Uva Wellassa University of Sri Lanka
Faculty of Science and Technology
Department of Computer Science and Technology
300 level 2nd Semester Examination – Jan. / Feb. 2016
CST 342-2 Cryptographic Systems

Uva Wellassa University

Instructions to candidates:
Duration: 02 hours
Number of questions: Four (04)
Answer all questions
Mark allocation: 100
Calculators are **allowed**.

1.

a. What are the **three (03)** major aspects concerned regarding the classification of Cryptographic Systems?
(3 mark)

b. Distinguish **Block** and **Stream** cipher.
(4 mark)

c.

i. What are the key advantages of **Digital Certificates**?
(3 mark)

ii. Discuss how the objective of producing **Digital Certificates** can be achieved with public key cryptography.
(5 mark)

iii. Explain how **one-to-one** secure communication is established with **asymetric key** cryptography.
(5 mark)

d. What is meant by a **Public Key Infrastructure (PKI)**?
(5 mark)

2.

a.

i. Decrypt the following ciphertext with **Caesar Cipher** (shift key = 4). Where k is the key (the shift) applied to each letter. The decryption function is specified as:
$e(x) = (x - k) \ (mod\ 26)$
Ciphertext: **yaygwx**
(5 mark)

ii. Discuss how the security of the Caesar Cipher can be further enhanced using appropriate examples.
(5 mark)

b. Encrypt the following plaintext with **Rail-fence Cipher** (Key=3)
Plaintext: **wearedeptofcstatuwu**
(5 mark)

c. Using an example comprised of a **three (3)** character key, explain the **Vigenere Cipher** encryption process.
(10 mark)

B1

3.

a.

i. Compare and contrast **RSA (Rivest, Shamir, and Adleman)** and **DSA (Digital Signature Algorithm)** crypto-algorithms focusing on the key generation strategy. (5 mark)

ii. Critially analyze the strength of RSA crypto-algorithm in perspective of cryptanalysis. (5 mark)

b.

i. Briefly explain the technique used in **Data Encryption Standard (DES)** encryption algorithm to expand 32 bit input data block (half-block of 64 bit) in to 48 bit output block in order to encode with a 48 bit key. (5 mark)

ii. Encode the bit string **0101 1101** with the key **1010 1010**.
(Hint: Use XOR Addition) (2 mark)

c. i. Why **Advanced Encryption Standard (AES)** is concered better than the **Triple DES (3DES)**? (4 mark)

ii. What are the **four (4)** operations repeatedly undergone for the each byte of the state (an array of 4×4 bytes) in each round (except the final iteration) in **AES encryption**? (4 mark)

4.

a.

i. What are the properites of a good **cryptographic hash function**? (4 mark)

ii. Briefly discuss the evolution of **SHA (Secure Hash Algorithm)** cryptographic hash functions. (2 mark)

iii. Explain the concept of **Salted Password** using the applicability of a **hash function**. (5 mark)

b.

i. List the **five (05)** criteria of a good cipher proposed by **Claude Shannon**. (5 mark)

ii. What is meant by **Kerberos**? (2 mark)

iii. What are the **three(3)** major forms of **Session hijacking**? (3 mark)

iv. What is a **Logic Bomb**? (1 mark)

v. Briefly discuss the concept of **Digital Immune Systems** in context of "Future of fighting against Viruses". (3 mark)