CENG471 CRYPTOGRAPHY
Midterm – 1 11 Nov. 2022
2022 Fall
Q & A

Student Name and Number: ________________________

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

Q.1) (25 points) Please answer the following questions:

a) (15 points) What is the substitution and permutation? Please explain and give example cryptographic schemes for each.

Answer:

Substitution: The characters (the letters) are replaced different characters. For instance; in Plain-text, the letter "a" is substituted with character "D" in cipher-text. The Sezar Ciphering uses substitution technique.

y= K + x (mod 26) and K=3

P= "a" then C=K +x = 3 +0 (mod 26) = 3 and it represents "D" in alphabet.

Permutation: In plain-text, the placement of the characters are change in the cipher-text.

For instance our Plaintext is "abcdef" and the Key is "2 4 1 5 3" to define the ciphering positions.

Plaintext	a	b	c	d	e	f	g	h	J	-
Position	1	2	3	4	5	1	2	3	4	
Key	2	4	1	5	3	2	4	1	5	3
Ciphertext	B	D	A	E	C	G	J	F	-	H

b) (10 points) Fill in the blanks:

The Vigenere and Hill ciphers permute blocks of letters rather than one letter at a time.

The Shift and Affine ciphers are examples of substitution ciphers.

Q.2) (30 points) Let $E_k(m), D_k(c)$ be a block cipher. Fischer S Mixer (FSM) mode encrypts a sequence of message blocks $m_1, m_2, \ldots$ by the sequence of ciphertext blocks $c_1, c_2, \ldots$ using the following method:

$$c_i = m_{i-1} \oplus E_k(m_i \oplus c_{i-1}), \qquad i \geq 1$$

m_0 and c_0 are fixed (public) initialization vectors.

CENG471 CRYPTOGRAPHY
Midterm – 1   11 Nov. 2022
2022 Fall
Q & A

Student Name and Number: ____________________

a) **(20 points)** Please describe how decryption is performed.
b) **(10 points)** Suppose ciphertext block c_i is damaged in transmission. Which plaintext blocks become un-decipherable as a result? Please explain.

Answer

a) XORing m_{i-1} to both sides of the encryption equation gives:

$$c_i \oplus m_{i-1} = E_k(m_i \oplus c_{i-1})$$

Applying the decryption function on both sides gives:

$$D_k(c_i \oplus m_{i-1}) = m_i \oplus c_{i-1}$$

So; $m_i = c_{i-1} \oplus D_k(c_i \oplus m_{i-1})$.

b) If c_i was damaged then m_i is damaged. If m_i is damaged then m_{i+1} is damaged. From then on all messages are damaged.

Q.3) (20 points)

a) (10 points) We chose $p = 13$ and please show that 3 and 2 can be our generators for Z_{13}^{*}.

Answer:

First we find the factors of $(13 - 1) = 12 = 3.2^2$

For the test of 2; $2^{\frac{12}{3}} = 2^4 = 16 \; mod \; 13 \equiv 3$

$2^{\frac{12}{2}} = 2^6 = 64 \; mod \; 13 \equiv 12$, Hence 2 can be chosen as a generator.

For the test of 2; $3^{\frac{12}{3}} = 3^4 = 81 \; mod \; 13 \equiv 3$

$3^{\frac{12}{2}} = 3^4.3^2 \; mod \; 13 \equiv 3.9 \equiv 27 \equiv 1 \; mod \; 13$, Hence 3 cannot be chosen as a generator.

b) (10 points) Using affine cipher with a = 9 and b = 5 decode the cipher-text message **UQP LDS**.

Answer: y = 9 x + 5   is encryption function, we have to find decryption function.

x = (y – 5)/9 mod 26   and this is x = 3.(y – 5) mod 26 and this is x = 3.y – 15 mod 26

Cipher text	U	Q	P	L	D	S
decryption	x=3.20 – 15	x= 3.16 - 15	x= 3.15 - 15	x= 3.11 – 15	x= 3.3 - 15	x= 3.18 - 15
result	x= 19	x= 7	x= 4	x= 18	x =20	x= 13
Plain text	t	h	e	s	u	n

CENG471 CRYPTOGRAPHY
Midterm – 1 11 Nov. 2022
2022 Fall
Q & A

Student Name and Number: ____________________

Q.4) (25 points) Please, first give the descriptions of confusion and diffusion terms and explain the importance on symmetrical cryptosystems. Then, please explain that these requirements are satisfied by which parts of DES and AES.

Answer:
Diffusion: The mechanism of diffusion seeks to **make the statistical relationship between the plaintext and ciphertext as complex as possible** in order to thwart attempts to deduce the key. Good diffusion spreads the influence of a single plaintext letter over many ciphertext letters. In terms of the frequency statistics of letters, diagrams, etc.in the plaintext, diffusion randomly spreads them across several characters in the ciphertext. This means that much more ciphertexts are needed to do a meaningful statistical attack on the cipher.
Confusion: it makes **relationship between ciphertext and key as complex as possible.** Good confusion can only be achieved when each character of the ciphertext depends on several parts of the key, and this dependence appears to be random to the observer.

In DES; at the simplest level, **diffusion is achieved through numerous permutations (S-P Boxes)** and **confusions is achieved through the XOR operation**.
In AES; **diffusion is achieved through Subbyte transformations by Galoi Field operations** and **confusions is achieved through the XOR operation**.