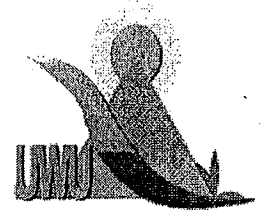


Uva Wellassa University, Sri Lanka
End Semester Examination – 2011 March
CST 342-2 Cryptographic Systems



Index No :

Time: Two (02) hours

Total 04 Questions.

Answer all questions.

Answer in the given space of each question.

01.

a) Name four characteristics of a good cipher.

(04 marks)

A large, empty rectangular box provided for the student to write their answer to question 1a.

b) Encrypt the following cipher text using Caesar cipher method.

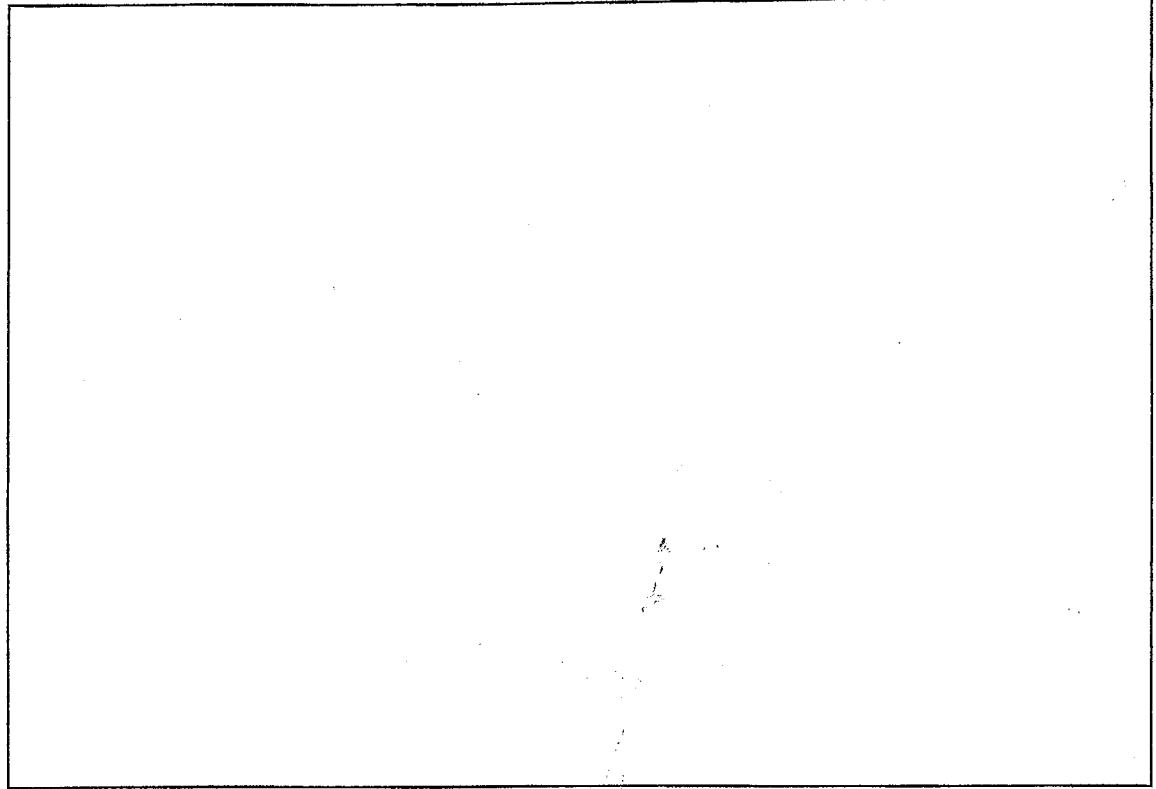
CRYPTOGRAPHIC SYSTEMS

(03 marks)

A large, empty rectangular box provided for the student to write their answer to question 1b.

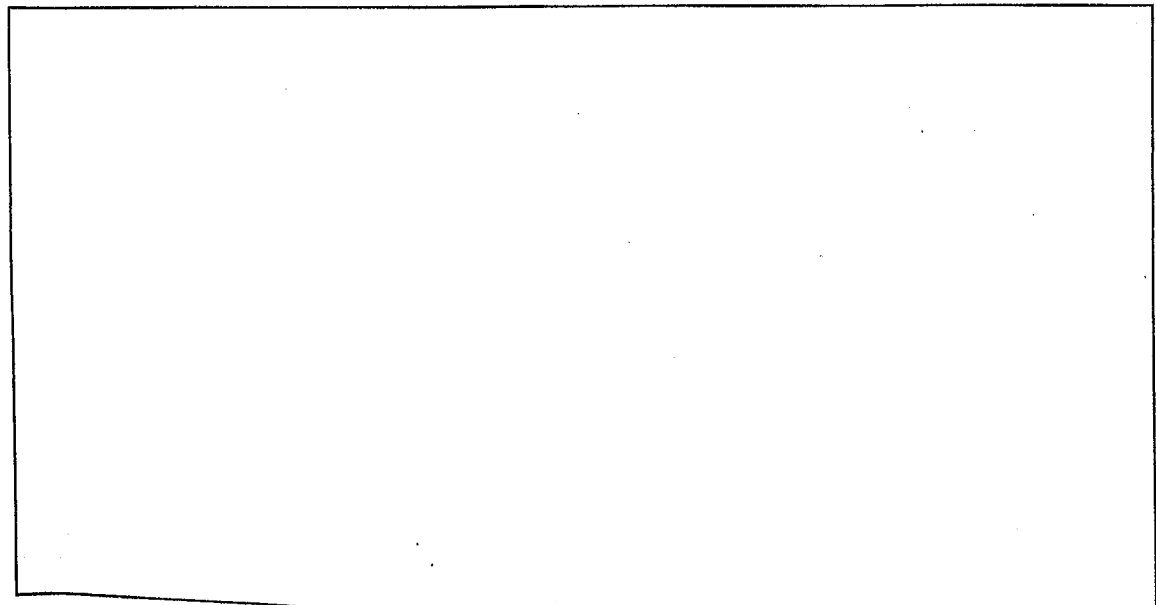
- c) Explain how Vernam cipher works by enciphering the following text using the random key: 82 44 3 58 11 60 5 48 88
PLAIN TEXT

(05 marks)



- d) What is the Kerchoff's principal? Explain the disadvantages upon an algorithm which has been designed without considering kerchoff's principal.

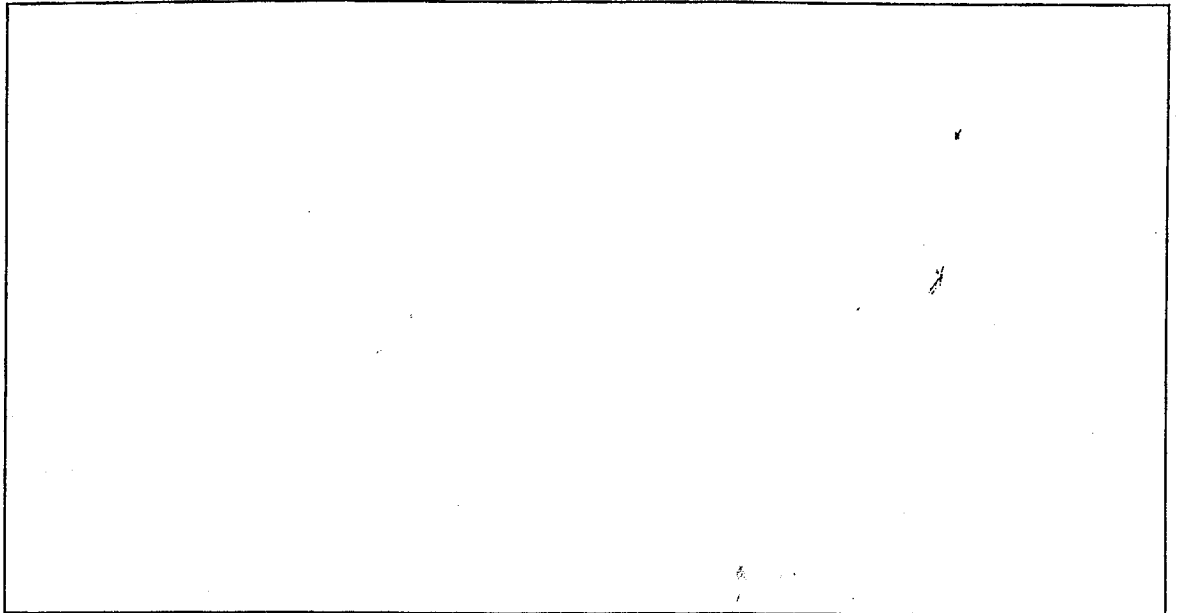
(04 marks)



he rand
05 mark

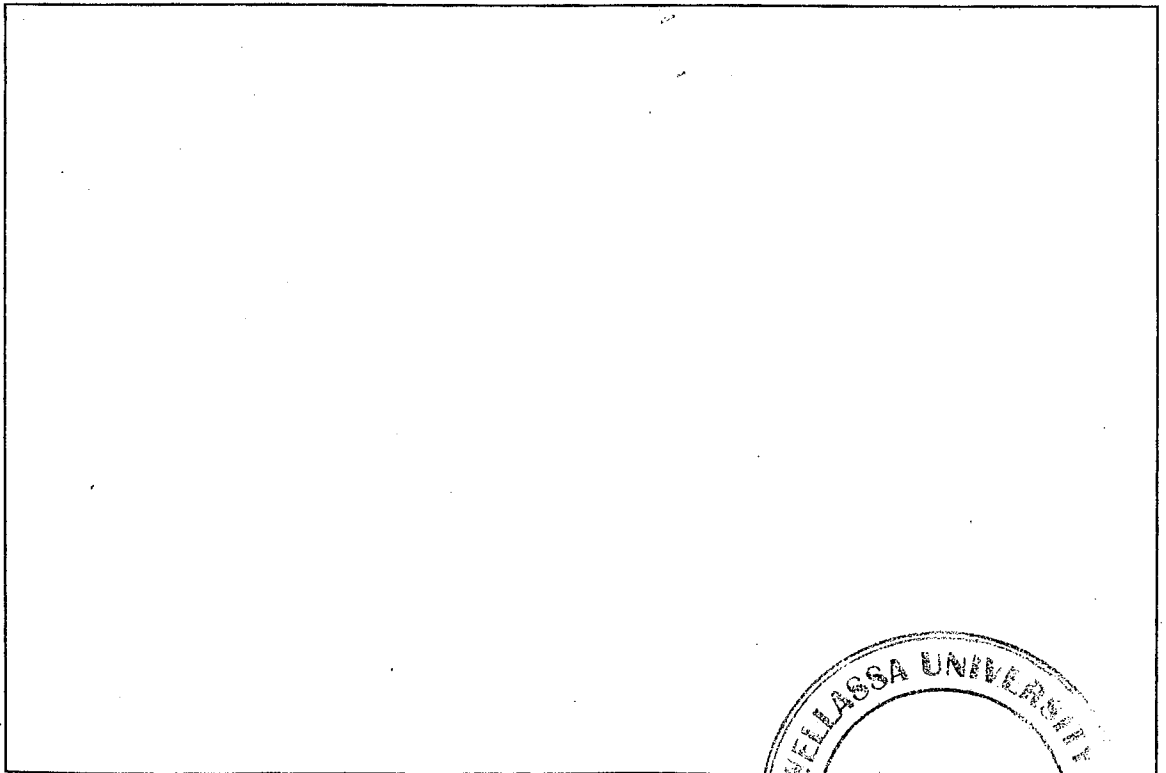
e) Name two hybrid cryptographic technologies and the reasons why they have been using as hybrid technologies without been used separately.

(04 marks)

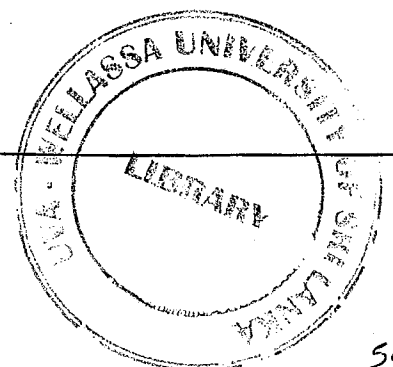


f) Write the steps for deriving a digital signature, which makes use of a one-way hash function such as SHA-1 and a public key cryptographic system such as RSA.

(05 marks)



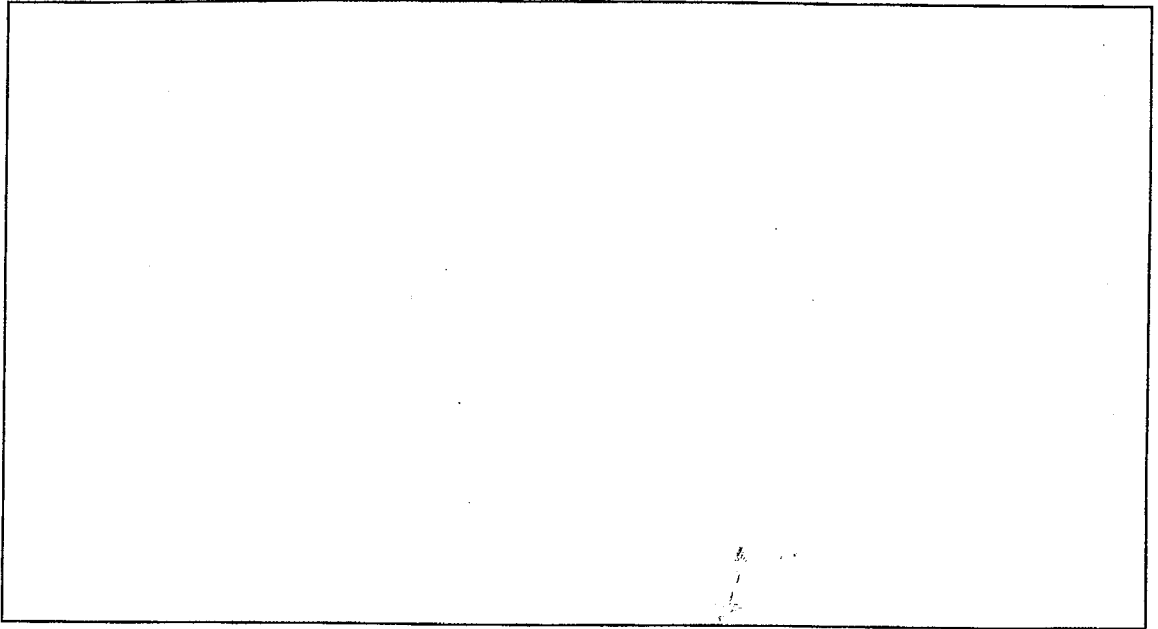
h has
arks)



02.

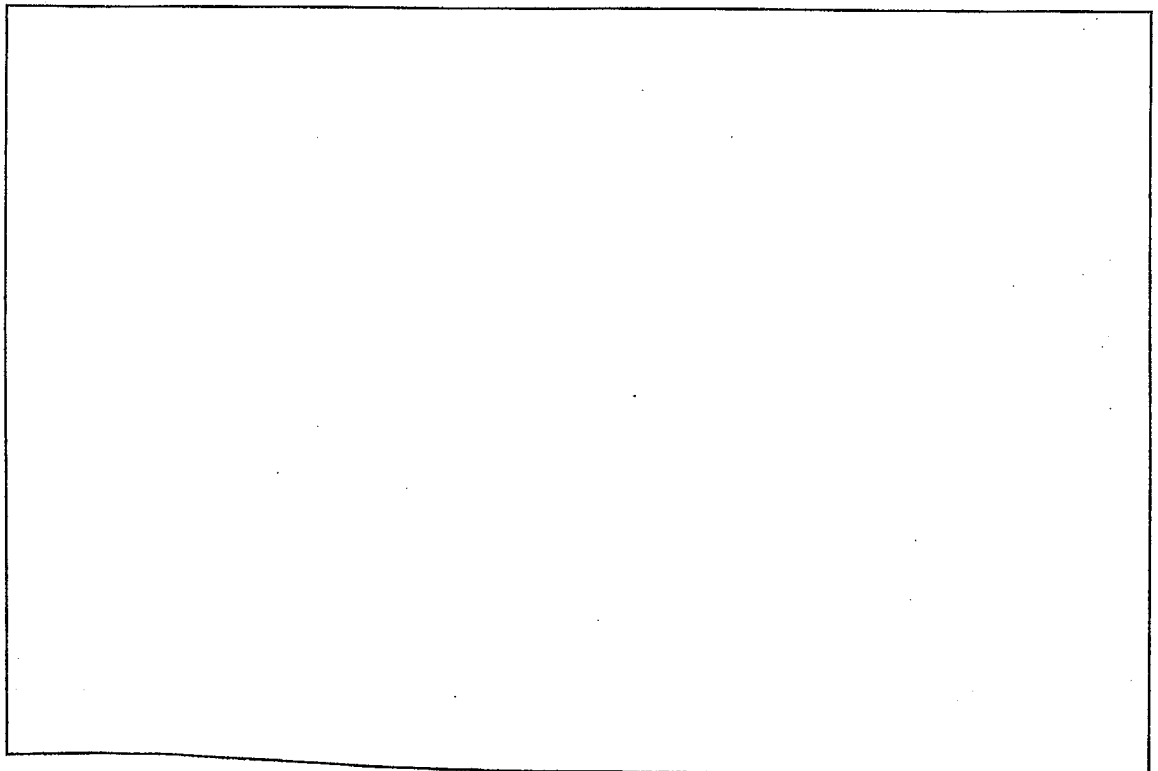
a) What is the greatest common divisor of 900 and 700?

(03 marks)



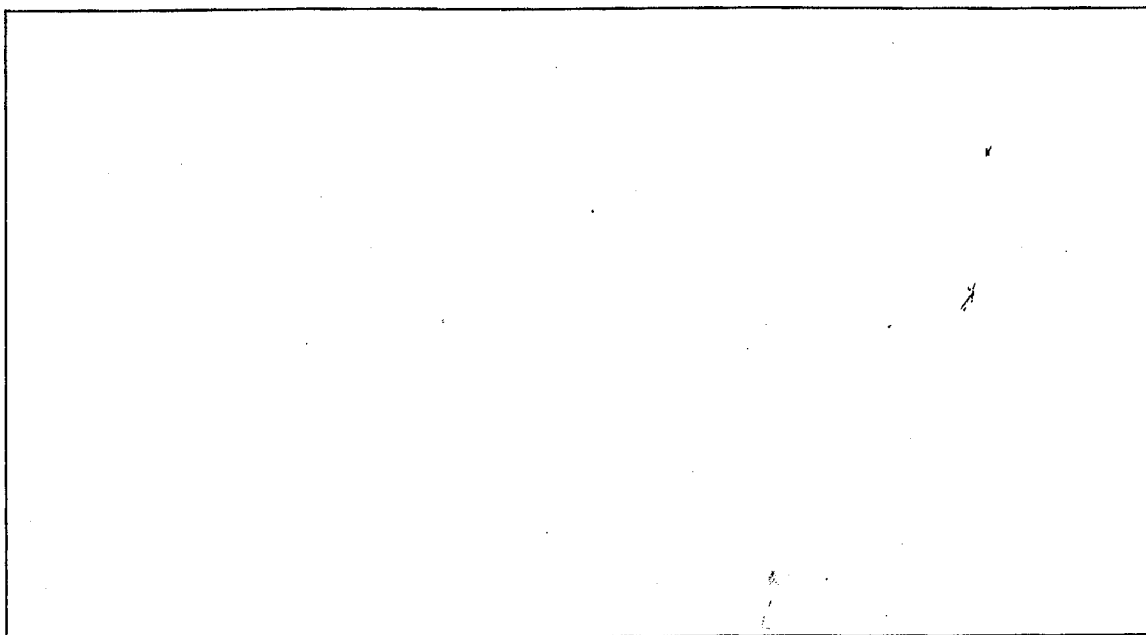
a) Suppose that RSA scheme is used for encryption and have chosen the integer values as $p=11$, $q=7$ and $e=5$ to encrypt a message $m=9$ in the public key system. What is the resulting cipher text?

(05 marks)



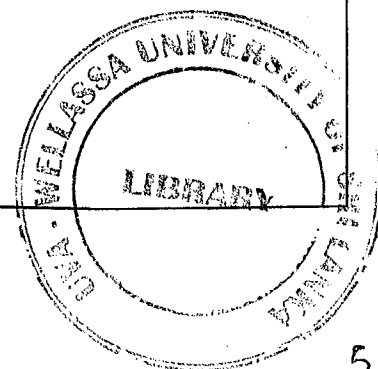
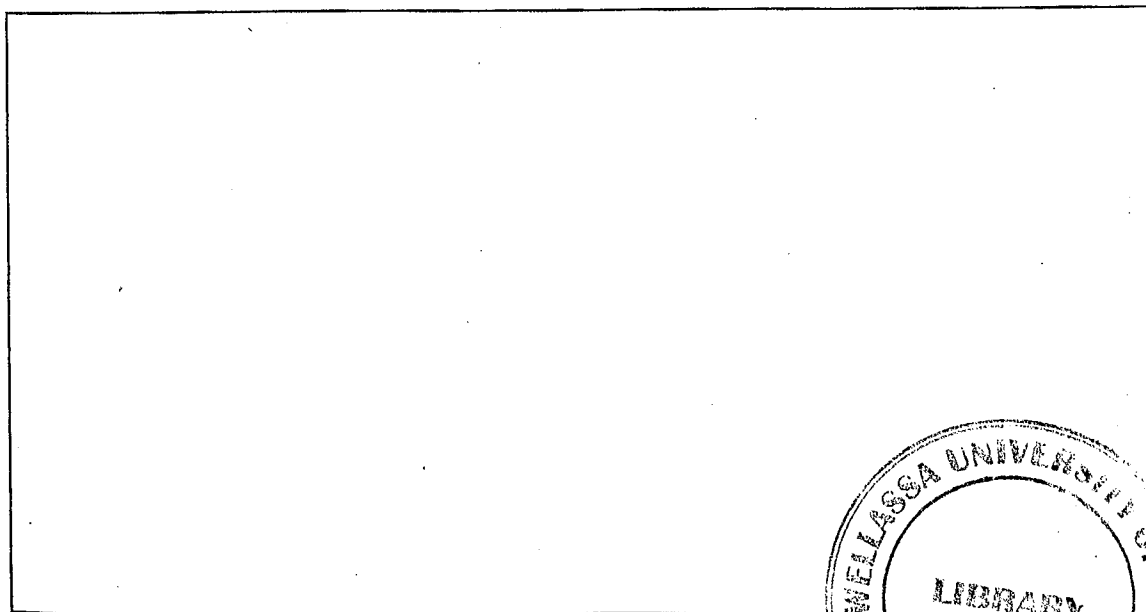
- b) Suppose the above system uses $d=5$ as the private key. What is the corresponding message m for the intercepted cipher text $c=10$?

(04 marks)

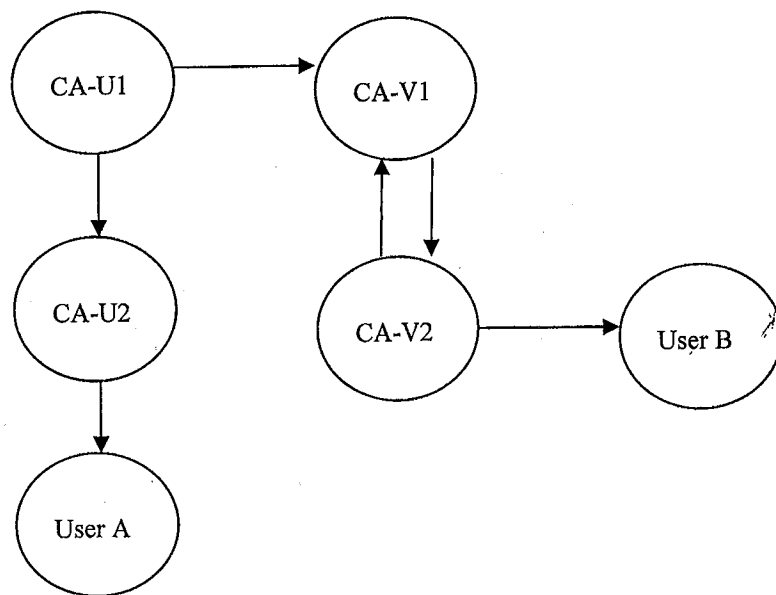


- c) Suppose we want to use the Diffie-Hellman Key Agreement protocol between two end points A and B, and have chosen the integer 2 as g and the integer 10 as p . A has got ' a ' and B has got ' b ' as the private keys respectively. For the private key ' a ' and session key X , we have the relation $X = g^a \pmod p$. If A generates the private key $a=4$ and B generates the private key $b=5$, what is the session key X between A and B?

(05 marks)



- d) User A receives the public key certificate of user B in the following cross-certified multiple PKI domains. What are the certificates which need to be verified by user A. Assume user A trusts only the certificate of CA-U1.



(03 marks)

- e) What are the attacks on packet filters?

(03 marks)

- f) What are the two types of access controls in database management systems?

(02 marks)

multiple
user

03.

a) What are the two types of IPSec communication modes?

(02 marks)

b) What are the advantages of eMoney order?

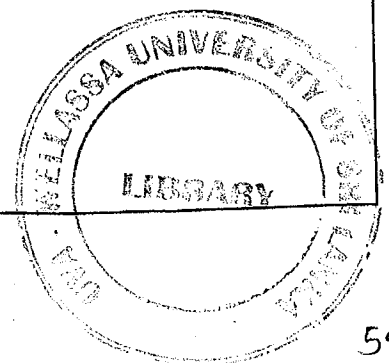
(03 marks)

c) List four certificate types used in cryptographic systems.

(04 marks)

d) Compare and contrast the security mechanism behind a normal password based authentication system vs security mechanism behind an ATM system.

(04 marks)

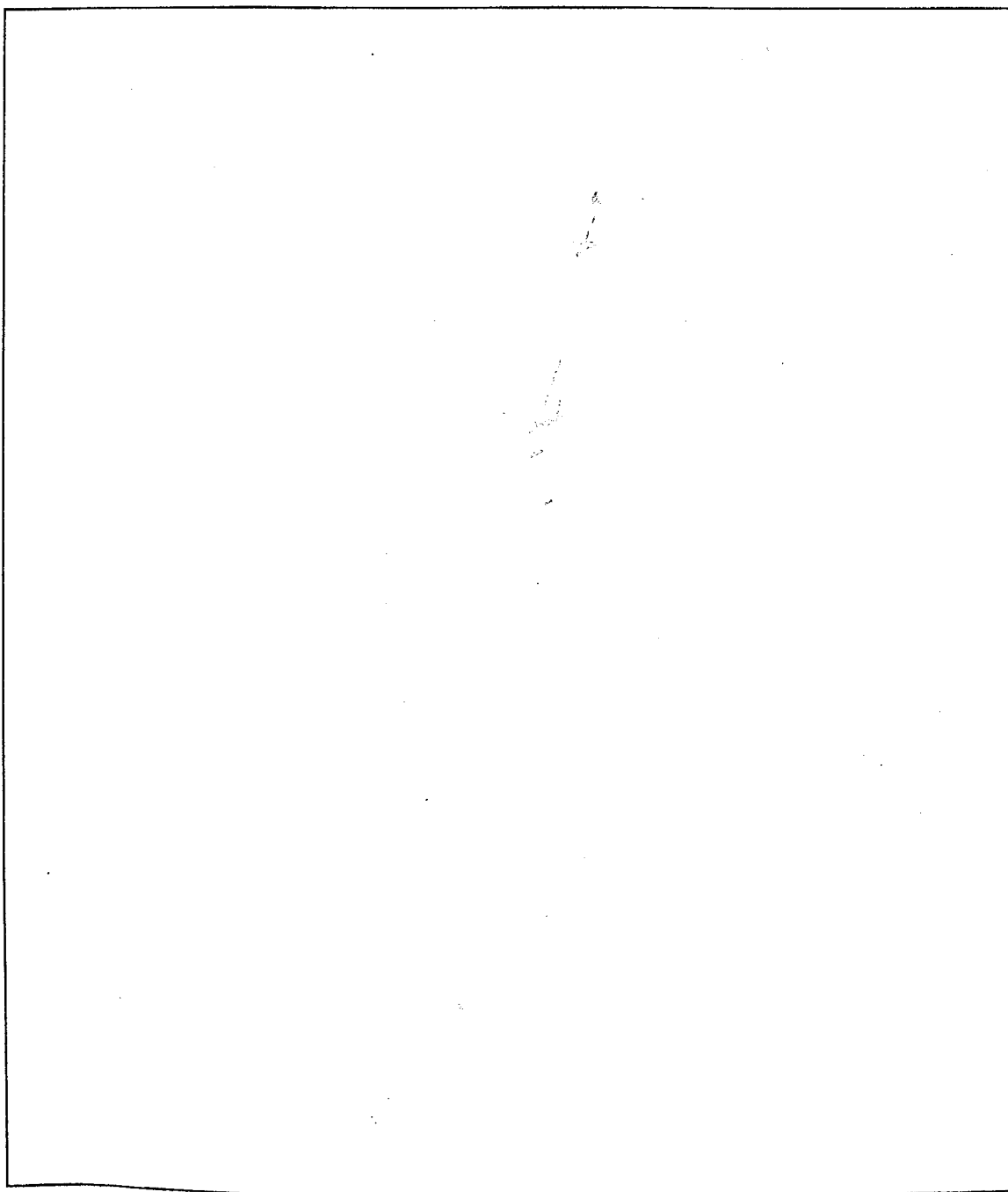


e) Following is an electronic voting protocol:

Every voter has his or her own private key and Commissioner of Elections (CE) owns public key. Firstly, each voter signs his vote with the private key. Then encrypts the vote with the public key of the CE and sends it to the CE. When all the votes are received, CE decrypts them, validates the signatures, tabulates the votes and announces the results.

1. Discuss the good side and the bad side of the above protocol?
2. Discuss how you are planning to overcome the weaknesses of the protocol.

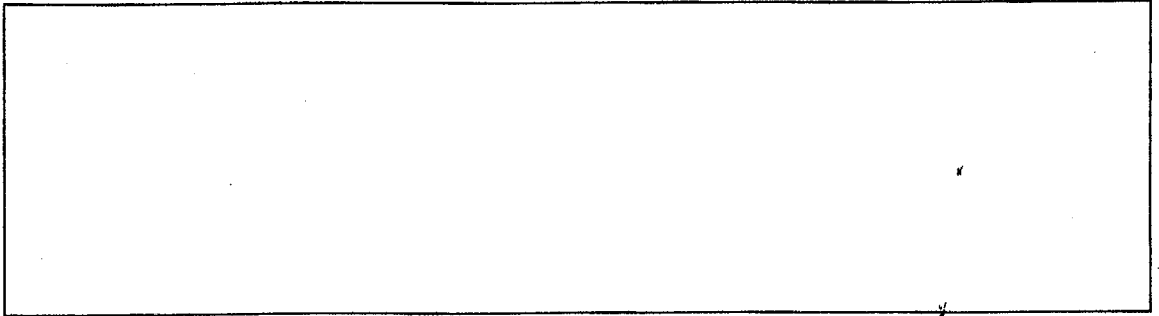
(12 marks)



04.

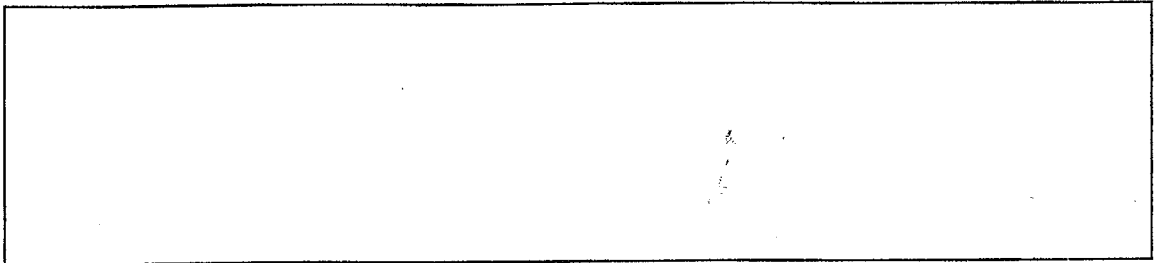
a) List four existing solutions for document protection in Web.

(04 marks)



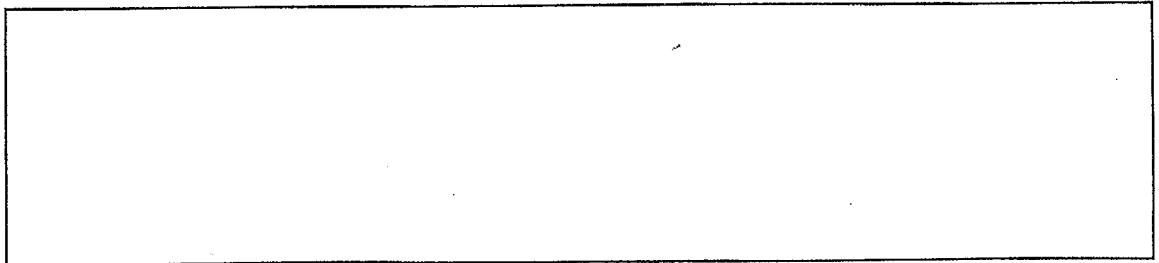
b) Name four intruder information gathering systems.

(04 marks)



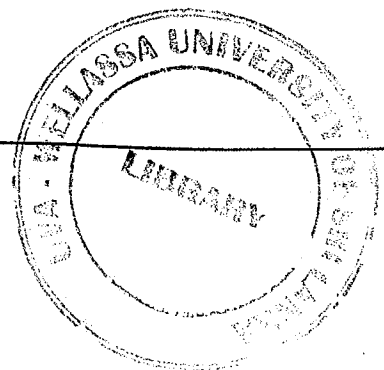
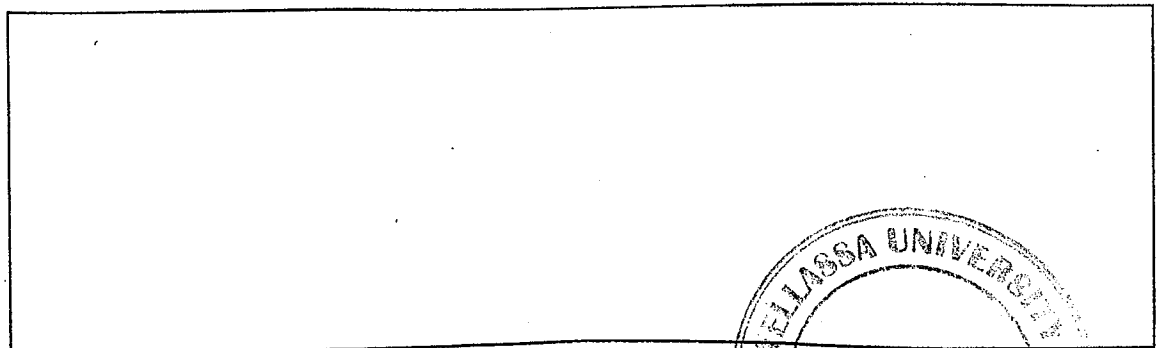
c) Name four anti-spamming techniques.

(04 marks)



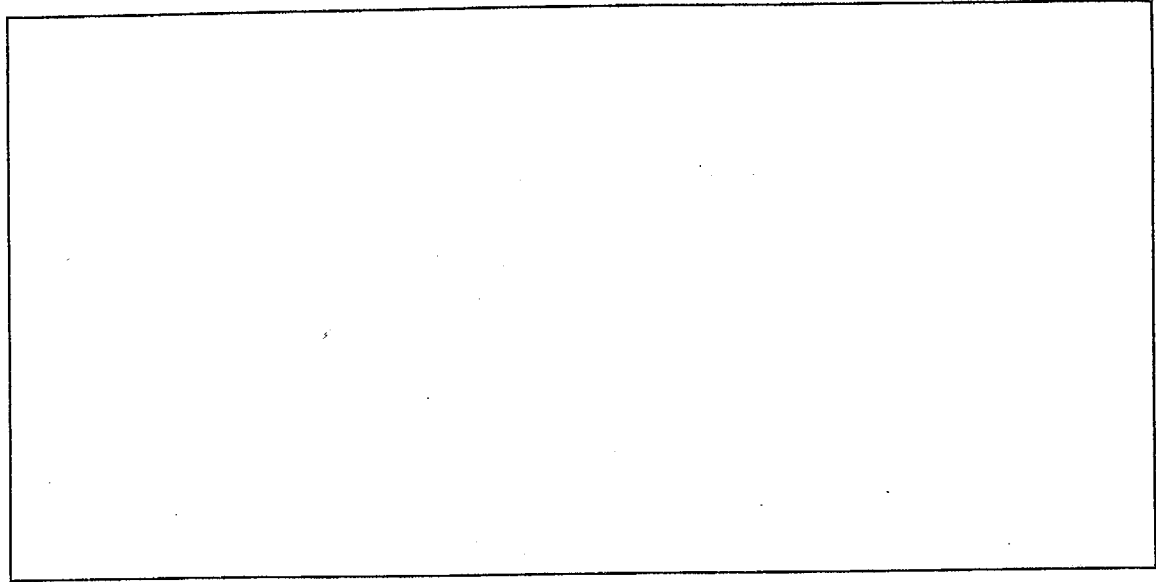
d) Name three types of firewall?

(03 marks)



e) Describe the limitations of a firewall.

(04 marks)



f) List three advantages and three disadvantages of Secure Electronic Transactions.

(06 marks)

