M.TECH/IT/2ND SEM /INFO 5202/2016
2016

CRYPTOGRAPHY AND NETWORK SECURITY
(INFO 5202)

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 alternatives for the following: **10 x 1=10**

(i) .... is an attack in Authentication
(a) Confidentiality (b) Integrity
(c) Fabrication (d) none of these

(ii) .... mode cannot be used for transmitting long messages.
(a) ECB (b) CBC
(c) OFB (d) All of these

(iii) .... algorithm uses 8 rounds of encryption.
(a) IDEA (b) DES
(c) FEAL (d) Both a and c

(iv) .... mode uses stream cipher.
(a) CFB (b) OFB
(c) All of these (d) None of these.

(v) OSI position of .... is between transport and application.
(a) IPSec (b) SSL
(c) both (a) & (b) (d) None of these.

(vi) .... is suitable for application where key does not change frequently
(a) AES (b) RC5
(c) MD2 (d) BLOWFISH.

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

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

(ix) .... Forensic tool is used for recovering information from mobile devices.
(a) HELIX 3 (b) XRY
(c) COFEE (d) None of These.

(x) .... is a combination of Cryptography and Cryptanalysis
(a) Linear Cryptanalysis (b) Differential Cryptanalysis
(c) Cryptology (d) None of these.

Group - B

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

(b) State the cipher text for the plain text "***cryptographyandnetworksecurity***" using(i) Caesar cipher technique with key=7 and (ii) Rail Fence technique.

(c) Discuss the concept of Digital Envelope.

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

2 + 4 + 2 + 4 = 12

3. (a) State the cipher text for the plain text "***cryptographyandnetworksecurity***" using
(i) PlayFair cipher technique with keyword= PLAYFAIR
(ii) Simple Columnar Transposition technique upto 3 rounds with keys for First round (5,3,2,1,4) Second round (4,3,2,1,5) and Third round (5,4,3,1,2)
(*Step detailing and diagram mandatory for above problem.*)

(b) Differentiate between Brute force attack and Cryptanalysis.

(c) Discuss different types of tool for Digital Forensic Analysis (Any four).

(3+3)+ 2 + 4 = 12

Group - C

4. (a) State the principles of Diffusion and Confusion. Illustrate the Key Shifting process in IDEA upto 8 rounds, showing key generation in each round with suitable example.

(b) Differentiate between Linear cryptanalysis and Differential cryptanalysis.

(c) Explain the encryption process of RC5 algorithm in detail.

(2+4) + 2 + 4 = 12

5. (a) Discuss the operation of CFB (Cipher Feedback) mode in detail.

(b) Why do we need Triple DES instead of Single DES algorithm? Why EDE mode is used instead of EEE mode in Triple DES?

(c) Compare between RC5, Blowfish, SAFER and AES algorithm.

4 + (2+2) + 4 = 12

Group - D

6. (a) Discuss the properties of Hash function.

(b) Explain SSL Handshake protocol in detail with suitable diagram.

(c) Why a Digital Certificate needs to be revoked?

(d) Compare between MD5 and SHA-1 algorithms.

2 + 6 + 2 + 2 = 12

7. (a) Explain the working principle of HMAC in detail with suitable diagram.

(b) Discuss the working principle of SHA1 in detail with suitable diagram.

(c) Discuss in detail the steps involved in creation of Digital Certificate.

4 + 4 + 4 = 12

Group - E

8. (a) Perform encryption and decryption using the RSA algorithm for the following: (p=3, q=11, e =7 and M=5) where p and q are initial two prime numbers and M is plaintext input). What are the limitations of RSA algorithm?

(b) Explain briefly Chinese Remainder Theorem. Find an integer that has a remainder 0f 3 when divided by 7 and 13, but is divisible by 12.

(c) Find the result of 3^{12} mod 11, 6^{12} mod 11 and 20^{62} mod 77 using Fermat's Little theorem.

4 + 4 + 4 = 12

9. (a) Users A and B use the Diffie-Hellman key exchange algorithm with a common prime q =71 and primitive root $\alpha = 7$.
   (a) If User A has a private key X_A =5, what is A's public key Y_A?
   (b) If User B has private key X_B = 12, what is B's public key Y_B?
   (c) What is the shared secret key?

(b) Use extended Euclidian Algorithm to find inverse of $(x^4 + x^3 + 1)$ in GF(2^5) using the modulus $(x^5 + x^2 + 1)$.

(c) Explain briefly MILLER-RABIN Primality test. Does the number 561 pass this test?

(1+1+2) + 4 + 4 =12