* S F - 8 3 2 7 / 2 0 0 *

SF-8327

B. E. - III (Sem. VI) (Computer) Examination

May / June - 2011

Information Security

Time : **3** Hours] [Total Marks : **100**

Instruction :

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) (COMPUTER)

Name of the Subject :

☛ INFORMATION SECURITY

☛ Subject Code No. : 8 3 2 7 ☛ Section No. (1, 2,.....) : 1&2

Seat No. :

Student's Signature

SECTION - I

1 (a) Answer the followings: **10**

(i) Define Data Integrity.

(ii) The key size of S-DES is 12 bit. True/False

(iii) Find out cipher text of for following plaintext "The world of Security" with ceaser cipher with key = 3.

(iv) What is block size of DES cipher ?

(v) What is the difference between block cipher and stream cipher ?

(vi) What is brute force attack ?

(vii) What is Transposition cipher ?

(viii) The RSA algorithm uses symmetric cryptography. True/False

(ix) An initialization vector is needed in counter mode. True/False

(x) RC4 is a stream cipher. True/False

(b) Answer the following :

(i) Encrypt "Advanced Encryption" using Hill Cipher. **6**

Use key $K = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$

(ii) Short note on Steganography. **4**

OR

What is difference between Prime and relative prime number ? Explain with example.

2 (a) Explain with diagram general depiction of S-DES encryption algorithm. **8**

(b) Consider Diffie Hellmen scheme with common prime q=71 and primitive root $\alpha = 71$. **6**

(i) If user A has Private Key X_A = 5. What is A's Public key ?

(ii) If user B has Private Key X_B = 12. What is B's Public key ?

(iii) What is shared secret key ?

3 Attempt the following : (any **four**) **16**

(i) In a public key cryptography using RSA, you intercept the cipher text C=10 sent to a user whose public key e=5, n=35. What is Plaintext M ?

(ii) What is the difference between OFB and CFB ?

(iii) Write short note on Key Distribution.

(iv) Explain security of RSA.

(v) Write short note on Euler's Theorem.

SECTION - II

4 (a) Do as directed :

(i) Inclusion of S-Box includes _____ in algorithm
  (a) Non Redundancy
  (b) Non Linearity
  (c) Finiteness
  (d) All of the above

(ii) What is not true about nonce ?
  (a) It can be used for authentication
  (b) It can be a random number
  (c) Time stamp can be used a s nonce
  (d) It can help in avoiding replay attack.

(iii) Which of the below is not true about Stegnography ?
  (a) It is used for data hiding
  (b) It is supplement to Cryptography
  (c) It does not alters the original message
  (d) Silver Threade on Indian Currency note is example of Stegnography.

(iv) In _____ attack, opponent tries all possible key on the cipher text.
  (a) Brute Force
  (b) Replay
  (c) Meet in Middle
  (d) None of the above

(v) Initial Vector (IV) used in SHA is of _____ bits.
  (a) 64
  (b) 128
  (c) 160
  (d) 32

(vi) MD5 uses 5 number of rounds of 16 steps each (True/False).

(vii) Cipher Feedback Block Mode works on block mode (True/False)

(viii) Hash function does not provide Digital Signature (True/False)

(ix) Define padding

(x) Give full form of SSL and TLS.

(b) Explain MD5 in detail with neat diagram. **10**

5 (a) Compare and contrast Link Encryption Approach and End-to-End Encryption Approach with realtime examples. **6**

(b) Explain Secure Electronic Transaction (SET) **9**

OR

5 (a) Define Authentication. Enlist and explain its requirements. **6**

(b) Explain Transport and Tunnel mode on the extension header for Authentication i.e. Authentication Header (AH) for both IPv4 and IPv6. **9**

6 Attempt any **three** : **15**

(i) Define MAC. Explain it in detail with neat diagram.

(ii) Explain in detail TLS (Transport layer Security)

(iii) Explain types of Firewalls

(iv) Explain various ways of distribution of public keys

(v) Give the full form of TGS. Explain its role and significance in Kerberos.
