20.5

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: Tahir Hameed **Roll No.** 15L-4089 **Section:** 8A

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
X [✓ 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) one-time pad
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 .
✓ [✓ 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
X [✓ 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)

e x p l a n a t i o n

4 23 15 11 0 13 0 19 8 14 13

l = 11
e = 4
g = 6

l e g l e g l e g l e

11 4 6 11 4 6 11 4 6 11 4

encrypted/ciphered number: 15 1 21 22 4 19 11 23 14 25 17

ciphered text: PbVWETLXOZR

a	= 0
b	= 1
c	= 2
d	= 3
e	4
f	5
g	6
h	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25

6

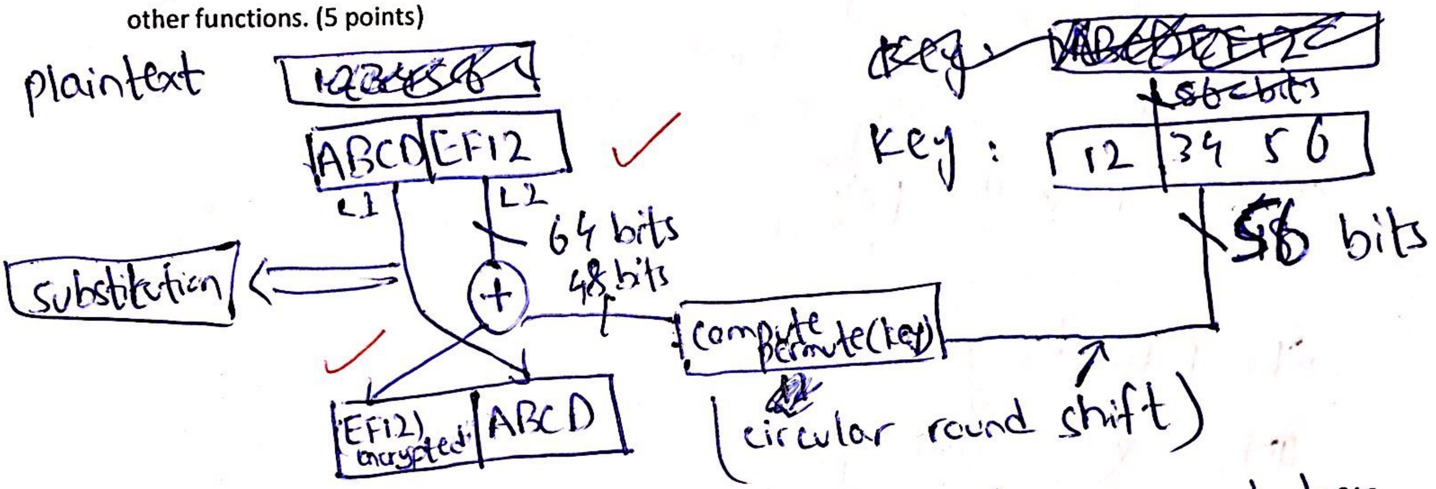
3

1

Q2. Define the avalanche effect. (2 Points)

Avalanche effect is the amount of differentce in the ciphered/encrypped ~~key~~ of big change by making a small changes in the plaintext. Eg changing 1 bit, changing 1 character randomly, changing all elements et..

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)



L2 & L1 are substited at round. And permutation of key is calculated. Input key is 64 bits. After permutation and circular round shift key is cut off to 48 bits.

Swap?
⊕?
decryption?

1.5

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

AES doesn't divide bits into partitions i.e like L1, L2 in Fiestel Cipher. ~~Moreover,~~ Thus, operations in every round are considered

for entire plaintext nor for a partition of it.

1

3.5

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

1) Substitute bytes
→each value in the matrix is substituted with a permutation box containing every possible ~~permutation~~ value for the plaintext.

2) Shift-rows
→ rows are ~~substituted~~ left shifted. with first row with zero shift, row2 with 1 shift to left. n rows shifting

3) Column-mixed
→ each column ✓ is mapped to a value equal to function of that column.

4

4) XOR with key:
→ XOR of plaintext with key.

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

~~1) Blinding~~

~~2) Time delaying~~

~~3) Adding a value to a key to get rid of matching ciphered text~~

1) Private keys should ✗ not be shared/ kept hidden.

2) Only public/private ~~ke~~ plaintext/key can ✗ encrypted/ decrypted ~~can~~ ~~keys~~

3) Public keys are accessible by anyone ✗

0

4

4) Algorithm while decrypting ✗ and encrypting is not exactly same. ✗ It is some changes

5) key is shared through a secured channel.

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

78216311 : 8839, 8849, 811, 311, 6311

0 ✗

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

1) Blinding
Don't take/show ~~show~~ too much time to encrypte text. show response of done while working on encrypting it

2) Time delaying
Add more time while decrypting

✗ 3) Adding a value to a (key / encrypted)

1

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

~~23^{23} mod 23~~ = 0

$= 23^{23} \% 23$

$= (23 \times 23 \times 23 \times 23 \times 23 \ldots$ (23 times) $\% 23)$

$(23 \% 23 \times 23 \% 23 \times 23 \% 23 \ldots$ .... (23 times))

0

$= (0 + 0$ to ... $0)$

1

$= 0$

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

Conventional

1) Algorithms for encryption and decryption are ~~Same~~ ~~[illegible]~~ shared.

2) Doesn't considered identity of the sender

3) Only secures plaintext

4) Algorithms are well known and can be vulnerable using brute force, mathematical attacks

5) ✓ One algorithm for both for encryption and derypton.

public key encryption

~~1)~~ 1) ~~Algorith~~ Public keys are shared

2) ✓ Algorithm for encrypted and decrypting is not same / not an exact match or follow a pattern.

3) ✓ Take account of identity

4) Secures both plaintext and identity

5) ✓ Public keys or private can encrypt or decrypt plaintext / works both ways

3