National University of Computer and Emerging Sciences, Lahore Campus

Course Name:	Information Security	Course Code:	CS3002
Degree Program:	BS (CS)	Semester:	Fall 2022
Exam Duration:	60 mins	Total Marks:	35
Paper Date:	26/09/22	Weight:	12.5
Exam Type:	Mid I	Page(s):	4

Student : Name:______________________________ Roll No.__________________ Section:________

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

Question 1: MCQs and True/False **[10 Marks] [CLO 1]**

1.1 A way of checking whether the private key matching the public key in a certificate has been compromised and so the certificate should no longer be accepted.

a) registration list
b) rejection list
c) revocation list
d) all of the above

1.2 A hash function is regarded as strong if a single bit change in the input changes the output by at least ____ .

a) 40%
b) 50%
c) 60%
d) 70%

1.3 When someone takes the place of a legitimate host, it is called _________.

a) Connection hijacking
b) IP Spoofing
c) Phishing
d) None of the above

1.4 Triple DES algorithm uses a data block size of _____ bits.

a) 56
b) 64
c) 112
d) 168

1.5 Which cyber security principle states that Security mechanisms should be as simple and small as possible?

a) Complete mediation
b) Least Privilege
c) Economy of mechanism
d) Open Design

1.6 Applying safeguards that eliminates or reduces residual risk is called defense strategy.

a) Avoidance
b) Acceptance
c) Mitigation
d) Transference

1.7 Contingency planning consists of

a) Incidence response planning
b) Disaster recovery plan
c) Business continuity plan
d) All of the above

1.8 Asymmetric cryptography is faster in computation compared to symmetric cryptography.

a) True
b) False

1.9 If Alice has a message to send to Bob and she wants to encrypt the message using asymmetric cryptography so that no one other than Bob can read it, she does so by using Bob's public key.

a) True
b) False

1.10 Weakness of an asset is called threat

c) True
d) False

Question 2: **[6 marks] [CLO 1]**

In each of the following scenarios, identify which security design principle is followed OR violated. Some of the security design principle are listed above in MCQ 1.5. Elaborate your response.

A. The company behind Telegram messenger hired some brilliant cryptographers to design proprietary security protocols for secret chats.

Violation of Open Design because proprietary protocols can not be subject to public scrutiny by experts.

B. Staff at an airline booking office is required to provide their password as well as scan their smart card before confirming a booking.

Separation of Privileges is being followed, as multiple security conditions are being checked.

C. A program successfully opens a file in write mode, but after a few hours, writing data to file fails due to permission errors.

Complete Mediation is being followed because initially the program had permissions. After some time the permissions were revoked. The operating system did not rely one-time check, instead it applied security checks on each access.

Alternate answer: Principle of least-privilege is followed because the program was given a temporary privilege escalation, which was taken back after some time.

Question 3: **[3+3+5 marks] [CLO 1]**

a) **Suppose you have received the following encrypted messages from the sender and you have been told that RSA algorithm is used to encrypt this information and the public key to decrypt the message is {7, 187}. Your task is to retrieve the original messages.**

C1 = 16
C2 = 24

16^{7} mod 187 = 135
24^{7} mod 187 = 29

b) **What is Euler Totient function (phi). What is the phi (Φ) of 19?**

Phi of a number n counts all co-prime numbers smaller than n.

phi (Φ) of 19 = 18 as 19 is a prime number

c) **Analyze the following statements for correctness. Justify with arguments.**

i. **Encryption with RSA is not vulnerable to man in the middle attacks.**

RSA by itself is vulnerable to MITM attacks because attacker can share their own public key with both parties without either of them realizing.

Alternate Answer: It is not vulnerable as in this mechanism the public key will be certified by the Certification Authority.

ii. **A strong hash function like SHA-512 alone can compute the Message Authentication Code (MAC).**

Hash function alone is not sufficient. MAC computation also requires a secret key as input, such as a pre-shared key or the private key of the sender.

Question 4: **[4+4] [CLO 4]**

User A wants to download an operating system image from the vendor website. On downloading the OS image, the user should be able to assess the integrity and authenticity of the OS image in an optimal way. Draw a diagram to illustrate the process to ensure and validate integrity and authenticity of the OS image. Briefly describe each step of the process illustrated in your diagram.

Diagram:

Figure on Lecture 5-6 slide # 29 BUT with an important change:

- **at the sending side, the key K is the private key of OS vendor**
- **at receiving side, K is public key of OS vendor**

Process Steps:

Vendor will have to create and attach MAC to in order to prove the integrity and authenticity of the downloaded image. Vendor signs the MAC with their private key. User downloads the image and verifies the MAC with vendor's public key.