TTKS0600, Encryption Techniques and Systems, Lecture assignment 1

Reichardt Roman

Slingerland Mark

# 1 Review questions

**List and Briefly define the three key objectives of computer security.**

* Confidentiality: Only people with proper authorization have access to the information.
* Integrity: Data must not be tinkered with or deleted by unauthorized individuals.
* Availability: Ensuring constant and reliable access to the information.

**List and Briefly define categories of passive and active security attacks.**

* **Passive**
  + Release of message contents: Publication of declassified information.
  + Traffic analysis: Intercepting data and analyzing its contents rather than changing it.
* **Active**
  + Masquerade: Using a fake identity to gain access to a system.
  + Replay: repeating or delaying a data transmission.
  + Modification of messages: Changing the contents of a data transmission.
  + Denial of Service: an interruption in an authorized user’s access to a computer network.

**What are the essential ingredients of a symmetric cipher?**

* Plaintext
* Encryption algorithm
* Secret key
* Ciphertext
* Decryption algorithm

**What are the two basic functions used in encryption algorithms?**

* Substitution
* Transposition

**How many keys are required for two people to communicate via a cipher?**

One

**What is the difference between a block cipher and a stream cipher.**

The way in which the plaintext is processed. Block cipher processes the input one block at a time. And stream cipher processes the input continuously, so one element at a time.

**What are the two general approaches to attacking a cipher?**

* Cryptanalysis
* Brute-force attack

**List and briefly define types of cryptanalytic attacks based on what is known to the attacker?**

* Ciphertext Only
  + Besides the encryption algorithm the attacker also knows the transmission contained ciphertext.
* Known plaintext
  + Besides the encryption algorithm the attacker also knows the transmission contained ciphertext and one or more plaintext-ciphertext pairs formed with the same secret key.
* Chosen Plaintext
  + The Encryption algorithm
  + The ciphertext
  + Plaintext message chose by cryptanalyst, together with its corresponding ciphertext generated with the secret key.
* Chosen Ciphertext
  + The Encryption algorithm
  + The ciphertext
  + Ciphertext message chose by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key.
* Chosen text
  + The Encryption algorithm
  + The ciphertext
  + Plaintext message chose by cryptanalyst, together with its corresponding ciphertext generated with the secret key.
  + Ciphertext message chose by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key.

**What are two problems with the one-time pad?**

* Any heavily used system might require millions of random characters on a regular basis.
* For every message to be sent, a key of equal length is needed by both sender and receiver.

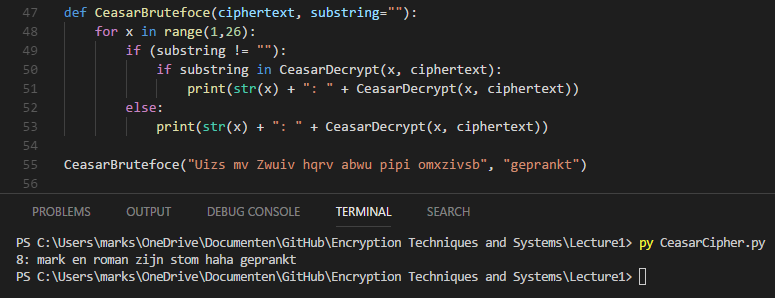
**What is steganography and what are the differences between encryption and steganography?**

Steganography is the practice of concealing information within data. The difference is that steganography does contain plaintext instead of using an encryption algorithm to create ciphertext.

# 2 Caesar Cipher

### 2.1 Encrypt & Decrypt

### 2.2 Caesar Cipher bruteforce

Code for optional word

# 3 Playfair Code

## 3.1 Construct a Playfair matrix with the key largest

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L | A | R | G | E |
| S | T | B | C | D |
| F | H | I/J | K | M |
| N | O | P | Q | U |
| V | W | X | Y | Z |

## 3.2 Construct a Playfair matrix with the key occurrence

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| O | C | U | R | E |
| N | A | B | D | F |
| G | H | I/J | K | L |
| M | P | Q | S | T |
| V | W | X | Y | Z |

## 3.3 Encrypt message: “Must see you over Cadogan West. Coming at once”

MU ST SE EY OU OV ER CA DO GA NW ES TC OM IN GA TO NC EX

UZ TB DL GZ PN NW LG TG TU ER OV LD BD UH FP ER HW QS RZ

## 3.4 Encrypt message: “Must see you over Cadogan West. Coming at once”. Using Playfair matrix from 3.1

MU ST SE EY OU OV ER CA DO GA NW ES TC OM IN GA TO NC EX

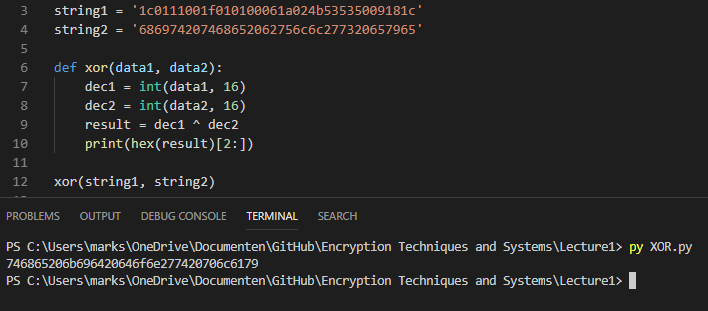
UZ TB DL GZ PN NW LG TG TU ER OV LD BD UH FP ER HW QS RZ

## 3.5 Compare encrypted messages of 3.3 and 3.4. Why did it happen?

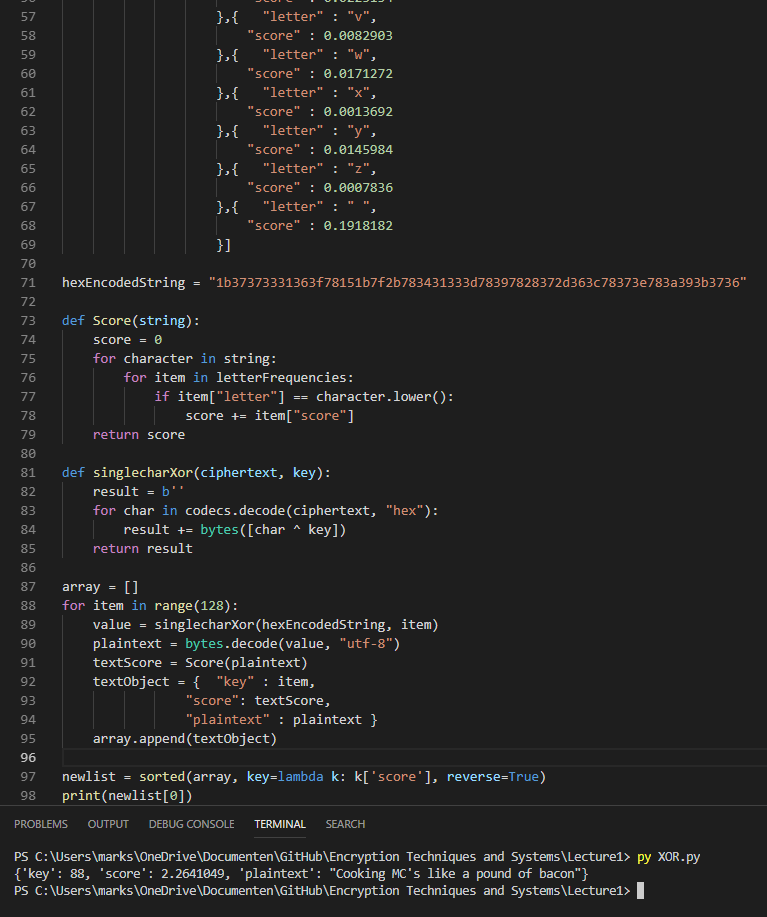
The messages are the same, because the columns and rows stills contain the same characters in the same sequence.

# 4 XOR

### 4.1 Cryptopals set 1 challenge 2



### 4.2 Cryptopals set 1 challenge 3



# General comments about assignment

The assignment in general was interesting but the sudden steepness in difficulty made assignment 4.2 quite challenging.

We are quite accustomed to pair programming, so we applied this proven method to this assignment, decreasing the possibility of bad code. We brainstormed together and applied continuous testing and debugging.