www.rtupaper.com

8E5002

8E5002

B.Tech. (Sem.VIII) (Main/Back) Examination - 2013
Computer Science
8CS2 Information System Securities
(Common with 8IT2)

Time : 3 Hours

[Total Marks : 80
[Min. Passing Marks : 24

Instructions to Candidates :
Attempt any five questions selecting one question from each unit. All questions carry equal marks. Schematic diagrams must be shown wherever necessary. Any data you feel missing suitably be assumed and stated clearly. Units of quantities used/calculated must be stated clearly.

UNIT - I

1. (a) Discuss the chinese remainder theorem. 8

   (b) Explain:
   (i) Galois field
   (ii) Division algorithm 8

OR

1. (a) State and prove Fermat's little theorem. 8

   (b) What is Primitive root? Explain an algorithm to determine Primitive roots. Determine all the Primitive roots of
   (i) 19 (ii) 25 8

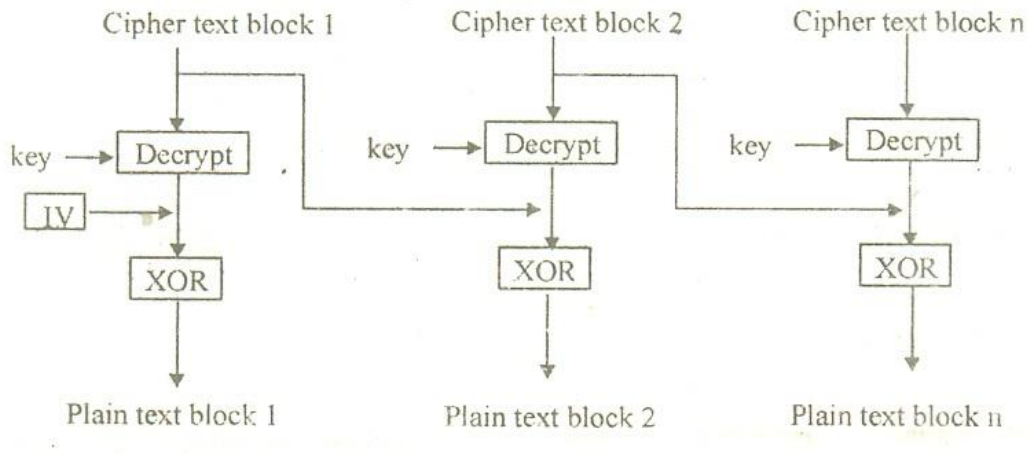
UNIT - II

2. (a) Using the following S-box, Determine 4 bit output for the following 6 bit input :
   (i) 101101 (ii) 110010
   (iii) 011010 (iv) 101010 4

10	00	09	14	04	05	08	11	10	11	12	14	03	01	05	13
13	07	00	09	03	12	07	05	04	07	14	10	09	12	09	14
13	06	04	06	05	11	06	13	07	10	10	11	07	11	08	11
01	10	13	00	00	04	10	09	08	13	03	01	06	10	06	10

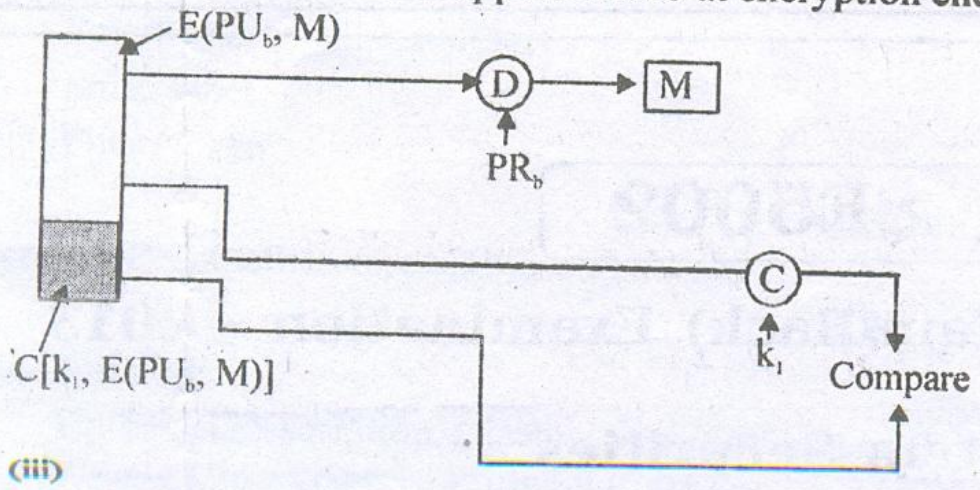
(b) Draw the encryption process of following decryption process.

(i)

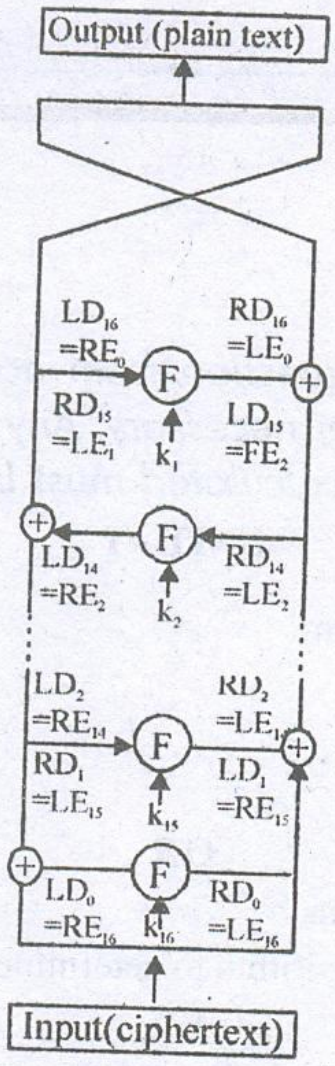


www.rtupaper.com

(ii) Also calculate and append MAC at encryption end.



(iii)



2+2+6

(c) What is the difference between confusion and diffusion. 2

OR

2. (a) Discuss the keyshifting process of International Data encryption algorithm. Also generate the subkey for the each round and output transformation in IDEA. 2+8=10

(b) In DES (Data Encryption Standard) Explain -
(i) Subkey Generation for each round.
(ii) 64 bit key is converted into 56 key.
(iii) Expansion permutation. 2+2+2=6

UNIT - III

3. (a) Perform RSA Encryption/Decryption process for following set of Data.

(i)	P = 5	q = 11	e = 3	M = 9
(ii)	P = 11	q = 13	e = 11	M = 7
(iii)	P = 17	q = 31	e = 7	M = 2

(b) Describe the distribution of Secret Keys using Public Key Cryptosystems. 3+3+3=9

OR 7

3. (a) Explain Diffie-Hellman key exchange algorithm in detail. Also discuss " Man in the Middle Attack" problem with suitable example.

(b) Write a short note on Discrete logarithms. 5+5=10

6

www.rtupaper.com

UNIT - IV

4. (a) What is the difference between Hash and MAC? Discuss the methods of accomplish the confidentiality and authentication using MAC and Hash. **2+8=10**

   (b) What is the digital signature? How authentication is accomplish using digital signature? **6**

OR

4. (a) Describe the MD5 algorithm in detail. Compare MD5 with SHA. **10**

   (b) Describe the various authentication schemes for mutual authentication based on shared secret key. **6**

UNIT - V

5. (a) Explain the concept of Dual signature in context of Secure Electronic Transaction (SET). Briefly describe the sequence of events that are required for a SET transaction. **8**

   (b) Explain the operational description of PGP in detail. **8**

OR

5. Write short notes on : **16**

   (a) S/MIME.

   (b) AH & ESP in transport mode.