MCA/4TH SEM/MCAP 2262/2021

CRYPTOGRAPHY AND NETWORK SECURITY
(MCAP 2262)

Time Allotted : 3 hrs **Full Marks : 70**

Figures out of the right margin indicate full marks.

Candidates are required to answer Group A and any 5 (five) from Group B to E, taking at least one from each group.

Candidates are required to give answer in their own words as far as practicable.

Group – A
(Multiple Choice Type Questions)

1. Choose the correct alternative for the following: **10 × 1 = 10**

(i) If a|b and b|c, then a|c.
(a) true (b) false (c) maybe (d) can't be said.

(ii) If $\emptyset$ denotes Euler's totient function, then value of $\emptyset$(37) is
(a) 24 (b) 37 (c) 36 (d) 1.

(iii) DES uses a key generator to generate sixteen _______ round keys.
(a) 32-bit (b) 48-bit (c) 54-bit (d) 42-bit.

(iv) Message authentication code is also known as
(a) key code (b) hash code
(c) keyed hash function (d) message key hash function.

(v) Which one of the following is not a public key distribution technique?
(a) Public-key certificates (b) Hashing certificates
(c) Publicly available directories (d) Public-key authority.

(vi) Digital signature cannot provide ________ for the message.
(a) integrity (b) confidentiality
(c) non-repudiation (d) authentication.

(vii) In ______, there is a single path from the fully trusted authority to any certificate.
(a) X.509 (b) PGP (c) KDC (d) none of the above.

(viii) SSL provides only ___________.
(a) authentication (b) confidentiality
(c) integrity (d) durability.

(ix) "A user intending to connect to one LAN may unintentionally lock onto a wireless access point from the neighboring network." Which type of Wireless network threat would you classify this under?

(a) malicious threat (b) network injection
(c) denial of service (d) accidental association.

(x) What is a genesis block in a blockchain system?
(a) the first block of a blockchain
(b) a famous block that hardcoded a hash of the book of genesis onto the blockchain
(c) the first block after each block halving
(d) the 2nd transaction of a blockchain.

Group – B

2. (a) Distinguish between active and passive security attacks.

(b) Give an example of replay attacks. Why are they considered to be fatal?

(c) List five basic properties of a good encryption algorithm.

4 + 4 + 4 = 12

3. (a) Prove the following: [(a mod n) (b mod n)] mod n = (a b) mod n.

(b) State and illustrate the Chinese Remainder Theorem with an example.

(c) Find the primitive root of 7.

5 + 5 + 2 = 12

Group – C

4. (a) Using the Vigenère cipher, encrypt the word "explanation" using the key leg.

(b) Explain the avalanche effect.

9 + 3 = 12

5. (a) What is a meet-in-the-middle attack in context of double DES?

(b) What is triple encryption? Why is the middle portion of 3DES a decryption rather than an encryption?

6 + (3 + 3) =12

Group – D

6. (a) Perform encryption and decryption using the RSA algorithm, for the following: p = 3; q = 11, e = 7; M = 5.

(b) Explain factoring attack and timing attack on RSA.

6 + (3 + 3) =12

7. (a) (i) How can two parties Bob and Alice initiate a secure communication using symmetric key cryptography in an open network environment, if they do not possess any asymmetric keys? You can assume that a public key authority is available.

(ii) Now if they possess asymmetric keys, how will Bob and Alice initiate a secure communication using symmetric key cryptography in the open network environment?

(b) Briefly explain the man-in-the-middle attack on Diffie-Hellman key exchange protocol.

(4 + 4) + 4 = 12

Group – E

8. (a) Consider a situation: an attacker (A) creates a digital certificate, puts a genuine organizations name (say Bank B) and puts the attacker's own public key. You get this certificate from the attacker, without knowing that the attacker is sending it. You think it is from the Bank B. How can this be prevented or resolved?
In another situation, the attacker (A) changes the bank's genuine certificate by replacing the bank's public key in the certificate with his own. How can this be prevented or resolved?

(b) What are the five principal services provided by PGP?

(3 + 4) + 5 = 12

9. (a) Consider a program D, which when run on a program P, i.e., if we run D(P), would return TRUE (if P is a virus) and FALSE (if P is not a virus). Now consider the following program:

```
Program CV :=
{. . .
    main-program :=
    {
        if D(CV) then goto next:
        else infect-executable;
    }
    next:
}
```

Here infect-executable is a module that scans memory for executable programs and replicates itself in those programs. Determine if D can correctly decide whether CV is a virus.

(b) Explain the parking lot attack that can be launched on wireless networks. What security measures can be taken to mitigate this attack?

6 + (3 + 3) = 12

Department & Section	**Submission Link**
MCA	https://classroom.google.com/c/MzE0NDg4MjY4OTM1/a/MzcxNTg0NDYyNjQ4/details