CS-GY6803- ISSEM Information Systems Security Engineering and Management
Spring Semester 2022 Lab2

For this lab, use Jupyter Notebook to write your responses.

Question 1: Please explain the following terms:

A. Cryptography
B. Encryption
C. Plain Text
D. Cipher Text
E. Decryption
F. Double Strength Encryption
G. Hybrid Encryption

Please read the following text carefully:

Shift Ciphers

If you have a message you want to transmit securely, you can encrypt it (translate it into a secret code). One of the simplest ways to do this is with a shift cipher. Famously, Julius Caesar used this type of cipher when sending messages to his military commanders.

We'll call this number the encryption key. It is just the length of the shift we are using. For example, upon encrypting the message "**cookie**" using a shift cipher with encryption key **3**, we obtain the encoded message (or ciphertext): FRRNLH.

Let's consider the following conversion table for English alphabets:

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

Table 2: Encoding English capital letters using integers from $\mathbb{Z}_{26}$.

1. Using the table, we can represent the letters in our message "cookie" with their corresponding numbers: 2 14 14 10 8 4.
2. Now add 3 (the encryption key) to each number to get: 5 17 17 13 11 7
3. Now use the table to replace these numbers with their corresponding letters: FRRNLH

Now, let's try doing the same thing for the word "**zero**". What letter would we use to replace the letter "z" when we encrypt? We use the letter "c", which can be viewed as being 3 places further along than "z" if, after we reach "z", we cycle the alphabet around to the beginning again.

After performing shift cipher encryption key 3, the message "zero" becomes CHUR. In terms of mathematical representation of our letters, the encryption of the message "zero" looks this way,

$$25\ 4\ 17\ 14 \rightarrow 28\ 7\ 20\ 17$$

What have we done mathematically? There is a handy mathematical concept that describes this very nicely. Define the following notation for integers a and b and integer $m > 1$:

$a \equiv b \pmod{m}$ means m is a divisor of $a - b$.

In summary, our encryption of the message "zero" using a shift cipher with encryption key 3 looks like this

$z \rightarrow 25 \rightarrow 25 + 3 \equiv 28 \pmod{26} \rightarrow C$
$e \rightarrow 4 \rightarrow 4 + 3 \equiv 7 \pmod{26} \rightarrow H$
$r \rightarrow 17 \rightarrow 17 + 3 \equiv 20 \pmod{26} \rightarrow U$
$o \rightarrow 14 \rightarrow 14 + 3 \equiv 17 \pmod{26} \rightarrow R$

How is the original (plaintext) message recovered from the ciphertext if the encryption key is known?

The following ciphertext was produced using a shift cipher with encryption key 3: CHUR. To decrypt it (i.e., to recover the plaintext message), we need to subtract 3 (. . . or add 23 . . . why is that the same?) to each of the numbers representing the ciphertext letters.

$C \rightarrow 2 \rightarrow 2 - 3 \equiv -1 \pmod{26} \rightarrow Z$
$H \rightarrow 7 \rightarrow 7 - 3 \equiv 4 \pmod{26} \rightarrow E$
$U \rightarrow 20 \rightarrow 20 - 3 \equiv 17 \pmod{26} \rightarrow R$
$R \rightarrow 17 \rightarrow 17 - 3 \equiv 14 \pmod{26} \rightarrow O$

Question 2:

Implement the above shift cipher in Python. You are expected to write two functions:

- **Encryption**: An encryption function that takes the plain text as input and returns the ciphertext as output. A good way to check if your function works correctly is to make sure that the output text of your function after encryption is NOT the same as your input text and manually check if each alphabet on in input has been replaced by 3 alphabets to the right
- **Decryption**: This function will take the output of the above encryption function and decode the message to give out the original plain text.

Note: You are expected to handle only alphabetic inputs for both your encryption and decryption functions.

Below is a sample set of inputs that your submission will be tested against and 10 more random inputs on top of these to make sure the functionality works for any alphabetic inputs.

- USA
- ISSEM
- CHICAGO
- CAPPUCCINO
- ZUPPA
- XAVIERS
- YELLOW
- SECURITY
- CYBERHUB
- HURRICANE

Question 3:

A) What is hash function in cryptography?

B) Write a hash function in Python to create the hash value of the following message:
Message = "Information Systems Security Engineering and Management"

To hash the above function use Python library- hashlib (SHA256)

C) Hash verification: Data can be compared to a hash value to confirm its integrity. The data is hashed at a certain time and the hash value is protected in some way (you can note it down, for this lab). Later, the data can be hashed again and compared to the protected value. If the hash values match, the data has not been altered. If the values do not match, the data has been corrupted.

Write a Python function which implements Hash verification by above method. Use that function to verify the data integrity of the message in part B of the question.

Submission:

This is a group submission. Please submit only one python notebook per group. Make sure to run all the functions and then download the notebook (format – ipynb). Title of the notebook should be lab2_group_<your group number>.ipynb. Good luck!