Basics of cryptography (CE057)

February 13, 2023

Assignment 1

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

Due date: 1 March 2023, 23:59 (GMT+3:30)
In this assignment you are going to answer questions related to historical ciphers and information theory.

- 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!**

Introduction to Cryptography (24 points)

(a) Consider a group of 20 persons who want to use symmetric-key cryptography to create pair-wise secure communications.How many keys need to be exchanged in total?

(b) You will consider the relation between passwords and key size. For this purpose we consider a cryptosystem where the user enters a key in the form of a password.
1. Assume a password consisting of 8 letters, where each letter is encoded by the ASCII scheme (7 bits per character, i.e., 128 possible characters). What is the size of the key space which can be constructed by such passwords?
2. What is the corresponding key length in bits?
3. Assume that most users use only the 26 lowercase letters from the alphabet instead of the full 7 bits of the ASCII-encoding. What is the corresponding key length in bits in this case?
4. At least how many characters are required for a password in order to generate a key length of 128 bits in case of letters consisting of
a. 7-bit characters?
b. 26 lowercase letters from the alphabet?

Classical Systems - Decrypt (46 points)

In this exercise, you are given several ciphertexts originating from classical systems. For each ciphertext, you need to answer the following questions:

- Which encryption scheme was used?
- What was the original plaintext message?
- What was the encryption key?

Or explain why it is not possible to decipher it.

(a) Consider the ciphertext:
”ZRPHQ, OLIH, DQG IUHHGRP!”

(b) Consider the ciphertext:
”JOVJVSHAL DHZ PUCLUALK MVBY AOVBZHUK FLHYZ HNV PU HZTHSS CPSSHNL PU OVUKBYHZ HUK OHZ AOYPCLK LCLY ZPUJL”

(c) Consider the ciphertext:
The ciphertext is available in ”permutation cipher.txt”

(d) Find the key for the following Vigenère-ciphertext and explain your approach.
Hint: You should subtract 1 from the estimator of the keylength you obtained from this ciphertext.
The ciphertext is available in ”vigenère cipher.txt”

(e) Hill cipher is a polygraphic substitution cipher based on linear algebra. Using this algorithm we encrypt plain text see in below. Let’s guess the key.
Plain text = [5 17, 8 3]
Cypher text = [15 16, 2 5]

Classical Systems - Encrypt (30 points)

(a) Encrypt the given plain text using mentioned algorithms and key. (please ignore the white space)
plain text = This is a secret message.

- Shift cipher algorithm, k = 8
- Affine cipher algorithm, k = (5, 21). Is it possible to encrypt this plain text using this algorithm? explain.
- Playfair cipher
- Vigenere cipher, k = (8, 2, 10, 7, 25, 6)