


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: _____ **Roll No.** _____

Section: _____

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

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)

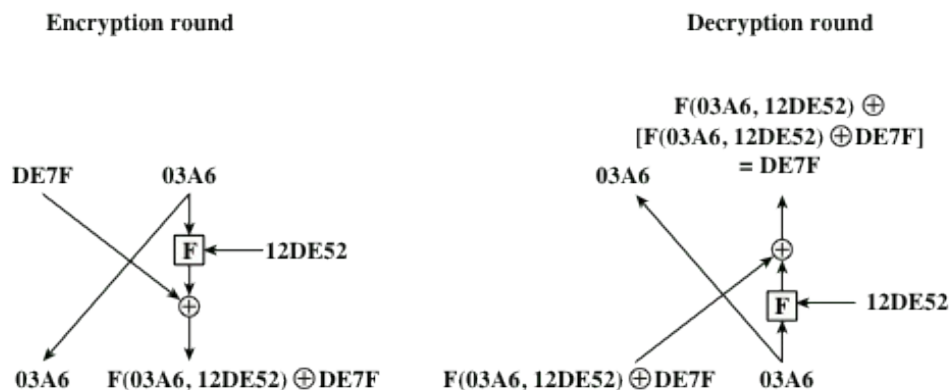
KEY: legleglegle

Answer: pbvwetlxozr

Q2. Define the avalanche effect. (2 Points)

The avalanche effect is a property of any encryption algorithm such that a small change in either the plaintext or the key produces a significant change in the ciphertext.

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)



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

AES does not split the input into two halves.

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

SubBytes

Each individual byte of State is mapped into a new byte in the following way: The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value. These row and column values serve as indexes into the S-box to select a unique 8-bit output value.

ShiftRows

The first row of State is not altered. For the second row, a 1-byte circular left shift is performed. For the third row, a 2-byte circular left shift is performed. For the third row, a 3-byte circular left shift is performed.

MixColumns

MixColumns operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in that column.

AddRoundKey

The 128 bits of State are bitwise XORed with the 128 bits of the round key.

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

1. It is computationally easy for a party B to generate a pair (public key PUB, private key PRb).

2. It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M, to generate the corresponding ciphertext:

$$C = E(PUB, M)$$

3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message:

$$M = D(PR_b, C) = D(PR_b, E(PU_b, M))$$

4. It is computationally infeasible for an opponent, knowing the public key, PU_b , to determine the private key, PR_b .

5. It is computationally infeasible for an opponent, knowing the public key, PU_b , and a ciphertext, C , to recover the original message, M .

Q7. 8839 and 8849 are two prime numbers. Their product is 78216311. Find all the factors of 78216311. (2 points).

1, 8839, 8849, 78216311.

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

Constant exponentiation time

Ensure that all exponentiations take the same amount of time before returning a result; this is a simple fix but does degrade performance

Random delay

Better performance could be achieved by adding a random delay to the exponentiation algorithm to confuse the timing attack

Blinding

Multiply the ciphertext by a random number before performing exponentiation; this process prevents the attacker from knowing what ciphertext bits are being processed inside the computer and therefore prevents the bit-by-bit analysis essential to the timing attack

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

[$23^{16} \bmod 23 \times 23^4 \bmod 23 \times 23^2 \bmod 23 \times 23 \bmod 23$] $\bmod 23$

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

Conventional Encryption	Public-Key Encryption
<p><i>Needed to Work:</i></p> <ol style="list-style-type: none"> 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. <p><i>Needed for Security:</i></p> <ol style="list-style-type: none"> 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if the key is kept secret. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key. 	<p><i>Needed to Work:</i></p> <ol style="list-style-type: none"> 1. One algorithm is used for encryption and a related algorithm for decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). <p><i>Needed for Security:</i></p> <ol style="list-style-type: none"> 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if one of the keys is kept secret. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.