CMPS 485 - Computer Security - Fall 2018
Homework 1

You need to submit this homework as a Word document to your GitHub repository.

1. [3 pts] You intercepted a message from a spy that was encoded using a one-time pad:
   WPGUC LV SUEI TGNKNC CU WFBLP GSB FESHMKGH

   Later, you find out that the plaintext for this message is:
   TAMIM AL MAJD SYMBOL OF PRIDE AND DEFIANCE

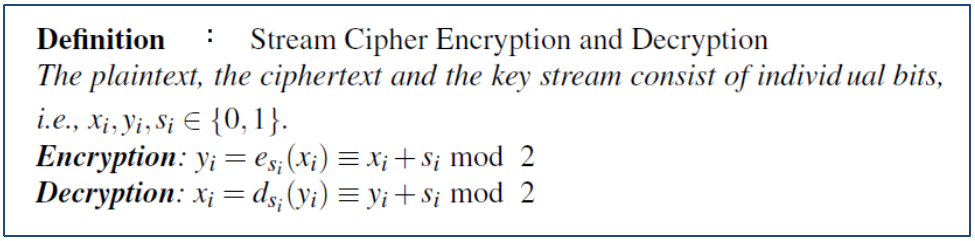
Given English alphabet:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

What is the key used for the encryption?

2. [2 pts] If it takes an attacker Taleh one day to try all possible keys for a 32-bit symmetric cipher, how long would it take him to try all possible keys for the same cipher with a 128-bit key?

3. The schema of binary stream cipher can be defined as:



Definition : Stream Cipher Encryption and Decryption
The plaintext, the ciphertext and the key stream consist of individ ual bits, i.e., $x_i, y_i, s_i \in \{0,1\}$.
Encryption: $y_i = e_{s_i}(x_i) \equiv x_i + s_i \bmod 2$
Decryption: $x_i = d_{s_i}(y_i) \equiv y_i + s_i \bmod 2$

This can easily be generalized to work with alphabets rather than binary.

a. [3 pts] Develop a cipher scheme which operates with the letters A, B, …., Z, represented by the numbers 0, 1, …, 25.

- What does the key stream look like? Suggest a simple function to generate it?
- What are the encryption and decryption functions?

b. [2 pts] Decrypt the following cipher text:

```
EXVNF WNY ZLYW SKRI
```

which was encrypted using the key stream:

```
BGRNT VFS WXLD CQJP
```