

RF-4041-42

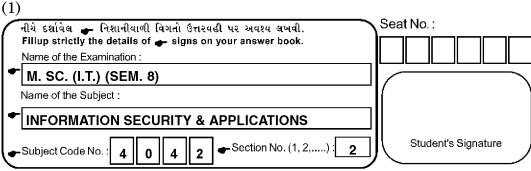
M. Sc. (I.T.) (Sem. VIII) Examination April/May - 2010

Information Security & Applications

Tim	${f RF-4041}$ [Total Marks : 7	70
Inst (1)	ructions:	
ની Fi Ni •	દર્શાવેલ → નિશાનીવાળી વિગતો ઉત્તરવહી પર અવશ્ય લખવી. up strictly the details of → signs on your answer book. me of the Examination : . SC. (I.T.) (SEM. 8) me of the Subject : IFORMATION SECURITY & APPLICATIONS	_
SI	oject Code No. : 4 0 4 1 Section No. (1, 2,) : 1	/
(2) (3)	Write sections I and Section II in separate sheet. Draw the figure and give example whenever necessary.	
1	 (a) Answer the following (any three) (i) State the difference between block and stream cipher? (ii) Explain OFB mode block cipher operation. (iii) Explain CFB mode. (iv) Explain SPI. 	6
	(b) Answer following questions (any two) (i) Write a note on stenography. (ii) Write a note on rotor machines. (iii) Explain key management using publicly available directory.	8
2	Answer the followig (any one) (i) Explain public key authority and public key certificates. (ii) What are the different ways of distribution of public keys. (iii) Write a note on polyalphabetic ciphers.	6
3	 (i) Write a note on S-DES key generation and encryption. (ii) Write a note on MD5 digest. (iii) Write a note on AES algorithm. 	
	(iv) Users A and b use Dieffie-Hellman key exchange technique a common prime $q = 71$ and a primitive root a (alpha_ = 7. If user A has private key $X_A = 5$, find A's private key Y_A . If user B has private key $X_B = 12$, find B's private key. What is the shared key?	ıe
RF-	041-42] 1 [Contd.	

RF-4042

Instructions:



- (2) Write sections I and Section II in separate sheet.
- (3) Draw the figure and give example whenever necessary.
- 4 Answer the following (any three)

18

- (i) State and explain the different types of replay attacks, also state the ways to cope with it.
- (ii) Discuss Needham/Schroeder protocol. Also discuss the Denning's revised protocol.
- (iii) Explain Oakley key determination protocol.
- (iv) Explain play fair cipher and encrypt M='FOOT" with key = "OUR".
- 5 (a) Answer the following: (any two)

8

- (i) State the firewall characteristics.
- (ii) What is SA and SA parameters?
- (iii) Explain ESP. Also explain ESP in tunnel and transport mode.
- (b) Answer the following:
 - (i) Explain in SA selectors?

6

OR

(i) Explain RC4 stream cipher?

- 6
- (ii) Explain the arbitrated digital signatures in brief.

RF-4041-42] 2 [200]