



Uva Wellassa University of Sri Lanka
Faculty of Science and Technology
Computer Science and Technology Degree Program
3rd Year 2nd Semester Examination – August/September 2014



CST 342-2 Cryptographic Systems

Number of questions: Four (04)
Answer all questions
Time allocation: Two (02) hours
Total mark: 100

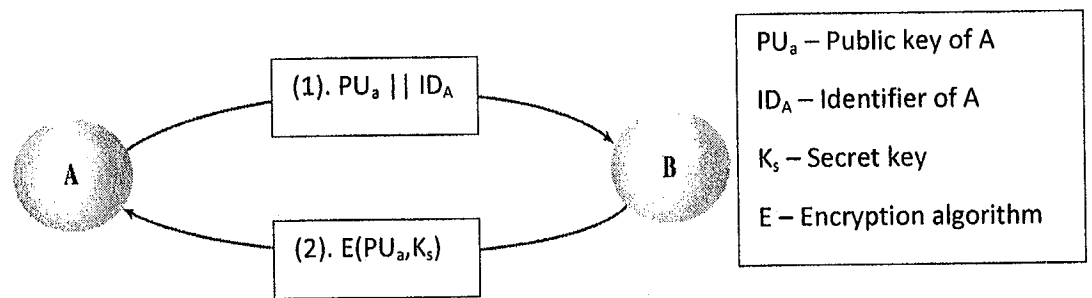
1.
 - a. Describe five components of symmetric encryption using a simplified model. (8 mark)
 - b. Explain Cryptanalysis and Brute-force attack. (4 mark)
 - c. Encrypt the message “must see you over cadogan west. Coming at once” using the following Playfair matrix. List all necessary steps. (8 mark)

M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

- d. Explain One-Time pad with appropriate advantages and disadvantages. (5 mark)
2.
 - a. Explain a single round of Data Encryption Standard using a simple diagram. (8 mark)
 - b. Explain the avalanche effect. (4 mark)
 - c. Describe Advanced Encryption Standard process using a diagram. (8 mark)
 - d. Compare conventional and public-key encryption. (5 mark)

- 3.
- Describe three main categories of public-key cryptosystems. (6 mark)
 - What is message authentication? (5 mark)
 - Explain message authentication process using a diagram. (6 mark)
 - Explain digital signature process. (5 mark)
 - List three applications of hash functions. (3 mark)

- 4.
- Explain the methods of key distribution. (4 mark)
 - Following diagram shows a simple secret key distribution by asymmetric encryption. It could be attacked by Man-in-the-middle attack. How do you implement Man-in-the-middle attack to the following method? (8 mark)



- Write necessary steps of mutual authentication using a trusted key distribution center. Use the following notations to write your steps. (Hint: Needham and Schroeder protocol) (8 mark)

A – Client A (Initiator)
 KDC – Key Distribution Center
 B – Client B
 K_a, K_b – Secret keys shared between A and KDC and B and the KDC respectively
 K_s – Session key
 ID_A, ID_B – Identity of A and B respectively
 N_1, N_2 – nonce N_1 and nonce N_2

- Briefly describe an overview of Kerberos using a diagram. (5 mark)