CENG471 CRYPTOGRAPHY
2019 FALL – Midterm 1 – Nov. 5, 2019 - ANSWERS

Note: *The exam is closed books and notes, the time is two hours.*

Student Number & Name: ______________________________

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13

o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25

Q. 1 (20 points) Encrypt *howareyou* using the affine function 5x+7 (mod 26). What is the decryption function? Check it works.

Answer.1)

Plain text		**Encryption**	**Cipher text**		**Decryption**	**Plain text**	
	x	**y=5.x+7 mod 26**		**y**	**x=(y-7).5^{-1} mod 26, and 5.21=1 mod26** **so; x = (y – 7).21 mod 26**	**x**	
h	**7**	**y=5.7+7=16 mod 26**	**q**	**16**	**x=(16-7).21 mod 26=189 mod 26=7**	**7**	**h**
o	**14**	**y=5.14+7=77 mod 26=25**	**z**	**25**	**x=(25-7).21 mod 26=378 mod 26=14**	**14**	**o**
w	**22**	**y=5.22+7=117 mod 26=13**	**n**	**13**	**x=(13-7).21 mod 26=126 mod 26=22**	**22**	**w**

Q. 2 (20 points) The following ciphertext was encrypted by an affine cipher mod 26.

The plaintext starts ***ha***. Decrypt the message.

C R W W Z

Answer.2)

Plain Text -x		Encryption Function y= a.x + b	Cipher Text - y	
h	7	2=a.7 + b	C	2
a	0	17=a.0 +b ; so b= 17	R	17

So; a.7 + 17 = 2 then 7.a= 2-17 mod 26 = -15 mod 26 = 11

To solve that 7a=11 mod 26 and find the value of a; a=11.7^{-1} mod 26, we have to find multiplicative inverse of 7.7^{-1}=1 mod 26, and the value of 7^{-1} is 15 because; 7.15 =105 mod 26 = 1 mod 26.

Since, a=11.7^{-1} mod 26 = 11.15 mod 26 = 165 mod 26 = 9. Hence; the encryption function is

y=9x+17 mod 26.

Decryption function should be ; x = (y-17).9^{-1} mod 26= (y-17).3 mod 26. Because, 9.3=27 mod 26=1.

CENG471 CRYPTOGRAPHY
2019 FALL – Midterm 1 – Nov. 5, 2019 - ANSWERS

Note: *The exam is closed books and notes, the time is two hours.*

Student Number & Name: ________________________________

So: decryption function is **x=(y-17).3 mod 26**

Plain Text -x		Encryption Function **y=9x+17 mod 26.**	Cipher Text - y		Decryption function **x=(y-17).3 mod 26**	**Plaintext**
h	7	y=9.7+17 mod 26= 80 = 2 mod 26	C	2	x= (2-17).3=11.3=33 = 7 mod 26	**h**
a	0	y=9.0+17 mod 26 = 17	R	17	x=(17-17).3=0.3=0 mod 26	**a**
			W	22	x=(22-17).3=5.3=15 mod 26	**p**
			W	22	x=(22-17).3=5.3=15 mod 26	**p**
			Z	25	x=(25-17).3=8.3=24 mod 26	**y**

Q. 3 (20 points) Suppose you have a language with only the 3 letters a, b, c, and they occur with frequencies .7, .2, .1, respectively. The following ciphertext was encrypted by the Vigenere method (shifts are mod 3 instead of mod 26):

C A A A B B C A C B C A B A C A A B C C C A C A

Show that it is likely that the key length is 2, and determine the most probable key.

Answer 3.)

a	b	c
0	1	2

Is our alphabet and we are working with mod 3.

First we will calculate the all coincidences for one, two and three shift for the cipher text strips.

C	A	A	A	B	B	C	A	C	B	C	A	B	A	C	A	A	B	C	C	C	A	C	A	
	C	A	A	A	B	B	C	A	C	B	C	A	B	A	C	A	A	B	C	C	C	A	C	A

Only 6 coincidences are exist.

C	A	A	A	B	B	C	A	C	B	C	A	B	A	C	A	A	B	C	C	C	A	C	A		
		C	A	A	A	B	B	C	A	C	B	C	A	B	A	C	A	A	B	C	C	C	A	C	A

Only 10 coincidences are exist.

C	A	A	A	B	B	C	A	C	B	C	A	B	A	C	A	A	B	C	C	C	A	C	A			
			C	A	A	A	B	B	C	A	C	B	C	A	B	A	C	A	A	B	C	C	C	A	C	A

Only 5 coincidences are exist.

The maximum coincidences are occurred with two shift case, therefore the most probably the key length is two. Now, we will divide the cipher text into two parts;

CENG471 CRYPTOGRAPHY
2019 FALL – Midterm 1 – Nov. 5, 2019 - ANSWERS

Note: *The exam is closed books and notes, the time is two hours.*

Student Number & Name: ______________________________

The letters in first part are encrypted by the first letter of key. And the letters in second part are encrypted by the second letter of key. Hence; we can implement the frequency analysis on each part separately.

C	A	A	A	B	B	C	A	C	B	C	A	B	A	C	A	A	B	C	C	C	A	C	A	
C		A		B		C		C		C		B		C		A		C		C		C		1.Part
	A		A		B		A		B		A		A		A		B		C		A		A	2.Part

Frequency of letters	a	b	c	
In the first part	2	2	8	
In the second part	8	3	1	

As described in question that you have a language with only the 3 letters a, b, c, and they occur with frequencies .7, .2, .1, respectively.

So; we can be sure that for the first part, the “a” letter is represented by “c” and for the second part, the letter “a” is represented by “a” again, and “b” is represented by “b” and “c” is represented by “c”.

The most probable key is (“c”-“a”=2-0=2) as “c” and (“a”-“a”=0) as “a” then **“ca”**.

Q. 4 (20 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 4.)

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**.

CENG471 CRYPTOGRAPHY
2019 FALL – Midterm 1 – Nov. 5, 2019 - ANSWERS

Note: *The exam is closed books and notes, the time is two hours.*

Student Number & Name: ______________________________

Q. 5 (20 points) There are different mode of operations as shown following table.

ECB	CBC	CFB	OFB	CTR
$C_i = E_{K1}(P_i)$	$C_{-1} = IV$ $C_i = E_K(P_i \text{ XOR } C_{i-1})$	$C_{-1} = IV$ $C_i = P_i \text{ XOR } E_K(C_{i-1})$	$C_i=P_i \oplus E_k(O_{i-1})$, with $O_{-1}=IV$	$C_i = P_i \text{ XOR } O_i$ $O_i = E_{K1}(i)$

You have a stream of real time data between two end points communication, and you would like to be sure the secrecy of this data flow by the most efficient and safe mode of operation on bit or byte level. Please, choose one of the mode of operations from table and explain that why this mode is the most suitable way to encrypt and decrypt your stream data?

(Please note that some of the encrypted data blocks can be lost or corrupted).

Answer 5.) For stream ciphering, we can prefer output feedback mode (OFB) or counter mode (CTR).

In OFB mode, the feedback information is independent from the message, therefore these are independently (in parallel) calculated, and any corruption on some bits/bytes never affect the other bits/bytes. CTR mode is also has same advantages and can be easily implemented by hw or sw. But, there is a weak point exist for CTR mode, the counter value should be used only one time and never reuse again, otherwise it can be broken.

Q.6 (10 points) What is the principle of Kerckhoffs for cryptographic implementations and why is it so important? Please explain.

Answer 6) In 1883, Kerckhoffs princibles are accepted and they are already in use, which is described the specifications/principles of a cryptosystem to be secure. According to this principle; the security of a crypto system should be depend on the secrecy of key instead of secrecy of encryption and decryption algorithms. The key should be updated/renewed periodically and never reuse again.