



Uva Wellassa University of Sri Lanka
Faculty of Science and Technology
Department of Computer Science and Technology
300 level 2nd Semester Examination – Dec.-2017/Jan.-2018
CST342-2 Cryptographic Systems



Part B

Number of questions: Three(03)

Mark allocation: 75

1.
 - a. Compare and contrast symmetric and asymmetric ciphers with appropriate examples. (10 mark)
 - b. Explain transposition technique which is used in cryptographic systems using an example. (10 mark)
 - c. Mention the importance of Message Authentication Code (MAC). (5 mark)

2.
 - a. List five (05) major categories of security services and explain. (10 mark)
 - b. Explain brute force attack with a real time example. (10 mark)
 - c. Mention the use of digital signature in the modern era. (5 mark)

- 3.
- a. Encrypt the message "must see you at library" using playfair matrix. Key is "university". (10 mark)
 - b. Decode the message "ltytufwnx" using Caesar cipher with shift+5. (8 mark)
 - c. Describe the working process of RSA algorithm. (7 mark)

