B.TECH/IT/8TH SEM/INFO 4243/2021

CRYPTOGRAPHY & NETWORK SECURITY (INFO 4243)

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

Figures out of the right margin indicate full marks.

Candidates are required to answer Group A and <u>any 5 (five)</u> from Group B to E, taking <u>at least one</u> 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) __________ is an attack in Authentication
(a) Confidentiality (b) Integrity
(c) Fabrication (d) None of these

(ii) __________is not a Computationally secure encryption algorithm.
(a) DES (b) IDEA
(c) RC5 (d) None of these

(iii) ____________cipher uses Vignere table
(a) Polyalphabetic (b) Polygram
(c) None of these (d) Monoalphabetic

(iv) _________ mode uses block cipher.
(a) CFB (b) OFB
(c) Both (a) and (b) (d) None of these

(v) _________ algorithm uses 8 rounds of encryption.
(a) DES (b) IDEA
(c) FEAL (d) SAFER

(vi) ________ algorithm can use 0-255 rounds of encryption.
(a) IDEA (b) DES
(c) RSA (d) RC5

(vii) ________ algorithm produces 128 bit hash value.
(a) MD5 (b) SHA
(c) All of these (d) None of these

(viii) Bastion host used in Screened subnet firewall is__________
(a) Application Gateway (b) Circuit Gateway
(c) Packet Filtering router (d) None of these

(ix) _________ forms the basis of randomness in an authentication token.
(a) Password (b) Seed
(c) User Id (d) None of these.

(x) Alert protocol is a sub protocol of__________
(a) DES (b) IDEA
(c) Blowfish (d) SSL

Group – B

2. (a) Discuss different kind of attacks possible on encrypted text. Differentiate between Replay attack and DNS spoofing.

(b) State the cipher text for the plain text "***fundamentals of network cryptology***" using(i) Caesar cipher technique with key=5 and (ii) Rail Fence technique.

(5 + 3) + 4 = 12

3. (a) Explain different kinds of Active attack. State the cipher text for the plain text "***NETWORK SECURITY***" using one time pad technique. key to be used is " **BARCEKAPERALONA**"

(b) Construct a vigenere table for poly alphabetic substitution technique. Using the table find the cipher text for plain text **"cryptology and security"**. Key to be used is **cryptography.**

(3 + 3) + (2 + 4) = 12

Group – C

4. (a) Explain Bucket Brigade attack with attached numerical parameters [n=11, g=7; x for sender=3; y for receiver=9 and x=8, y=6 for attacker].

(b) Discuss Single round encryption of IDEA algorithm in detail including Output transformation round.

4 + 8 = 12

5. (a) Discuss single round operation of DES encryption algorithm with neat sketch.

(b) Explain the following algorithm modes with neat diagram:
(i) Cipher feedback mode.
(ii) Electronic codebook mode.

5 + 7 = 12

Group – D

6. (a) Explain RSA algorithm in detail. Calculate public key and private key for p=7 and q=13 using RSA algorithm.

(b) What is Authentication token? State the features of Authentication token. Explain the working of Authentication token.

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

7. (a) Differentiate between Challenge-Response authentication token and Time based authentication token

(b) State the requirements of Hash function.

(c) Differentiate between Certificate based authentication and Biometric authentication.

4 + 4 + 4 = 12

Group – E

8. (a) Explain establish security capabilities phase of handshake protocol in SSL. Explain server authentication and key exchange phase of handshake protocol in SSL.

(b) Explain client authentication and key exchange phase of handshake protocol in SSL.

4 + 4 + 4 = 12

9. (a) Assume a 24-bit input as 101010111100000101100110, and transform it into its Base-64 equivalent.

(b) Explain three ideas to understand the whole concept of PGP Certificates.

6 + 6 = 12

Department & Section	**Submission Link**
IT	https://classroom.google.com/c/Mjk4NjI3NTY2MzU5/a/MzYwMTU0OTY3NzQz/details