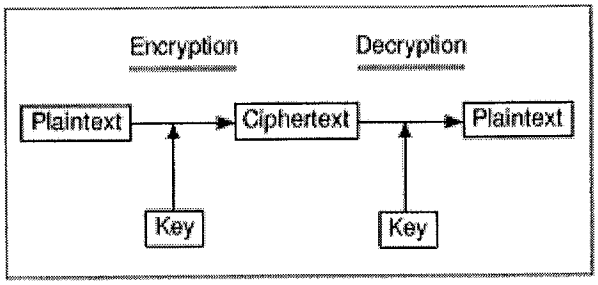
Uva Wellassa University of Sri Lanka
Faculty of Science and Technology
Department of Computer Science and Technology
300 level 2nd Semester Examination – Dec. 2018 / Jan. 2019
CST342-2 Cryptographic Systems

Uva Wellassa University

Instructions to candidates
Duration: Two (02) hours
Number of questions: Four (04)
Mark allocation: 100 mark
Answer all questions.

1.

a. Define the terms Cryptography and Cryptanalysis. (4 mark)
b. Briefly explain how encryption supports a secured communication. (3 mark)
c. Briefly explain the importance of digital signature in message authentication. (3 mark)
d. Describe encryption and decryption process with the aid of the picture below. (6 mark)



e.

i. Encrypt the message "defend the east wall of the castle" using Caesar cipher with 4 as the key. (4 mark)
ii. The message "gzzgiq gz jgct" was encrypted using the Caesar cipher with 6 as the key. Decrypt the message. (4 mark)

2.

a. List down the three (03) dimensions considered for the classification of cryptographic systems. (4 mark)
b. What is the key difference between Symmetric and Asymmetric key cryptography? (4 mark)
c. Briefly describe the Asymmetric key cryptography with the aid of graphical explanation. (6 mark)
d. Briefly describe the operations of Key Distribution Center (KDC). (5 mark)
e. Briefly explain the key elements of Public Key Infrastructure (PKI). (6 mark)

51

3.

a.

i. What is Rivest-Shamir-Adleman (RSA) algorithm and why it is considered as the widely used asymmetric algorithm? (4 mark)

ii. Encrypt and decrypt M = 4 with RSA algorithm while clearly stating the intermediate steps. Assume that p = 3 and q = 11. (12 mark)

b. Briefly explain how RSA differs from Digital Signature Algorithm (DSA). (5 mark)

c. Discuss the security issues of Data Encryption Standard (DES) and how Triple DES (3DES) overcomes the issues. (6 mark)

4. Write short note on any four (04) topics given below. (24 mark)

a. Alberti-Vigenere Cipher

b. Security of RSA

c. Brute-force attack

d. DES modes of operation

e. Four (04) stages of AES encryption