UNIVERSITY OF RUHUNA

Faculty of Engineering

End-Semester 8 Examination in Engineering: November 2016

Module Number: EE8204 **Module Name: Information Security**

[Answer all the questions, each question carries 10 marks]

PART- B

Q1. a) i) Security in mobile communication technologies such as 2G, 3G and 4G Long Term Evolution (LTE) is a critical factor. Relate information security concepts to mobile communication.

ii) Explain the term plausible deniability and the method to overcome this issue.

iii) What is meant by avalanche affect in cryptography?

[4 Marks]

b) Consider the following cryptographic scheme which employs three phases for encrypting a plaintext. The encoding scheme used is given in Table Q1 b) - I.

Table Q1 b) - I

Letter	A	C	E	F	G	I	N	S
Code	000	001	010	011	100	101	110	111

1st phase :

Double transposition with a 3×4 matrix. Key : [3,1,2] [4,2,1,3]

2nd phase :

One Time Pad (OTP) process with the key "SA SA SA SA SA SA".

3rd phase:

If the three bits representing a letter can be symbolized as $b = b_L b_M b_R$.

For every 3 bits or letter, output of this phase is given by $b = \begin{cases} b_L \bar{b}_M b_R, & b_L = b_R \\ b_L b_M b_R, & b_L \neq b_R \end{cases}$ and the changes are done according to Table Q1 b) - II.

Table Q1 b) - II

b	$\bar{b}$
0	1
1	0

If the cipher text is "SNICCSEGNFAS", determine the plaintext.

[6 Marks]

Q2. a) i) Explain how the Cipher Block Chaining (CBC) mode of symmetric key encryption schemes work and the way they recover from erroneous cipher blocks.

ii) Briefly explain an application of hash functions in information security perspective.

iii) "Elliptic Curve Cryptography (ECC) is a popular method used in cryptographic systems to enhance the performance". Explain.

[4 Marks]

b) Consider the points $P_0 \equiv (0, y_0), P_1 \equiv (1, y_1), P_2 \equiv (2, y_2)$ and $P_3 \equiv (3, y_3)$ which are lying on the elliptic curve $E: y^2 = x^3 + 15x + c \pmod{37}$.

Note:

Method of adding two points $P_1 \equiv (x_1, y_1)$ and $P_2 \equiv (x_2, y_2)$ on the Elliptic Curve $E: y^2 = x^3 + ax + c \pmod{p}$; $P_1 + P_2 = P_3 \equiv (x_3, y_3)$

where
$$x_3 = m^2 - x_1 - x_2 \pmod{p}$$
$$y_3 = m(x_1 - x_3) - y_1 \pmod{p}$$
$$m = (y_2 - y_1)(x_2 - x_1)^{-1} \pmod{p}, \text{ if } P_1 \neq P_2$$
$$m = (3x_1^2 + a)(2y_1)^{-1} \pmod{p}, \text{ if } P_1 = P_2.$$

i) If $y_3 = 9$, determine the values y_0, y_1 and y_2.

ii) Use the algorithm given above to compute the addition of points P_0 and P_2. [Hint : Only consider the positive values of y_0 and y_2]

iii) Entities A and B uses this elliptic curve along with point P_1 to implement a symmetric key based secure channel. What is the established symmetric key, if the secret values of A and B are 2 and 1 respectively?

[6 Marks]

Q3. a) i) Describe what is meant by dictionary attack and a method to avoid it.

ii) Explain the two phases in biometric based authentication systems.

[2 Marks]

b) Mention three access control policies and briefly explain one of them.

[2 Marks]

c) Consider the mutual authentication and key establishment protocol shown in Figure Q3. This protocol uses a timestamp T and public key cryptography. Show that Trudy can attack the protocol to discover the key K. We assume that the cryptography is secure. Modify the protocol to prevent such an attack by Trudy.

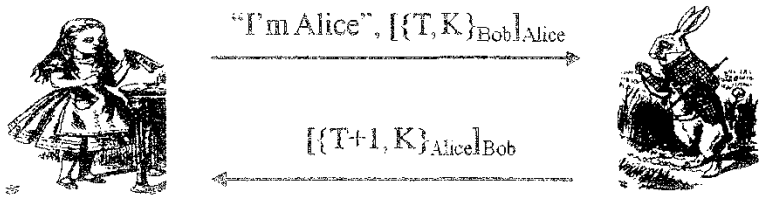

Figure Q3

[3 Marks]

d) Propose a simple and secure protocol to communicate between a web client and a web server with known cryptographic primitives such as public / symmetric key crypto, timestamps, hash....etc. Illustrate the proposed protocol using a message flow diagram.

[3 Marks]