National University of Computer and Emerging Sciences, Lahore Campus

Course Name:	Information Security	Course Code:	CS3002
Program:	BS(Computer Science)	Semester:	Fall 2023
Duration	60 minutes	Total Marks:	35
Date:	02-10-23	Weight	12.5
Exam Type:	Midterm-I	Pages	4

22

Student : Name: Hashim Bilal Roll No. 20L-1219 Section: BCS-7B

Instruction: If you think some information is missing then make an assumption and write it clearly.

Question 1: [CLO:1] [5 marks]

1. The process of identifying vulnerabilities and threats and their impact and probability of occurring an attack is called _____.
   a. Vulnerability assessment
   b. Vulnerability identification
   c. Threat detection
   d. Risk analysis

2. Receiving an SMS message where the sender's number is fake, is an attack against _____.
   a. Confidentiality
   b. Integrity
   c. Availability
   d. Authenticity

3. Which block cipher mode does not allow parallel encryption of blocks?
   a. Cipher Block Chaining (CBC)
   b. Counter mode
   c. Electronic Code Book (ECB)
   d. All of these

4. Sam maintains a public key ring in his computer. He will pick a key from the ring during
   a. Asymmetric encryption
   b. Signing a message
   c. Asymmetric decryption
   d. Both a and c

5. In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____
   a. Scaling of the existing bits
   b. Substitution of the existing bits
   c. Addition of zeros
   d. Addition of ones

Question 2: Short Questions [CLO: 3] [6 +4 marks]

Part I:

Identify the kind of attacks in each of the following statements and identify at least a couple of reasons the people fall for that

a. You receive a phone call. The caller claims that they are from a bank, and ask your debit card number and OTP for the purpose of account confirmation, otherwise your account will be blocked.

Phishing
Reasons:
1. Naiveness of people
2.

b. You tried to login to your flex account during which you ignored a warning displayed by the browser and later on you came to know that your login credentials have been stolen.

Connection Hijack
Reasons:
1. Naiveness of people
2.

c. The outgoing network traffic of your system has suddenly increased and on diagnosis, you have identified that your system is constantly sending a specific request to a server.

IP Spoofing
Reason:
1. Naiveness of people

Part II:

We studied following security design principles: Least privilege, Failsafe defaults, Separation of privilege, Economy of mechanism, Psychological acceptability, Complete mediation, Least common mechanism. Analyze the following scenarios and identify, with reasoning, what security design principle is being applied? Also state what advantages are achieved due to that principle.

A. Marketing staff do not have access to engineering design files.

least Privelege (could be Fail Safe Defaults as well)
Reason: The access of the staff is minimum to the data, i.e having least Privelege
Advantages:
1. Users cannot be spoofed by anyone on the system

B. Company database is protected by only one layer of encryption rather than two layers.

Economy of Mechanism
Reason: The security mechanism is simple (one layered only) instead of complex system, which matches Principle of economy of mechanism.
Advantages:
1. less number of errors occurred
2. Easy to test and debug the system
3. Cheap time complexity

Question 3:

a. Encrypt the text "voteforme" using Vigenère cipher with a key 245. [CLO:1] [2+4+4 marks] (4)

votefoeme
24524524S
xsyggjttqj

Ciphu = "xsygjttqj"

b. Show the process of Diffie-Helman key exchange using a prime 47 and generator 11. Suppose Alice chooses a secret 9 and Bob chooses 16.

p = 47, g = 11

Alice x = 9, Bob y = 16

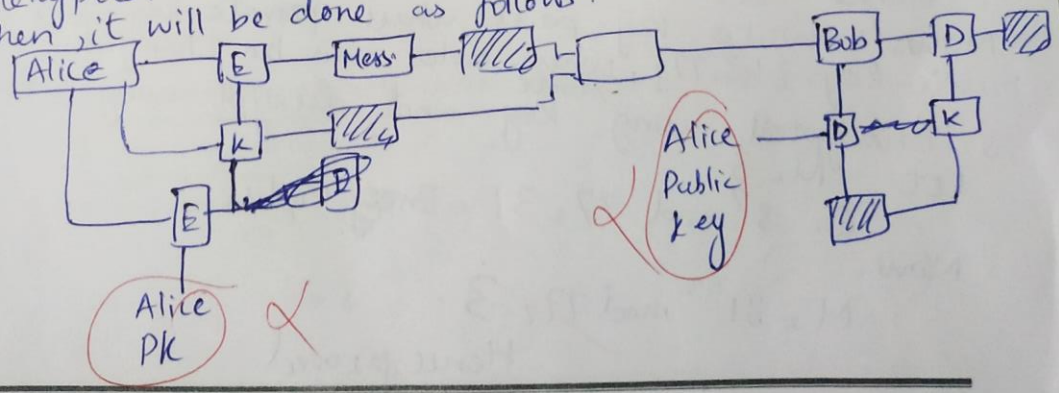
X = 11^9 mod 47 = 9^{11} mod 47 = 16

Y = 11^{16} mod 47 =

key At Alice = Y^x mod 47 X^y mod 47

c. What is a digital envelope? Demonstrate its working with the help of an example! What are the advantages of this mechanism?

A digital envelope is a technique used to share secret key along with the message to receiver. Lets say Alice want to send a message to bob encrypted with a secret key, and share that key as well. Then, it will be done as follows:



Advantages:

1. Authenticity of Sender
2. Integrity of the message 3. No Hijack/Man in middle

0083

Question 4:

Describe the key development mechanism using RSA when the values of p and q are given to be 7 and 11 respectively? Although there are multiple options for choosing the encryption value 'e', let's choose 7 that fulfill the criteria and then find 'd' accordingly. You should provide all details and outcome should be written in the form of private and public keys. Demonstrate the working of your system by encrypting a number and then retrieving it back using decryption. [CLO:1] [10 marks]

Let $p = 7$, $q = 11$

1. Calculating $\phi(n)$, where $n = p \times q$, $n = 77 (7 \times 11)$

$\phi(n) = (p-1)(q-1)$, since $\phi(n) = n-1$, $n \in \{Prime\}$

$\phi(n) = (6)(10) = 60$

2. Selecting 'e', which is 7 and is co-prime to $\phi(n) = 60$. (10)

3. Now, find 'd' and for that use Euclid's Algorithm;

$60k+1$, $k = 1, k = 2, \ldots$

$60k+1 = 60(1)+1 = 61$ (not divisible by 7)

$= 60(2)+1 = 121$ (not divisible by $e = 7$)

$= 60(3)+1 = 181$ (not divisible by $e = 7$)

$= 60(4)+1 = 241$ (not divisible by $e = 7$)

$= 60(5)+1 = 301$ (divisible by 7)

$301 / 7 = 43$

Hence $d = 43$

4. Write key pairs, where private key $= \{7, 77\}$ public key $= \{43, 77\}$, where roles can be changed.

5. Encrypted using private key and decrypt using public key.

Let $M = 3$

$C = 3^7 \bmod 77 = 31$ = Ciphel

Now,

$M = 31^{43} \bmod 77 = 3$

Hence, proved