

Printed Pages : 4



ECS029

(Following Paper ID and Roll No. to be filled in your Answer Book)

PAPER ID : 120601

Roll No.

--	--	--	--	--	--	--	--	--	--

B.Tech.

(SEM. VI) THEORY EXAMINATION, 2014-15
CRYPTOGRAPHY & NETWORK SECURITY

Time : 3 Hours]

[Total Marks : 100

- Note:** (1) Attempt all question.
 (2) All question carry equal marks.

1 Attempt **any four** question. **5×4=20**

- (a) Describe the encryption and decryption process of a block cipher in Cipher Feedback (CFB) mode.
- (b) Encrypt plaintext "controller of" using play fair cipher with key "examination". Take your own assumption as required.
- (c) In case of Hill Cipher answer the following.
 - (i) Give the relationship between the key and ciphertext if the plaintext is a multiplicative identity matrix (I).

- (ii) Obtain the decryption key to be used for deciphering the cipher text, if the following key K are used for the enciphering the message.

$$K = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$$

- (d) What is double DES? What kind of attack on double DES makes it useless?
- (e) What will be the required mechanism for the following attacks? Also write the services offered by the respective mechanism.
- (i) Masquarde
 - (ii) Modification of Message
 - (iii) Reading of message
 - (iv) Denial of service
 - (v) Traffic analysis
- (f) Distinguish between the following:
- (i) Differential and linear cryptanalysis.
 - (ii) Feistel and non-feistel block cipher.

2 Attempt **any four** question. **5×4=20**

- (a) Using Chinese Remainder Theorem (CRT) solve the following simultaneous congruence's :
- $$x \equiv 3 \pmod{9}, \quad x \equiv 2 \pmod{10} \text{ and } x \equiv 3 \pmod{11}.$$

- (b) Apply Miller Rabin Algorithm using base 2 to test whether the number 341 is composite or not.
- (c) Perform encryption and decryption using the RSA algorithm, for $p=5$, $q=11$, $e=3$ and $M=9$
- (d) Compare DES and AES. Which one is bit-oriented? Which one is byte - oriented? Also list possible approaches to attacking the RSA algorithm.
- (e) What is the advantages of using OFB over the other block cipher modes of operation?
- (f) What is the difference between statistical randomness and unpredictability?

3 Attempt **any two** question. **10×2=20**

- (a) What is message authentication code? How it differs from hash function? Explain different properties of a hash function and general structure of Secure Hash Code.
- (b) What do you understand by birthday attack? With the help of suitably chosen scenario, explain how a birthday attack can be launched.
- (c)
 - (i) What is digital signature? What is direct and arbitrated digital signature. How a digital signature differs from message authentication?
 - (ii) Discuss the process of signing and verifying in DSS.

4 Attempt **any two** question. **10×2=20**

- (a) Diffie-Hillman key exchange algorithm is vulnerable to man-in-the-middle attack, how? Users A and B use a Diffie-Hillman key exchange protocol with a chosen common prime $p = 23$ and primitive root $g = 7$. Given that private key of A and B are 3 and 5 respectively. Determine the public key of A and B. Further determine the shared secret keys K.
- (b) Explain single round of DES and generation of key with block diagram.
- (c) Write short notes on any two of the following.
 - (i) Kerberos Realms
 - (ii) Public key distribution
 - (iii) X.509 certificate.

5 Attempt **any two** question **10×2=20**

- (a) Explain the concept of dual signature in context of Secure Electronic Transaction (SET). Briefly describe the sequence of events that are required for a SET.
- (b) Explain the services of PGP.
- (c) Write short notes on any two of the following:
 - (i) Virus phases and its types
 - (ii) Intrusion detection
 - (iii) Secure Socket Layer (SSL)