TAMPERE UNIVERSITY – DEPARTMENT OF COMPUTING SCIENCES

Security Protocols: Helping Alice and Bob to Share Secrets (COMP.SEC.220)

Tutorial 1: Introduction to Cryptography

Antonis Michalas antonios.michalas@tuni.fi
Mindaugas Budzys mindaugas.budzys@tuni.fi
Hossein Abdinasibfar hossein.abdinasibfar@tuni.fi

August 19, 2024

SUBMISSION DEADLINE: 09.09.2024 AT 23:00

Tutorial Description

Welcome to the lab sessions for the Security Protocols course. For today's lab exercise, you will have the opportunity to implement your first set of cryptosystems. You will be tasked with building and analyzing the Caesar, Double Caesar and Affine ciphers.

EXERCISE 1 – CAESAR CIPHER

Julius Caesar used a simple Substitution Cipher to communicate with his troops. He used a very simple rule that required that each letter be replaced with another letter from the set of alphabets. He substituted each letter with the letter that is 3 places ahead in the set of alphabets, so that "a" was replaced with "d", "b" with "e" and so on. As is described in lecture 1 of the course, there are several variations of the Caesar's cipher. The simplest one, Shift Cipher, requires a user to first pick a shift number K and then do the mapping. Hence, instead of substituting each letter by the letter that is 3 places ahead as described in the original cipher, the user substitutes a letter with another letter that is K places ahead. Therefore, if $K = 5$, the user replaces with the letter 5 places ahead ("a" is replaced with "f").

TASK 1: What is the keyspace for the Caesar Cipher. Is it possible to implement a brute force attack on this cipher or not?

TASK 2: Implement this version of Caesar's cipher (both encryption and decryption). First, a user should be prompted to enter the shift number K (how would you solve the problem of an invalid K). Subsequently, the user should be given the option to decrypt or encrypt a message. The user should be prompted to input the plaintext (or the ciphertext – depending on the selected mode) to be encrypted or decrypted. The program, on successful run, should output a valid ciphertext or plaintext depending on the selected operation mode.

- What is considered to be an invalid K?
- Implement a simple timer to measure the encryption and decryption times. What are your observations?

TASK 3: In this task, you are to break the Caesar's cipher you implemented in Task 2. To do so, you are required to write a program that will do the following:

- Read the ciphertext "IYE RKFO NYXO GOVV DY VOKBX DRSC DOMRXSAEO. LED DRSXQ GSVV QOD WYBO NSPPSMEVD - KNWSX";
- Calculate all possible keys for Caesar's cipher;
- Using each calculated key, attempt to decrypt the given ciphertext;
- Output all possible keys along with the corresponding decrypted message. What is the original message?
- How long does your program take to recover the encryption key and the original message?

EXERCISE 2 – DOUBLE CAESAR CIPHER

Alice wishes to communicate securely with her friend Bob. However, Alice and Bob only know how to use the Caesar's cipher. Alice argues that "Caesar's cipher is not secure enough". Therefore, they decide to use an apparently improved variation of the Caesar's cipher. Alice and Bob agree to encrypt their messages with a Caesar cipher of shift 13, and then encrypt the generated ciphertext with a shift of 9 (this is referred to as a Double Caesar's cipher).

1. Using the program you created in Exercise 1: Task 2, implement the Double Caesar's cipher described above (both encryption and decryption);
2. Decrypt the ciphertext "PDA BENOP NQHA KB BECDP YHQX EO UKQ ZKJ'P PWHG WXKQP BECDP YHQX". In which movie was the plaintext used?
3. Is it more secure? If so, is it considered *fully secure*?
4. What can you generally observe by using this double encryption?
5. Compared to original Caesar's cipher, is there any performance drop off?

EXERCISE 3 – AFFINE CIPHER

After a considerable amount of research, Bob comes across the Affine cipher as an alternative cipher to use to communicate with his friends. In this cipher, a letter is mapped to its equivalent numerical value, encrypted with a simple mathematical function, and converted back to a letter. In a simple implementation of this cipher, each letter of the alphabet is mapped to an integer in the range 0 - 25 (the size of the english alphabet). The 'key' consists of 2 numbers, 'a' and 'b'. The encryption process is given by:

$$E(x) = (ax + b) \mod m$$

where x is the numerical value of the letter to be encrypted and m is the size of the keyspace (26). The decryption process is given by:

$$D(x) = c(x - b) \mod m$$

where c is the modular multiplicative inverse of a. Use table 1 to assist you.

1. Using the keys, a = 7 and b = 5, encrypt the plaintext "aliceandbob";
2. How secure is the Affine cipher as compared to the original Caesar's cipher?

3. Using the keys, a = 11 and b = 2, decrypt the ciphertext "MDS CTMZU MDS CTMZU".

a	1	3	5	7	9	11	15	17	19	21	23	25
c	1	9	21	15	3	19	7	23	11	5	17	25

Table 1: Modular Multiplicative Inverses of mod 26

EXERCISE 4 – FREQUENCY ANALYSIS

Frequency Analysis is a well known technique for cracking ciphers. In this approach, we observe the frequency with which a letter or alphabet appears in the ciphertext. In theory the most common letters in a ciphertext will correspond to the most common letters in the plaintext. The most common letters in the plaintext are likely to be the most common letters in the language (letters by frequency of appearance in English can be found online). Now your task is to utilize frequency analysis to decrypt the following ciphertext (Hint: Check this link – Frequency Analysis)

"FGWGRN OL UGFFQ IOZ QL IQKR QL SOYT, WXZ OZ QOF'Z IGV IQKR NGX EQF IOZ. OZ'L IGV IQKR NGX EQF UTZ IOZ QFR ATTH DGCOFU YGKVQKR. OZ'L IGV DXEI NGX EQF ZQAT, QFR ATTH DGCOFU YGKVQKR. ZIQZ'L IGV VOFFOFU OL RGFT." OF VIOEI DGCOT VQL ZIOL JXGZT LQOR, VIG LQOR OZ QFR ZG VIGD VQL IT LHTQAOFU ZG? IOFZ: Q SGFU KXFFOFU LTKOTL YGK WGBOFU

1. What is the decrypted message from the ciphertext above?;
2. What do you think are the most common letters in the above cipher? Is it different from the most common letter in the english language?;
3. What do you think are the least common letters in the above cipher? Is it different from the least common letter in english language?
4. What are the answers to the questions in the decrypted message?
5. How long did it take you to crack the cipher? Do you think this is a secure approach to encrypting messages?