problems (30 points)

(a) What is DES? How does it work? Explain why the number of rounds in DES is 16?

(b) Explain the differences between a block cipher and a stream cipher?

(c) Why was DES replaced by AES?

(d) Is there any way to recover an encrypted message if we don't know the key or initialization vector used during encryption?

(e) What's the difference between DES and 3DES?

(f) What are the different types of attacks that can be performed on DES?

(g) What are the two best known general attacks against block ciphers?

Computer Assignment (70 points)

How can you use the Data Encryption Standard (DES) algorithm for image encryption and decryption? Describe the steps involved in encrypting and decrypting an image using DES. Additionally, explain why using ECB mode for DES encryption is not secure, and suggest an alternative mode that provides stronger security? Finally, provide a code snippet in Python (or any) that demonstrates how to encrypt and decrypt an image using 3DES.