



RF-4041-42

M. Sc. (I.T.) (Sem. VIII) Examination
April / May – 2010
Information Security & Applications

Time : 3 Hours]

[Total Marks : 70

RF-4041

Instructions :

(1)

नीचे दशांशके निशानीवाणी विगतो उत्तरवही पर अवश्य लपवी. Fillup strictly the details of signs on your answer book.		Seat No. :	
Name of the Examination :		<input type="text"/>	
M. SC. (I.T.) (SEM. 8)		<input type="text"/>	
Name of the Subject :		<input type="text"/>	
INFORMATION SECURITY & APPLICATIONS		<input type="text"/>	
Subject Code No. : <input type="text"/> 4 <input type="text"/> 0 <input type="text"/> 4 <input type="text"/> 1		Section No. (1, 2,.....) : <input type="text"/> 1	
		Student's Signature	

(2) Write sections I and Section II in separate sheet.

(3) Draw the figure and give example whenever necessary.

- 1 (a) Answer the following (any three) **6**
- (i) State the difference between block and stream cipher?
 - (ii) Explain OFB mode block cipher operation.
 - (iii) Explain CFB mode.
 - (iv) Explain SPI.
- (b) Answer following questions (any two) **8**
- (i) Write a note on stenography.
 - (ii) Write a note on rotor machines.
 - (iii) Explain key management using publicly available directory.
- 2 Answer the followig (any one) **6**
- (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.
- 3 Answer following questions (any three) **15**
- (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?

RF-4042

Instructions :

(1)

नीचे दशावेक निशानीवाणी विगतो उत्तरवडी पर अवश्य कभवी. Fillup strictly the details of signs on your answer book.	Seat No. :
Name of the Examination :	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
<input type="text" value="M. SC. (I.T.) (SEM. 8)"/>	<input type="text" value="Student's Signature"/>
Name of the Subject :	
<input type="text" value="INFORMATION SECURITY & APPLICATIONS"/>	
Subject Code No. : <input type="text" value="4"/> <input type="text" value="0"/> <input type="text" value="4"/> <input type="text" value="2"/>	Section No. (1, 2,.....) : <input type="text" value="2"/>

- (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
- State and explain the different types of replay attacks, also state the ways to cope with it.
 - Discuss Needham/Schroeder protocol. Also discuss the Denning's revised protocol.
 - Explain Oakley key determination protocol.
 - Explain play fair cipher and encrypt M='FOOT' with key = "OUR".
- 5 (a) Answer the following : (any two) 8
- State the firewall characteristics.
 - What is SA and SA parameters?
 - Explain ESP. Also explain ESP in tunnel and transport mode.
- (b) Answer the following :
- Explain in SA selectors? 6
- OR**
- Explain RC4 stream cipher? 6
 - Explain the arbitrated digital signatures in brief. 3
-