8E5002

Roll No. : ______________________ Total Printed Pages : 3

8E5002

B. Tech. (Sem. VIII) (Main) Examination, April/May -2012
Computer Science
8CS2 Information System & Securities (Common for CS & IT)
(Common with 8CS2, 8IT2)

Time : 3 Hours] [Total Marks : 80
[Min. Passing Marks : 24

*Attempt any **five** questions. Selecting **one questions** form **each unit**. All question carry equal marks. Schematic diagrams must be shown wherever necessary. Any data you feel missing suitably be assumed and stated clerly.*

Unit of quantities used/calculated must be stated clearly.

Use of following supporting material is permitted during examination.
(Mentioned in form No. 205)

1. ________ Nil ________ 2. ________ Nil ________

UNIT - I

1. (a) State and prove Euler's Theorem. 6

(b) Discuss Chinese remainder theorem in detail. 10

OR

1. Write short note on :

(i) Group

(ii) Field

(iii) Ring

(iv) Galois field

4×4=16

UNIT - II

2. (a) Differentiate following :

(i) Active attack and passive attack.

(ii) Diffusion and confusion.

8

(b) Describe the following transposition techniques with suitable example.

(i) Vernam Cipher

(ii) Simple columnarTransposition Technique.

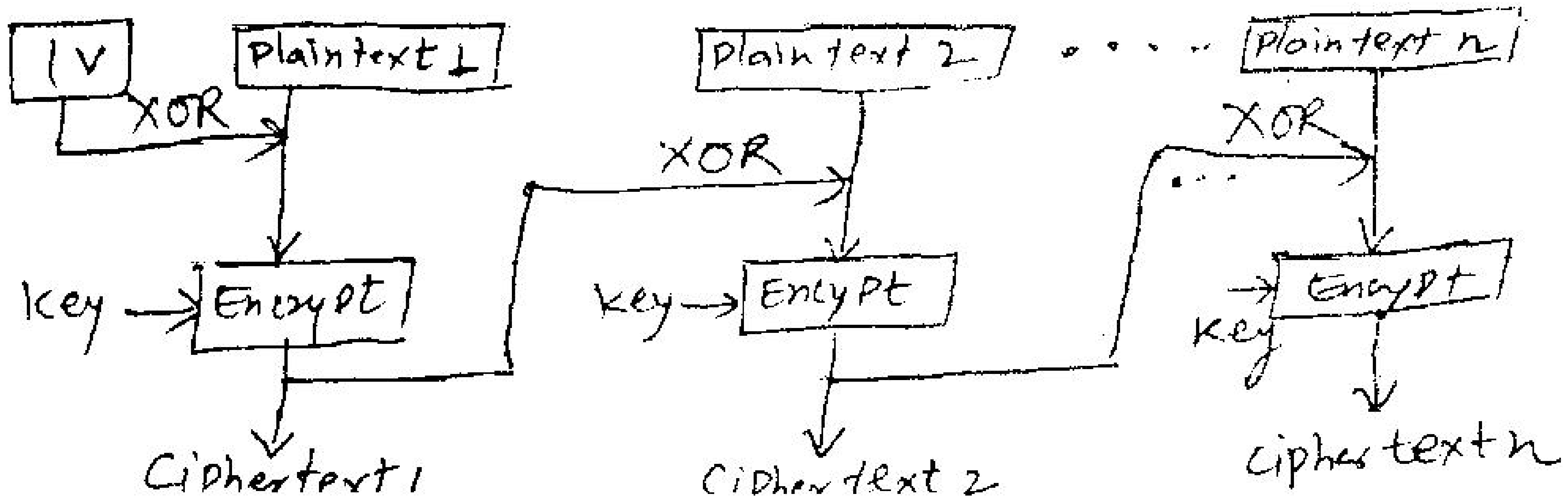
8

OR

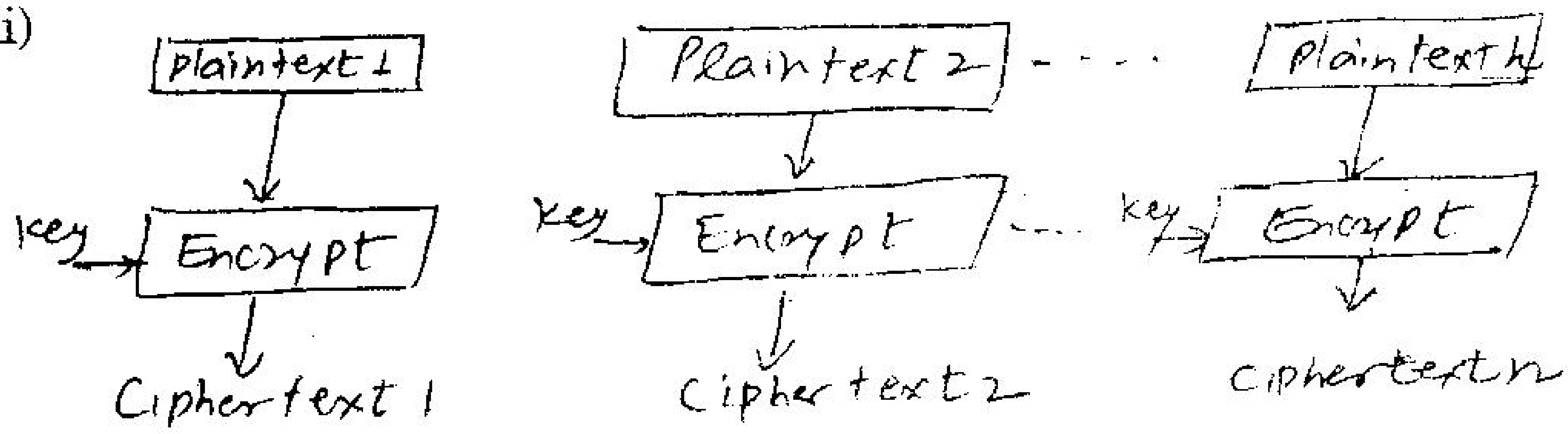
2 (a) Draw the decryption process of following.

6

(i)



(ii)



(b) Explain International Data encryption Algorithm (IDEA) in detail and also discuss the use of key shifting technique in IDEA.

10

OR

2 (a) How many keys are required for secure communication among 1000 person if.

(i) Symmetric key encryption algorithm is used

(ii) Asymmetric keykey encryption algorithm is used.

6

(b) Describe the DES (Data Encryption Standard) algorithm in detail.

10

UNIT - III

3 (a) Describe the Diffie-Hellman key exchange algorithm in detail. Also discuss the "Man in the middle attack" problem associated with the algorithm.

16

OR

(a) Perform encryption and decryption using RSA algorithm.

P = 3 Q = 11 E (public key) = 7

M (plain text) = 5

8

(b) Describe the following scheme for distribution of public keys :

(i) Public key authority

(ii) Public key certificate.

8

UNIT - IV

4 (a) Describe the Digital signature. Show how signing and verification is done using DSS (Digital Signature standard).

12

(b) Give the difference between hash and message authentication code.

4

OR

4 (a) Explain MD5 Message digest algorithm withits logic and compression function.

10

(b) Write short note on :

(i) Two-way public key

(ii) One-way public key

6

. UNIT - V

5 (a) Describe how PGP provide confidentiality and authentication service for e-mail application.

8

(b) Write short note on :

(i) S/MIME

(ii) X.509 certificate

8

OR

5 Write short note on :

(a) Approaches for intrusion detection

(b) Authentication Header.

16