SPECIAL SUPPLE B.TECH/CSE/7TH SEM/CSEN 4162/2018

CRYPTOGRAPHY AND NETWORK SECURITY
(CSEN 4162)

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) In symmetric key cryptography, the private key is kept by
- (a) sender
- (b) receiver
- (c) sender and receiver
- (d) there is no private key in the network.

(ii) What is Advanced Encryption Standard (AES)?
- (a) Block cipher
- (b) Stream cipher
- (c) Bit cipher
- (d) None of the mentioned.

(iii) AES uses a _____ bit block size and a key size of _____ bits.
- (a) 128; 128 or 256
- (b) 64; 128 or 192
- (c) 256; 128, 192, or 256
- (d) 128; 128, 192, or 256.

(iv) In cryptography, the order of the letters in a message is rearranged by
- (a) transposition ciphers
- (b) substitution ciphers
- (c) both (a) and (b)
- (d) none of the mentioned.

(v) Hacking refers to
- (a) data access without permission
- (b) data updating without permission
- (c) data deletion without permission
- (d) all of the above.

(vi) If an efficient algorithm for factoring large number is discovered which of the following schemes will be known to be not secure?
- (a) AES
- (b) Diffle-Hellman
- (c) RSA
- (d) EI Gammal.

(vii) In the digital signature technique, the sender of the message uses _____ to create cipher text
(a) own symmetric key (b) own private key
(c) the receiver's private key (d) receiver's public key.

(viii) An attack on a cipher text message where the attacker attempts to use all possible permutations and combinations is called
(a) Brute-Plaintext attack (b) Birthday attack
(c) Known-Plaintext attack (d) Chosen-plaintext attack.

(ix) The process to discover plain text or key is known as
(a) cryptanalysis (b) crypto design
(c) crypto processing (d) crypto graphic.

(x) Which one of JUPITER, Blowfish, RC6, Rijndael and Serpent is not a cryptographic algorithm?
(a) JUPITER (b) Blowfish
(c) Serpent (d) Rijndael.

Group – B

2. (a) Discuss the concept of Caesar Cipher. Use Caesar cipher with key = 15 to encrypt the message "Hello".

(b) Explain the Diffie-Hellman Key Exchange Algorithm. Alice and Bob want to establish a secret key using the Diffie-Hellman Key Exchange Algorithm. Assuming the values as n = 11, g = 5, x = 2 and y = 3, find out the values of the secret keys K1 and K2.

(c) Distinguish between message integrity and message authentication.

(1 + 1) + (3 + 2) + (1 + 4) = 12

3. (a) Find the values of (i) 7^7 mod 9 and (ii) 3^{110} mod 13.

(b) Explain with examples the various active and passive attacks that can be performed by an intruder.

(c) Discuss the algorithm for rail fence technique. What will be the output of the following plain text if rain fence technique was used to encode it?
Plain Text: We the people of India

(1.5 + 1.5) + 5 + 3 = 12

Group – C

4. (a) Discuss the pros and cons of symmetric and asymmetric key cryptography.

   (b) What are the 4 main stages of AES operation? What would be the following state matrix after the Shift Row Operation?

ac	21	34	ec
02	76	ea	02
13	50	46	a4
92	76	ab	Ba

   (c) Consider a plain text alphabet ***G***. Using RSA algorithm and the values of E, D and N as 3, 11 and 15, find out the encrypted cipher text. Verify that on decryption, the cipher text transforms back to the plain text ***G***.

3 + 5 + 4 = 12

5. (a) State and compare the different models of a block cipher.

   (b) Explain the encryption process of Cipher Feedback (CFB) Mode using suitable diagram.

   (c) Explain double DES and triple DES using suitable diagrams.

4 + 4 + 4 = 12

Group – D

6. (a) What are the key requirements of message digests? Why is SHA more secured than MD5?

   (b) What is authentication? What are the objectives of authentication?

   (c) Discuss the weaknesses of the password based authentication method. Explain the biometric authentication method.

4 + 4 + 4 = 12

7. (a) What do you understand by two-factor authentication method?

   (b) Explain the Kerberos third-party authentication model with suitable diagram.

   (c) What is digital signature? Write a short note on the Digital Signature Algorithm (DSA).

3 + 4 + (2 +3) = 12

Group – E

8. (a) What is a firewall? What are the different types of firewall? Explain the working principle of each briefly.

   (b) What are the limitations of a firewall?

   (c) What is a worm? How does it differ from a virus?

6 + 3 + 3 = 12

9. (a) What are the different security services provided by PGP?

   (b) Explain how PGP provides confidentiality and authenticity of electronic mails.

   (c) Explain the necessity of base-64 conversion in PGP.

3 + 5 + 4 = 12