37

National University of Computer and Emerging Sciences, Lahore Campus

Course Name:	Network Security	Course Code:	CS411
Program:	BS (Computer Science)	Semester:	Spring 2020
Duration:	60 Minutes	Total Marks:	40
Paper Date:	26-02-2019	Weight	10
Section:	-	Page(s):	6
Exam Type:	Mid-1		

Student : Name: Bilal Arif **Roll No.** 16L-4120 **Section:** A

Instruction/Notes:

1. **You may use rough sheets but you should not attach them to the question paper. All the work that you want to be graded needs to be on the question paper itself.**
2. **Points for each question are roughly related to the time that needs to be spent on that question. Avoid spending excessive time on questions with less points and less time on questions with more points.**

MCQs – 1 point each

Q1. _____ techniques map plaintext elements (characters, bits) into ciphertext elements.
A) Transposition
B) Substitution
C) Traditional
D) Symmetric

Q2. Joseph Mauborgne proposed a cipher that uses a random key that is as long as the message so that the key does not need to be repeated. The key is used to encrypt and decrypt a single message and then is discarded. Each new message requires a new key of the same length as the new message. This scheme is known as a(n) _____ .
A) pascaline
B) one-time pad
C) polycipher
D) enigma

one time

Q3. A way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is _____ .
A) rail fence cipher
B) cryptanalysis
C) polyalphabetic substitution cipher
D) polyanalysis cipher

Q4. Asymmetric encryption can be used for _____ .
A) both confidentiality and authentication
B) neither confidentiality nor authentication
C) Confidentiality
D) Authentication

Q5. Two issues to consider with the computation required to use RSA are encryption/decryption and _____ .
A) time complexity
B) trap-door one-way functions
C) key generation
D) asymmetric encryption padding

4

Q6._____ depend on how long it takes to execute the decryption algorithm.
A) Mathematical attacks
B) Timing attacks
C) Chosen ciphertext attacks
D) Brute-force attacks

Q7. In the general structure of the AES encryption process the input to the encryption and decryption algorithms is a single _____ block.
A) 32-bit
B) 256-bit
C) 128-bit
D) 64-bit

Q8. The AES cipher consists of *N* rounds, where the number of rounds depends on the _____ .
A) key length
B) output matrix
C) State
D) number of columns

Q9. A technique referred to as a _____ is a mapping achieved by performing some sort of permutation on the plaintext letters.

A) transposition cipher
B) polyalphabetic cipher
C) Caesar cipher
D) monoalphabetic cipher

Q10. The methods of _____ conceal the existence of the message in a graphic image.
A) steganography
B) decryptology
C) cryptology
D) cryptography

Q1 . Use the Vigenere cipher to encrypt the word "explanation" with the key "leg". For substitution, use the values a=0, b=1, c=2, ... z=25. Show the working. (3 Points)

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

key : leg = "11 4 6"

E	x	p	l	a	n	a	t	i	o	n
4	23	15	11	0	13	0	19	8	14	13
11	4	6	11	4	6	11	4	6	11	4
15	1	21	22	4	19	11	23	14	25	17

3

p	b	v	w	e	t	l	x	o	z	r

8

ciphertext = pbvwetlxozr

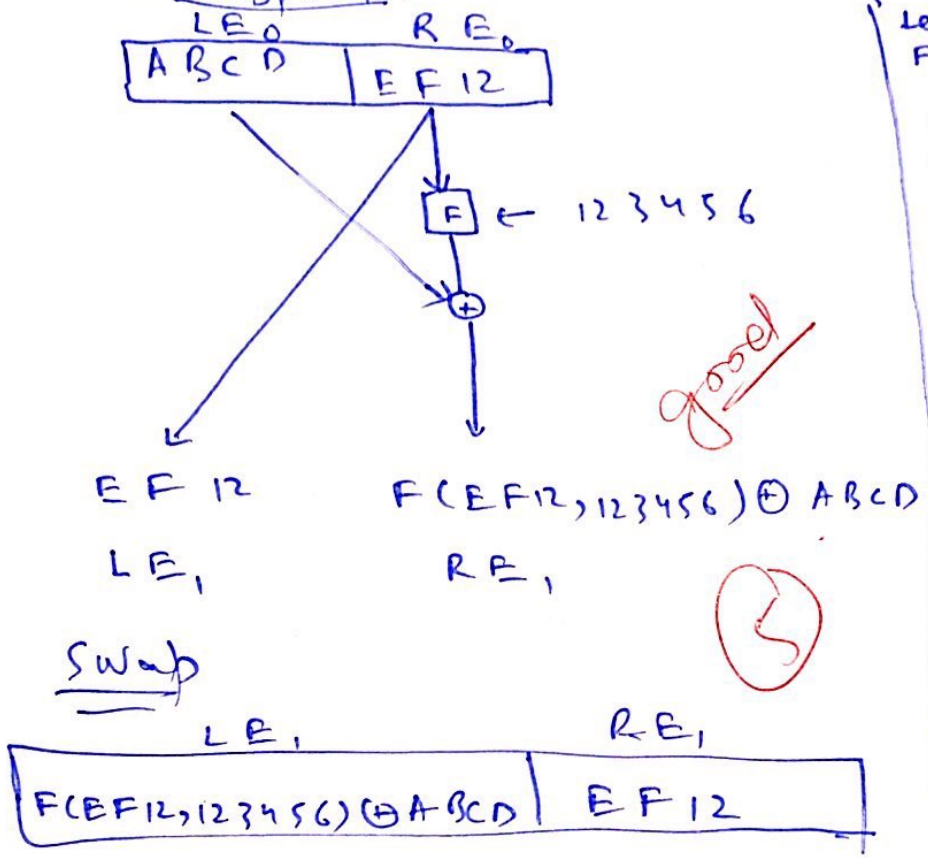
Q2. Define the avalanche effect. (2 Points)

It means that with a little change in either key or plaintext, ciphertext changes immensely.

2

Q3. Suppose that we have a Feistel Cipher where everything is the same except that there is only one encryption round (instead of 16). The hexadecimal key that is being used in the encryption round is 123456. Suppose that the hexadecimal input string for this round is ABCDEF12. Draw a comprehensive diagram which shows the complete working of encryption and decryption along with the inputs and outputs. You do not need to compute the bitwise operations. Similarly, abstract from the details of other functions. (5 points)

Encryption:

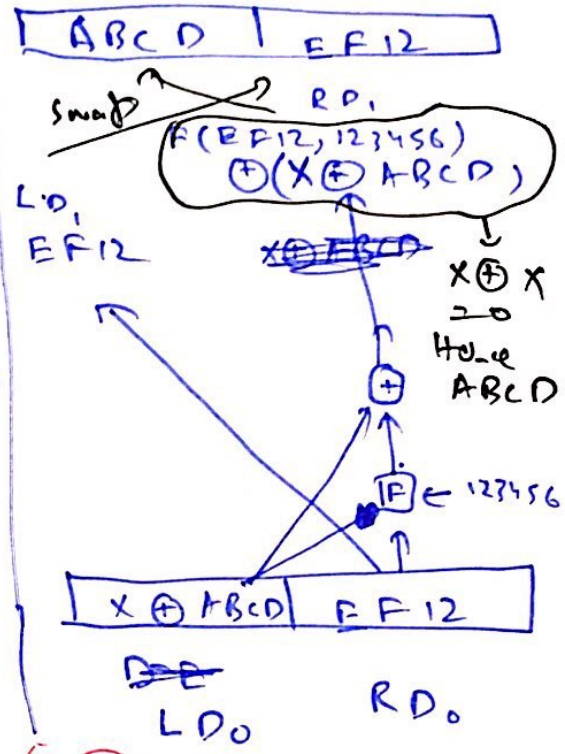


good

5

Decryption

Let's say:
F(EF12, 123456) = X



Q4. How does AES not have a Feistel structure? (1 point)

Because it does not divide the input block in two halves for processing and using matrix state instead.

1

It also doesn't have the concept of swapping input.

8

Q5. Briefly describe the 4 different stages of AES. (1+1+1+1=4 points)

① Substitute column: In this stage an "S-box" is used to map bytes elements in current state into a new Transformation. It is 16 x 16 Matrix in case of 128 bit input.

② Shift Rows: In this stage 1st Row is not shifted, 2nd is shifted left by 1 column, 3rd is shifted left by 2 column and 4th by 3 columns.

③ Column Mix: In this stage, diffusion is done, for this one column contributes to the values of all of the bytes of that column for this $\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$ matrix is multiplied with current states

4

④ Add Round key: At this stage each byte of current state is XORed with corresponding byte of key.

Q6. What are the 5 requirements to make a public-key crypto system a secure algorithm? (5 points)

① It should be computationally easy for reciever to decrypt ~~mess~~ cipher knowing algorithm and private key.

② It should be computationally easy to generate a pair of related keys for sender/reciever.

③ It should be computationally infeasible for adversy to decrypt message using algorithm and public key

④ It should be infeasible for adversary to guess Private key given public key and algorithm.

5

⑤ Gap between p and q should be b/w $10^{75} - 10^{100}$

⑥ p-1 and (q-1) should have large Prime factor

⑦ gcd for (p-1) & (q-1) should be small.

Q7. 8839 and 8849 are two prime numbers. Their product is 78216311. Find all the factors of 78216311. (1 points).

factors of 78216311 are {8839, 8849, 78216311, 1}

1

Q8. Briefly describe the three major ways you can deter a timing attack on RSA. (3 points)

① Constant Exponentiation: make algorithm work such could it takes equal time to decrypt all possible ciphers. This technique is not considered good.

② Add Random delay: Add some random delay so that cryptanalyst does not guess actually decryption time of algorithm

3

③ Blinding: Multiply cipher text with some number to change bits, so that cryptanalyst can't do bit by bit analysis which is required for RSA.

Q9. 23^{23} mod 23 = 0. Prove it using calculations. (1 point)

$[(23^4 \% 23) \times (23^4 \% 23) \times (23^4 \% 23) \times (23^4 \% 23) \times (23^4 \% 23) \times (23^2 \% 23) \times (23 \% 23)]$

$[(0) \times (0) \times (0) \times (0) \times (0) \times (0) \times (0)]$

$= 0$

1

5

Q10. What are the differences and similarities in conventional and public-key encryption? (5 points)

Differences:

Public key	Conventional
① It uses two keys, one public key for Encryption and another different Private key for decryption	① only one key for both encryption and decryption
② Uses two related Algorithms, One for Encryption, another for decryption.	② only one algo for both encryption and decryption
③ No need to have a secure key transfer channel.	③ Need to have a secure key transfer channel
④ given public key, ciphertext and Algorithm, no one should be able to ~~get~~ guess private key	④ given ciphertext and Algorithm, key should not be guessable

3

Similarities,

① Both are intended to Provide Security of Information.

② Both use key and an Algorithm for decryption/Encryption.

③ Both use transposition & substitution / confusion & diffusion to secure message.