20

# 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:** 16L-4182 **Roll No.** 16L-4182 **Section:** 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



3

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)

Key = leg
word = explanation
First Step
length(key) = length(word)
∴ key = legleglegle

15 1 21 22 4 19 11 23 14 25 17

encrypt text : pbvwetlxozr

3

6

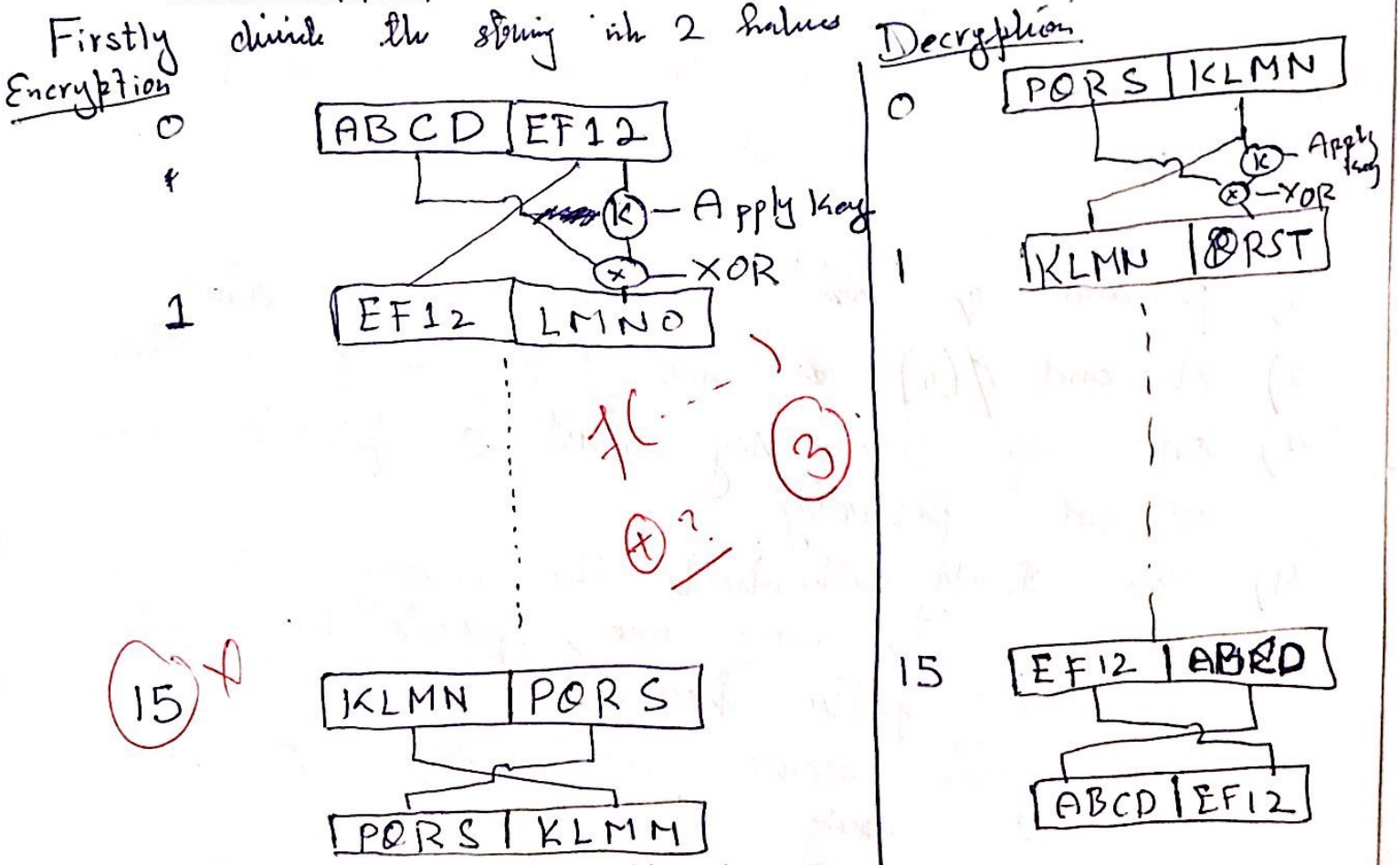
Q2. Define the avalanche effect. (2 Points)

Avalanche effect is defined as when we change any 1 bit in the key. This will create the wrong output.

1

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)

Firstly divide the string in 2 halves




3

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

AES does not have Feistel structure because in AES there are some permutation added with the key.



4

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

1) Matrix Formation : In this first we make 128 bit into 16 bytes and make 4x4 matrix and all 44 word key and make 4 word matrix each.

2) Shifting : In 4x4 matrix. First row have 0 left shift. Second row have 1 left shift. Third row have 2 left shifts and the last row having 3 left shift.

3) Reshuffling / Multiplication : Multiply with a matrix of each row with 4x4 matrix which are given.

4) Rounds : Apply rounds on key with XOR and swapping

4

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

1) p and q must co-prime of each other
2) d and $\phi(n)$ must co-prime of each other.
3) one of the key must be private i.e., do not publicize
4) You should authenticate the message when you recieve it. using your private key and sender's public key.
5) You should secure the message when you send it using others public key.

1



5

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

Factors = 8839, 8849, 1

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

i) The public key does not decrypt the message same which we encrypt using private key.

ii) The private key does not decrypt the message same which we encrypt using public key.

iii) The both keys don't give the sign of authentication and security.

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

$23 \times 23^{22} \bmod 23 = 0$

$23^{22} \times (23 \bmod 23) = 0$

$23^{32} \times 0 = 0$

$0 = 0$ Proved



1

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

Differences

| Conventional Encryption | Public Key Encryption |
| --- | --- |
| i) There is only 1 key to encrypt or decrypt the message | i) There are two keys to encrypt or decrypt the message. |
| ii) There is no private or public concept in this type. | There is one private key or one public key in this type |
| iii) The key length is equal to Cipher text | The key length is not equal to Cipher text. |

Similarities

i) Both are using for encryption or decryption of message

ii) Both require keys for encryption or decryption.

1