**1. Consider Substitution cipher vs. the One one-time pad cipher: Which one of these is called unbreakable and perfectly secure, and why? (5 points)**

**ANSWER:** If we consider the Substitution vs the one one-time pad cipher that which one of these are unbreakable and perfectly secure so the answer will be “the one-time pad cipher. The main reason for that is the key size of the encryption. The key size of the cipher text is usually as long as the size of the plaintext. Whereas the key used by the substitution is fixed and can be guessed easily or used again and again. The other reason is that substitution cipher usually has patterns which can be guessed by cryptanalysis, but the one-time pad is fully unique.

**2. Write your full name in lowercase without any spaces (e.g., "John Smith" should write his name as "johnsmith"). Encrypt this plaintext into ciphertext it using Caesar substitution cipher with k=8 (i.e., each letter is shifted by 8 positions forward). Show all of your work. (Hint: Create a table with letters from your name in different cells of a row and show the cipher text calculations in the following rows). (10 points)**

**ANSWER:** My Name is Shouzab khan, so the plaintext will be “shouzabkhan”. if I want to convert this plaintext into ciphertext using the Caesar Substitution cipher with K=8 so the ciphertext will be: “apwmrijspif”

**Working shown below:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PlainText | s | h | o | u | z | a | b | k | h | a | n |
| CipherText | a | p | w | m | r | i | j | s | p | i | f |

We will just shift each alphabet by 8 and you will get your ciphertext.

3. Nole Ksum sent you a letter encrypted with a substitution cipher. However, you do not know the value of the shift (k). How can you figure out the plain text given only the cipher text? State two ways to do so and explain how they work. (5 points)

**ANSWER:** If I receive a letter encrypted with a substitution cipher and however, I don’t know the value of the shift(k), I can figure out the plain text by the given cipher text by using two methods: the one is brute force attack and the second is Frequency Analysis.

The brute force attacks means that you try all the possibilities until you find the value of K shift. Which decrypts the cipher text into plaintext.

The brute force works like you start with the K shift value of 1 and try to decrypt the ciphertext. Check the converted plaintext if it good so you solved the problem otherwise try with other possibilities of the key shift value. Repeat this step until you get the plaintext.

Like known by the name frequency analysis it shows that we are going to see the frequencies of the alphabets or numbers. We will check how much is the frequency of the letter. Such as in English the most repeated letter is e so we have to try e with each cipher text were it fits in. like we have to make all the educated guesses and find the plaintext.

You have to calculate the frequency of letters in the ciphertext, look at the pattern in the cipher text and then have an educated guess to replace all the letters with most common letters like e or 1 in numbers. Unless your guess doesn’t decrypt the ciphertext you have to try again and again. At last, you will be succeeded.

4. Use your name as plain text (lowercase, remove spaces). Use the following one-time pad based to generate the cipher text using one time pad: "thequickbrownfoxjumpsoverthelazydog". Show all of your work (i.e., name in one row, letter values in the following row, one time pad in the following row, letter values of one-time pad in the following row, results of applying the one-time pad in the following row, and the corresponding cipher text in the final row).

**ANSWER:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Name: | s | h | o | u | z | a | b |
| Letter value: | 18 | 7 | 14 | 20 | 25 | 0 | 1 |
| One time pad key: | t | h | e | q | u | i | c |
| Letter value of key: | 19 | 7 | 4 | 16 | 20 | 8 | 2 |
| Result: | 37 | 14 | 18 | 36 | 45 | 8 | 3 |
| Mod 26 of (greater than 25): | 11 | 14 | 18 | 10 | 19 | 8 | 3 |
| Corresponding cipher text: | l | o | s | k | t | i | d |

5. Ecila and Selrahc are exchanging messages over an insecure line. Yrollam is listening in between and has the ability to modify, delete, or insert messages. How can Ecila and Serahc ensure each of the following? Explain the process and the technique(s) for each of the problems below:

a. If Selrahc receives a message from Ecila, the contents have not been modified by Yrollam. (5 points)

**ANSWER:** to ensure that Selrahc receives a message from Ecila, and the content have not been modified we can ensure it by adding digital signature to the message. Ecila will add her private key in the end of the message which be only known by Selrahc. Ecila public key will be used by Selrahc to ensure that the message is signed by the Ecila. If Yrollam had temper the message in between so Selrahc will came to know that Ecila digital signature is not there in the message and the message is compromised.

b. If Selrahc receives a message from Ecila, it is not a replay of an older message previously sent by Ecila, (5 points)

**ANSWER:** to ensure that it is the replay to the previous message you can just add a timestamp to each message Ecila send to the Selrahc. It will be a time added to the message at which the message was created and sent. Selrahc who receives the message will keep record of the time which she received already to check the integrity of message. If selrahc receives such message whose timestamp is not matching the last message, she received it means the message it compromised.

c. If Ecila sends three messages to Selrahc, Yrollam cannot delete the second message without getting detected by Ecila. (5 points)

**ANSWER:** Yrollam cannot delete the second message without getting detected by the Ecila if Ecila and Selrahc add hash chain like any Sha series (Sha-256, Sha-512 or any other). By this if yrollam delete the second message so Ecila will get to know that hash chain is broken. In this each message include the hash function of the previous message. By this you can verify the integrity of the message by verifying the hash in each message.

d. Yrollam cannot insert a fake message from Ecila to Selrahc (i.e., Yrollam sends the fake message to Selrahc and pretend that this is actually fro Ecila). (5 points)

**ANSWER:** By adding a digital signature in each message which is send by Ecila to Selrahc. By doing this the Selrahc can find the private key of the Ecila in the message which shows that message is not compromised and is directly send from Ecila.