UNIVERSITY OF SRI JAYEWARDENEPURA

B.Sc. (General) Degree

Third Year First Semester Terminal Course Unit Examination – June 2019

CSC 378 1.5 Computer Security

Duration: One and half (1 ½) hours

Answer all questions.

Question 1 (30 marks)

(a) Compare and contrast symmetric and asymmetric cryptograph. **[5 Marks]**

(b) Consider the cipher defined by the following equation where *n* is the length of the key and *z* is the length of the alphabet and the other symbols have their usual meanings.

$$E_K(P) = C \text{ where:}$$

$$C_i = (P_i + K_i \bmod n) \bmod z$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

If the alphabet is English, z = 26, K = "DCS", and P = "USJP", find C. **[4 Marks]**

(c) Kerckhoffs says "A cryptosystem should be secure even if everything about the system, except the key, is public knowledge". How can it be secure when the algorithm is a public knowledge? **[5 Marks]**

(d) Briefly explain the four major types of security attacks and what security feature(s) lose in each type.

Malware
Phishing
SQL Injection Attack
Cross-Site Scripting (XSS)
Denial of Service (DoS)
Session Hijacking and Man-in-the-Middle Attacks
Credential Reus

[8 Marks]

(e) When we are defining security policies for an organization, there are different levels of actions and categories. Briefly explain those three levels of actions and for types of categories in computer security risk management.

[8 Marks]

Question 2 (35 marks)

(a) Assume the head of an institute wants to distribute an important notice to everyone in the institute electronically. Though the normal email system can be used to distribute the message, they want to use a security mechanism to assure the originality of the message and the sender of the message. By clearly mentioning all the important points, explain a solution for this scenario.

[12 Marks]

(a) Name four malicious codes and explain each in brief.

[8 Marks]

(b) What is a digital certificate? Why do we need it?

[6 Marks]

(c) Name three attacks a normal web site is exposed to and suggest countermeasures for each.

[9 Marks]

Question 3 **(35 marks)**

(a) Answer the following questions regarding crypto currencies.

i. What is a crypto currency?

ii. What are the motivations behind it?

iii. What are the barriers for the development of crypto currencies?

[15 Marks]

(b) What is a block chain? Explain its usage.

Blockchain is a digital ledger that stores transaction details.
these records are stored in containers called blocks,
these blocks are linked to each other and are secured using cryptography

[8 Marks]

(c) What is a smart contract? Explain the ways it can be used to serve people.

[8 Marks]

(b) Write four security tips for a person who is using online services.

[4 Marks]

* * * * END OF PAPER * * * *