C 1169 **(Pages : 2)**

Name...

Reg. No.......................................

SIXTH SEMESTER B.TECH. (ENGINEERING) [09 SCHEME] DEGREE EXAMINATION, APRIL 2016

CS/PTCS 09 L01—INFORMATION SECURITY

Time : Three Hours Maximum : 70 Marks

Part A

Answer **all** *questions.*

I. (a) Users A and B use the Diffie Hellman key exchange technique a common prime q = 11 and a primitive root alpha = 7. If user A has private key $X_A = 3$, what is A's public key Y_A ?

(b) A transposition block has 10 inputs and 10 outputs. What is the order of permutation group ? What is the key size ?

(c) List the types of security attacks.

(d) Define the roles of Oakley key determination protocol and ISAKMP in IPSec.

(e) Explain how malicious programs exploit the principle of stack overflow for attacking systems.

(5 × 2 = 10 marks)

Part B

Answer any **four** *questions.*

II. (a) Describe the block cipher modes of operation in detail.

(b) Explain public key certificates.

(c) What are the positive and negative effects of firewall ?

(d) Mention the uses of Biometric authentication.

(e) Why is there a separate Change Cipher Spec Protocol in SSL and TLS rather than including a change_cipher_spec message in the handshake protocol ? Justify your answer.

(f) Mention the security features provided by Windows Operating system.

(4 × 5 = 20 marks)

Part C

Answer **all** *questions.*

III (a) Name the main components of the public key cryptosystem and formulate the security requirements. Discuss the use of the system for secrecy and authenticity.

Or

Turn over

(b) Let the prime numbers be $p = 11$ and $q = 13$, public key $e = 11$ and plain text M = 7. Perform encryption and decryption using RSA algorithm.

IV (a) Discuss about access control mechanisms and covert channels.

Or

(b) What is two —factor authentication? Explain in detail.

V (a) Bring out the importance of security associations in IP.

Or

(b) What were the problems that the Kerberos address? Explain in detail.

VI (a) Explain Operating system security functions in detail.

Or

(b) Write a note on the following :

(i) Software recovery Engineering.

(ii) Trusted OS.

(4 × 10 = 40 marks)