NETWORK SECURITY
(ECEN 3234)

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) An asymmetric-key (or public-key) cipher uses
(a) 1 Key (b) 2 Key (c) 3 Key (d) 4 Key.

(ii) The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not
(a) Authenticated (b) Joined (c) Submit (d) Separate.

(iii) The substitutional cipers are
(a) Monoalphabatic (b) Sami alphabetic
(c) polyalphabetic (d) both (a) and (c).

(iv) For RSA to work, the value of P must be less than the value of
(a) p (b) q (c) n (d) r.

(v) Calculate the GCD of 1160718174 and 316258250 using Euclidean algorithm
(a) 882 (b) 770 (c) 1078 (d) 1225

(vi) The multiplicative Inverse of 24140 mod 40902 is
(a) 2355 (b) 5343 (c) 3534 (d) Does not exist.

(vii) DES follows
(a) Hash Algorithm (b) Caesars Cipher
(c) Feistel Cipher Structure (d) SP Networks.

(viii) The number of tests required to break the Double DES algorithm are
(a) 2112 (b) 2111 (c) 2128 (d) 2119.

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

(x) Use Caesar's Cipher to decipher the following
HQFUBSWHG WHAW
(a) ABANDONED LOCK (b) ENCRYPTED TEXT
(c) ABANDONED TEXT (d) ENCRYPTED LOCK.

Group – B

2. (a) What is the difference between mono alphabetic and poly alphabetic cipher?

(b) Explain in detail Feistel Block Cipher structure with neat sketch.

4 + 8 = 12

3. (a) Illustrate and explain the key generation process in Data Encryption Standard (DES).

(b) What is double DES? What kind of attack on double DES makes it useless?

8 + 4 = 12

Group – C

4. (a) Write the RSA algorithm for Encryption and Decryption. Given p = 3, q = 11, e = 7, & m = 5, perform RSA encryption and decryption.

(b) Briefly explain the idea behind Elliptic Curve Cryptography (ECC)? Define the public & private keys in this system.

8 + 4 = 12

5. (a) Briefly explain Deffie Hellman key exchange with an example.

(b) Explain the Chinese remainder theorem with an example?

6 + 6 = 12

Group – D

6. (a) Write the methodology involved in computing the keys in Secure Sockets Layer (SSL) protocol.

(b) Describe how master secret is created from pre-master secret in Transport Layer Security (TLS).

8 + 4 = 12

7. (a) List and briefly define three classes of intruders. What is the difference between statistical anomaly detection and rule-based intrusion detection?

(b) List and briefly define four techniques used to avoid guessable passwords.

(3 + 4) + 5 = 12

Group – E

8. (a) What is the role of compression in the operation of a virus? Discuss the typical phases of operation of a virus or worm?

   (b) List three design goals for a firewall. What is the difference between a packet-filtering router and a stateful inspection firewall?

(2 + 4) + (2 + 4) = 12

9. Write short notes on any *three* of the following: **(4 × 3) = 12**
   (i) Cipher Block Chaining Mode
   (ii) Confusion and Diffusion properties of Modern Ciphers
   (iii) Message authentication code (MAC)
   (iv) Mix Columns Transformation in AES cipher
   (v) Euler's totient function

Department & Section	Submission Link
ECE	https://classroom.google.com/w/Mjk5ODU4Nzc3MjI0/tc/MzY0NTI0Njg0MjQz