33.5

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: Momin Siddique **Roll No.** 16L-4173 **Section:** CS-B

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

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

16L-4173 CS-B

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)

Repeat the key on the plain text.

1

L E G L E G L E G L E
E X P L A N A T I O N

→ We use a 26x26 matrix to substitute by looking "key" character in row & Plain text character in column. Corresponding alphabet is replaced. But here substitution is already given in numbers

E X P L I
4. 23. 15 11. 0 13 0 19. 8. 14. 13.

→ L+E E+X

or L-E E-X

6

16L-4173 CS-B

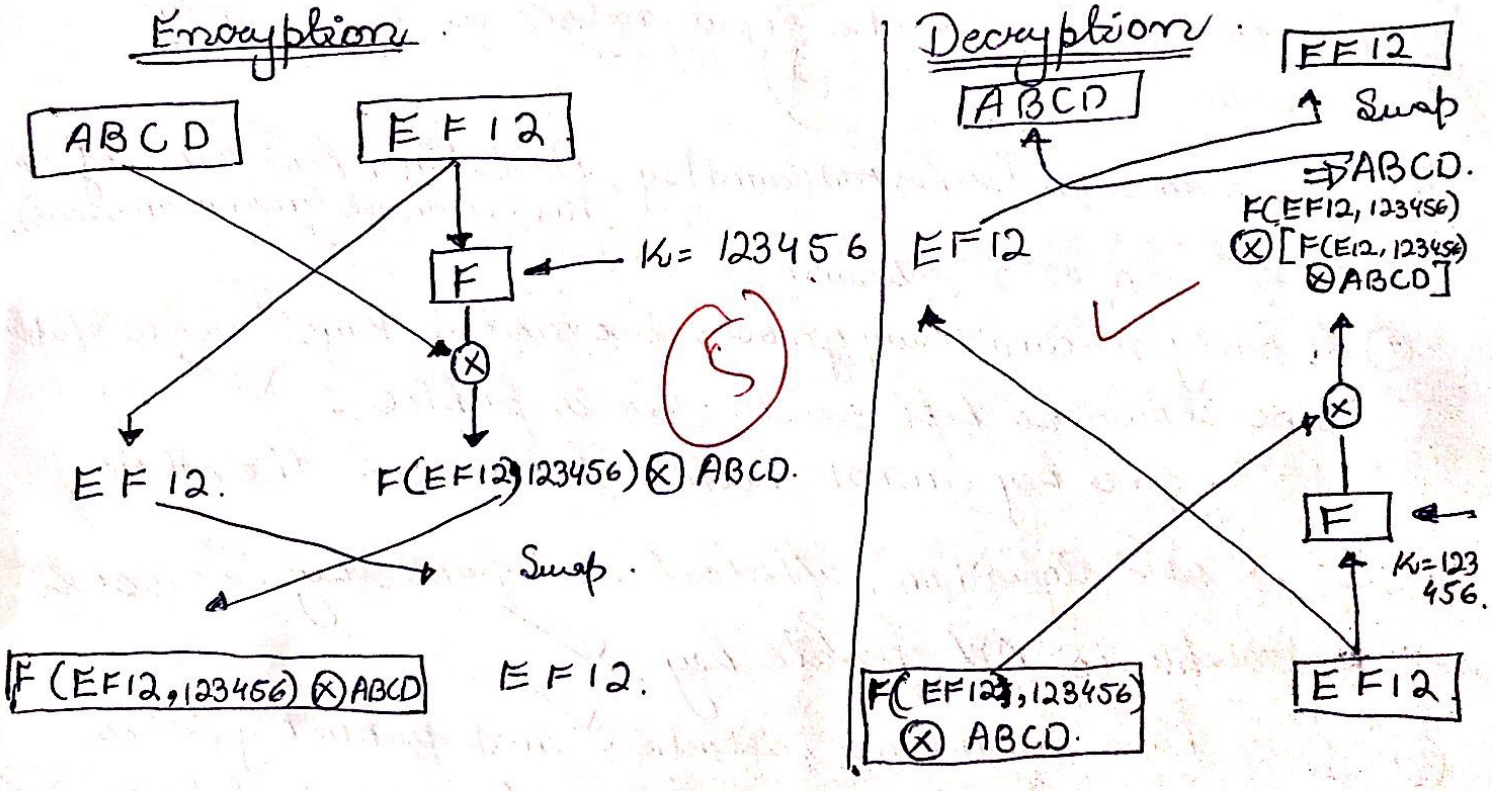
1.5

Q2. Define the avalanche effect. (2 Points)

plain

A small change in key or in ciphertext will lead to a significant change in the ciphertext after performing some rounds. This is avalanche effect.

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)



5

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

1

AES does not have a Feistal structure because it treats (applies transforms) on the input as a whole rather than dividing it as done in Feistal.

7.5

16L-4173 CS-B

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

There are four transforms Applied on input matrix

① Subbyte substitution: Each byte in the input matrix is replaced by another byte from "S-box". 4 bits for row, 4 bits for column. Inverse is done using Inverse S-box

② Shifts rows: Shifts rows such that every byte in one column is distributed to other col. No shift for first row, 1 circular left for 2nd; 2 for 3rd, 3 for 4th row. Inverse is done using right shift

③ Mix Columns: Multiply each col by a matrix $\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$ to obtain a new column.

④ Add roundKey: XOR the input matrix with the key matrix.

4

There are N rounds, R_0 has AddroundKey, R_1 to R_{N-1} have 4 transform, R_N has three (minus mix col)

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

The five require as follows.

① A party A can easily generate two related keys (Private & Public). One should be kept secret, other is public.

② ~~Actual~~ One key cannot help to determine the other.

③ If we have algorithm, ciphertext and public key, it is still infeasible to get private key.

④ If we have algorithm, ciphertext and public key, it is infeasible to get plaintext. (because of one way trapdoor)

⑤ Either key can be used for encryption and other would be used for decryption, They perform complimentary operations

4

16L-4173 CS-13.

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

1, 8839, 8849, 78216311.

1

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

Three ways are.

(1) Add random delay: Add random delay to every decryption so pattern cannot be judged.

(2) Constant time: Every decryption should come after a specific time. Intervals are fixed to avoid patterns. This may result in worst performance as we are waiting even after the decryption has completed.

3

(3) Blinding: Multiply ciphertext with a number (random). So, the decryption time changes and pattern cannot be traced.

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

$$\left[(23^3 \bmod 23) \times (23^3 \bmod 23) \times (23^3 \bmod 23) \times (23^2 \bmod 23) \times (23^3 \bmod 23) \times (23^3 \bmod 23) \times (23^3 \bmod 23) \times (23^2 \bmod 23)\right] \bmod 23$$

$$= [0 \times 0 \times 0 \times 0 \times 0 \times 0 \times 0 \times 0] \bmod 23$$

$$= 0 \bmod 23$$

$$= 0$$

4

16L-4173 CS-B.

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

Conventional	Public Key
Differences	
① Only has one key (Secret)	① Has two keys (Public & Private)
② Encryption/, decryption algos are reverse of each other	② Both algos are related.
③ Key has to be transported via a safe channel.	③ Private is always with the user. Public is known to the Public.
④ No authentication.	④ Provides sender authentication.
⑤ Used only for secrecy	⑤ Used for ① Secrecy ② Authentication ③ Key exchange
Similarities:	
① No way to know ~~cipher~~ Plain text if secret key is kept safe.	① No way to know the plain text if private key is kept secret.
② Knowledge of algorithm and ciphertext cannot lead to key. and plain text.	② Knowledge of algorithm and ciphertext cannot lead to Private key and plaintext

4