

Printed Pages : 4



EIT-701

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

PAPER ID : 113702

Roll No.

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

B. Tech.(SEM. VII) (ODD SEM.) THEORY
EXAMINATION, 2014-15**CRYPTOGRAPHY AND NETWORK SECURITY**

Time : 3 Hours]

[Total Marks : 100

- 1 Attempt any **four** questions : **(5×4=20)**
- (a) Explain Feistel Encryption and Decryption algorithms. What is the difference between Diffusion and Confusion?
 - (b) Compare and contrast substitution techniques with Transposition techniques under classical encryption.
 - (c) What is the most security-critical component of DES round function? Give a brief description of this function.
 - (d) What is the difference between block cipher and stream cipher? What are the different modes of block cipher operation? Explain any one of them.
 - (e) What is the idea behind meet-in-middle attack? How it can be avoided in 3 DES?

113702]

1

[Contd...

- (f) The Hill Cipher uses the following key for enciphering the message.

$$K = \begin{pmatrix} 3 & 2 \\ 5 & 7 \end{pmatrix}$$

Obtain the decryption key used for deciphering the cipher text.

2 Attempt any **four** questions : (5×4=20)

- (a) Describe RSA algorithm, encryption and decryption function. In RSA, given $e=07$ and $n=33$, encrypt the message "ME" using 00 to 25 for letters A to Z.
- (b) Write the pseudo code for Miller Rabin primality testing. Test whether 61 is prime or not using the same Miller Rabin test.
- (c) Describe the Fermat's Little Theorem. Using Fermat's theorem, find the value of $3^{201} \pmod{11}$.
- (d) Define Ring and Field. Give an example of ring which is not a field.
- (e) Illustrate the concept of Chinese Remainder Theorem. By using Chinese Remainder Theorem solve the simultaneous congruence $X \equiv 2 \pmod{P}$ for all $P \in \{3, 5, 7\}$
- (f) Describe Diffie-Hellman Key Exchange Algorithm. Users A & B use the Diffie-Hellman key exchange technique a common prime $q=83$ and a primitive root $\alpha=13$.
- i. If user A has private key 5, what is A's public key?
 - ii. If user B has private key 12, what is B's public key?
 - iii. What is the shared key?

113702]

2

[Contd...

3 Attempt any **two** questions : (10×2=20)

- (a) Write the Digital Signature Algorithm (DSA) of Digital Signature Standard. What is the implication if same K (secret per message) is used to sign two different message using DSA?
- (b) What are the requirements of a Message Authentication Code (MAC)? Discuss the logical structure, components and algorithmic steps of MD5 algorithm.
- (c) (i) Differentiate between the following:
 - a) Hash Code and Message Authentication Code (MAC)
 - b) Weak collision resistance and Strong collision resistance.
- (ii) Describe birthday attack against any hash function. Give the mathematical basis of the attack.

4 Attempt any **two** questions : (10×2=20)

- (a) Enlist various services supported by S/MIME. Explain how S/MIME supports these services. What is the purpose of content type field in MIME header ?
- (b) What is Digital Certificate? Give the format of X.509 certificate showing the important elements of the certificate. How is an X.509 certificate revoked ?
- (c) Explain the full-service Kerberos environment? What are the principle differences between version 4 and version 5 of Kerberos ?

113702]

3

[Contd...

- 5 Attempt any **two** questions : **(10×2=20)**
- (a) Explain the concept of security association (SA) in IPSEC. What is the use of ISAKMP protocol in IPSEC?
 - (b) Who are the participants in SET (Secure Electronic Transaction) system? Describe in brief the sequence of events that are required for a transaction.
 - (c)
 - (i) What are the types of Firewall? Explain them
 - (ii) What do you understand by Trusted System? Explain the concept of reference monitor.

113702]

4

[4925]