* S F - 8 3 5 0 / 2 0 0 *

SF-8350

B. E. III (Sem. VI) Examination

May / June – 2011

Information Technology

Time : Hours] [Total Marks : **100**

Instructions :

(1)

નીચે દર્શાવેલ ☛ નિશાનીવાળી વિગતો ઉત્તરવહી પર અવશ્ય લખવી.
Fillup strictly the details of ☛ signs on your answer book.

Name of the Examination :

☛ **B. E. 3 (Sem. 6)**

Name of the Subject :

☛ **Information Technology**

☛Subject Code No. : **8 3 5 0** ☛Section No. (1, 2,.....) : **Nil**

Seat No. :

Student's Signature

1 (a) Attempt the following : **10**

(i) Explain security attacks. **3**

(ii) Compare unconditionally secure and computationally secure encryption scheme. **3**

(iii) Give encryption and decryption equations for Caesar cipher. **2**

(iv) Enlist possible approaches to attacking the RSA algorithm. **2**

(v) Explain diffusion and confusion with respect to block cipher principles. **2**

(b) Explain single round of Data Encryption Standard (DES) with diagram. **10**

2 (a) Explain AES encryption and decryption with diagram. **7**

OR

(a) Explain Playfair cipher. Using keyword monarchy, find out plaintext for the cipher text DPMULIF. **7**

(b) Discuss RSA algorithm in detail. Using p = 17, q=11, explain the procedure of encryption and decryption for the message M=88. **8**

3 Attempt any **three** : **15**

(i) Explain public key crypto systems. **5**

(ii) What is key distribution ? Explain Key Distribution Scenario. **5**

(iii) What is Euler's Totient Function ? Find $\phi(n)$ for $n = 21, 27$, and 10. **5**

(iv) Write Euclidean algorithm. Find GCD of 1970 and 1066. Are this relatively prime numbers ? Justify your answer.

4 (a) Attempt the following : **5**

(i) Name any two replay attacks.

(ii) State one way property of Hash function.

(iii) SHA-1 uses 4 rounds of 16 steps. (True/False)

(iv) Version 4 of Kerberos makes use of DES (True/False)

(v) Define : SSL Session

(b) Give full form of the following : (any **five**) **5**

(i) DOI

(ii) ESP

(iii) PGP

(iv) SSL

(v) S/MIME

(vi) SMTP.

5 (a) Explain Security Associations parameters. **8**

(b) Explain SSL record Protocol. **7**

OR

5 (a) Explain MD-5 algorithm. **8**

(b) Explain Digital Signature Algorithm. **7**

6 (a) Attempt the following : (any **three**) **15**

(i) Write difference between version 4 and version 5 of Kerberos.

(ii) State the types of firewalls. Explain any one of them.

(iii) Draw X.509 certificate format and explain any three elements of it.

(iv) Explain Birthday Attack.

(b) Attempt the following :

(i) State properties of MAC function. **3**

(ii) Explain S/MIME functions. **4**

(iii) Write benefits of IPSec. **3**
