B.TECH/IT/6TH SEM/INFO 3233/2021

CRYPTOGRAPHY & NETWORK SECURITY (INFO 3233)

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) ___________ suffers from Meet in the Middle attack.
(a) Double DES (b) Triple DES
(c) RSA (d) SSL

(ii) ___________ is a Computationally secure encryption algorithm.
(a) DES (b) BDE
(c) RC5 (d) Both a and c

(iii) ___________ cipher facilitate one to many substitution
(a) Polyalphabetic (b) Polygram
(c) Homophonic (d) Monoalphabetic

(iv) ___________ mode suffers from message stream modification attack.
(a) CFB (b) OFB
(c) Both (a) and (b) (d) None of these

(v) ___________ algorithm uses 8 rounds of encryption.
(a) IDEA (b) DES
(c) RSA (d) Both a and b

(vi) DNS Secure protocol is a countermeasure used in ___________ attack.
(a) PEM (b) Pharming
(c) SSL (d) None of these

(vii) OSI position of ___________ is between transport and application.
(a) IPSec (b) PGP
(c) SSL (d) None of these.

(viii) ___________ is susceptible to Bucket Brigade attack.
(a) Diffie-Hellman key exchange algorithm (b) Double DES algorithm
(c) Both(a) and (b) (d) None of These

(ix) __________ firewall does not hinder system performance.

(a) Hardware (b) Software
(c) Hybrid (d) None of these

(x) Alert protocol is a sub protocol of __________ .

(a) DES (b) IDEA
(c) Blowfish (d) SSL

Group – B

2. (a) State the cipher text for the plain text "**25, Elgin road, Kolkata-700126**"using Playfair substitution technique. Keyword to be used is **NETWORKSECURITY** (*Step detailing and diagram mandatory for above problem.*)

(b) State the cipher text for the plain text "***cryptography and network security***" using the following techniques:
(i) Rail Fence technique
(ii) Simple Columnar Transposition technique up to 3 rounds with keys for First round (6,3,2,1,4,5) Second round (5,4,3,2,1,6) and Third round(2,4,6,3,5,1) (*Step detailing and diagram mandatory for above problem.*)

(c) Differentiate between Masquerade and Pharming.

5 + (2 + 3) + 2 = 12

3. (a) Discuss different types of attack on an encrypted text performed by Cryptanalyst.

(b) State the conditions for an encryption algorithm to be computationally secure.

(c) Differentiate between Symmetric key cryptography and Asymmetric key cryptography.

5 + 2 + 5 = 12

Group – C

4. (a) Explain the following algorithm modes with neat diagram:
(i) Cipher feedback mode
(ii) Electronic Codebook mode
(iii) Cipher Block Chaining mode

(b) Explain Diffie-Hellman key exchange algorithm.

9 + 3 = 12

5. (a) Explain RC5 encryption algorithm in detail with neat diagram.

(b) Explain key generation in IDEA encryption algorithm from round 1 to 4.

(c) Discuss Single round encryption of DES algorithm in detail with neat diagram.

4 + 4 + 4 = 12

Group – D

6. (a) Explain RSA algorithm in detail. Calculate public key and private key for p=7 and q=11 using RSA algorithm.

   (b) State the properties of Digital Signature.

   (c) Explain the working of Authentication token.

(3 + 3) + 3 + 3 = 12

7. (a) Differentiate between Certificate based authentication and Biometric authentication.

   (b) State any four requirements of Hash function.

   (c) Explain the working of HMAC algorithm in detail with neat diagram.

4 + 4 + 4 = 12

Group – E

8. (a) Why is Base-64 encoding required in email security protocols? Discuss about different types of Firewall Configurations with neat diagrams.

   (b) Explain the working of Record protocol in detail with neat diagram. Explain the concept of key rings in PGP.

(1 + 6) + (3 + 2) = 12

9. (a) Describe with diagram how VPN protects the traffic passing between two hosts on two different private networks.

   (b) Explain the following phases of handshake protocol in SSL with neat diagram:
   (i) Server authentication and key exchange
   (ii) Client authentication and key exchange.

   (c) Explain with neat sketch, the working of PEM mail security protocol.

4 + 4 + 4 = 12

Department & Section	Submission Link
IT	https://classroom.google.com/c/Mjk4NjI3NTcwNTgw/a/MzY0NjQzNzYzMTUy/details