Uva Wellassa University of Sri Lanka
Faculty of Science and Technology
Department of Computer Science and Technology
300 level 2nd Semester Examination – Sept. / Oct. 2015
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. Explain the term **Cryptanalysis.** (3 mark)

b. What is a **block cipher**? (2 mark)

c.

i. Compare and contrast **symmetric key cryptography** vs. **asymmetric key cryptography**. (5 mark)

ii. Discuss the role of **Digital Certificates** in public key discovery. (5 mark)

iii. Secure Key distribution is one of the major challenges in cryptography. What are the typical techniques used to achieve the objective? (5 mark)

d. Organizations operate in financial, logistic and defence domains are the victims of **SQL injection** malicious attack in most cases.
i. What is a SQL injection? (3 mark)
ii. Why those mentioned application domains are critical? (2 mark)

2.

a.

i. Decript the following ciphertext with **Caesar Cipher** (Shift key = 7). Where k is the key (the shift) applied to each letter. The decryption function is :
$e(x) = (x - k) \ (mod\ 26)$
Ciphertext: **dlsshzzh** (5 mark)

ii. Propose 3 possible modifications those can be introduced to enhance the security of the Caesar Cipher. (5 mark)

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

c. i. Linear congruential generator is a very simple example of a random number generator. All linear congruential generators use the following formula:
$r_{n+1} = a \cdot r_n + c \ mod\ (m)$

61

What is the major drawback of the **Linear Congruential Generator (LCG)**? Justufy your anwser with an appropriate example.
(Hint: Chooses the values of a, c and m with care, then the generator produces a uniform distribution of integers from 0 to m – 1.)

(3 mark)

ii. Using an appropriate example, explain the **Blum-Blum-Shub (BBS)** random number generation and cryptosystem. The BBS equation is as follows.
$X_{i+1} = X_i^2 \ mod \ n$
(Hint: The receiving party makes his BBS key as follows:
The recipient chooses two distinct Blum primes p and q (Assume p mod 4 = 3.) and computes their product, $n = pq$. The number n will be his public key,
while its factorization is his private key.)

(8 mark)

3.

a.

i. Differentiate **RSA(Rivest, Shamir, and Adleman)** crypto-algorithm with **DSA(Digital Signature Algorithm)** crypto-algorithm based on encryption / decryption key generation strategies.

(5 mark)

ii. List the key steps followed in order to generate public and private keys in RSA crypto-algorithm.

(5 mark)

iii. Encrypt and decript M=2 with RSA algorithm while clearly stating the intermediate steps.
Use the values specified below:
n=33, e=7, d=3.

(5 mark)

b.

i. Consider the following statement:
"The **Data Encryption Standard (DES)** is an outdated symmetric-key method of data encryption."
Do you agree with the above statement? Justify your answer.

(5 mark)

ii. Why **Advanced Encryption Standard (AES)** is secure than **Data Encryption Standard (DES)**?

(5 mark)

4.

a.

i. What is a **hash function**?

(2 mark)

ii. A cryptographic hash function must be able to withstand all known types of cryptanalytic attack. Discuss 3 properties of a good cryptographic hash function.

(5 mark)

b.

i. What meant by **Spyware**?

(2 mark)

ii. Distinguish a **firewall** and an **antivirus software**. (5 mark)

iii. List the essential features of a good antivirus software. (4 mark)

iv. What are the essential security aspects related to handling payment gateways and e-commerce web sites? (5 mark)

v. What is a **Dictionary attack**? (2 mark)

51