UNIVERSITY OF RUHUNA

Faculty of Engineering

End-Semester 8 Examination in Engineering: November 2017

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

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

PART- B

Q1 a) i) E-commerce is an advancement in finance and marketing which allows its users to conduct transactions securely via Internet (online). Relate Confidentiality, Integrity and Availability (CIA) concepts to E-commerce.

ii) Explain the term authenticity and its importance regarding information access.

iii) Explain the 'depth issue' associated with One-Time-Pads (OTPs).

[5 Marks]

b) Consider the following cryptographic scheme which employs two phases for encrypting a plaintext.

1st phase

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

2nd phase

OTP cipher is used with the following encoding scheme. Key : acghoprtyacg

Letter	A	C	G	H	O	P	R	T	Y
Code	0000	0001	0010	0011	0100	0101	0110	0111	1000

If the encrypted code is '0000 0111 0000 1011 0111 0000 0010 0000 1101 1000 0111 0011', determine the plaintext by decrypting this cipher.

[5 Marks]

Q2 a) The round function of the Data Encryption Standard (DES) algorithm is given below.

$$F(R_{i-1},K_i) = P-box\left(S-boxes\left(Expand\left(R_{i-1} \oplus K_i\right)\right)\right)$$

i) Briefly explain the function of each stage of this process and mention their security features.

ii) Compare the operation of block cipher modes in block ciphers.

[3 Marks]

b) i) Describe the uses and vulnerabilities of 'Sign-and-Encrypt' and 'Encrypt-and Sign' approaches in asymmetric key encryption schemes.

ii) Explain the Diffie-Hellman (DH) Man-in-the-Middle (MiM) attack using appropriate diagrams and state a method to remedy this attack.

[2 Marks]

c) The term 'Homomorphic Encryption' is a form of encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result and when decrypted, matches the result of operations performed on the plaintext. For plaintext values x_1 and x_2, the homomorphism concept can be explicated as, $Decryption\left[Encryption\left(x_1\right) \otimes Encryption\left(x_2\right)\right] = x_1 \otimes x_2$. If an encryption algorithm adheres to above mentioned concept for every mathematical operation (addition, multiplication, division and etc.), such an algorithm is named as Fully Homomorphic Encryption (FHE) scheme. Although secure FHE systems are not yet developed, partially homomorphic features can be found on existing encryption schemes such as RSA, Paillier and ElGamal. Out of these, RSA encryption algorithm attributes for multiplicative homomorphism. The RSA encryption algorithm is given below.

- Two prime numbers are selected as p and q.
- $N = pq$
- $\phi\left(N\right) = \left(p-1\right)\left(q-1\right)$
- Select e such that, e is relatively prime with $\phi(N) \Rightarrow GCD\left[e, \phi(N)\right] = 1$.
- $d = e^{-1} \bmod \phi(N)$
- Encryption : $E = M^e \bmod N$ where M is the message to be encrypted
- Decryption : $M = E^d \bmod N$

where GCD stands for Greatest Common Divisor.

i) Verify the RSA encryption algorithm from the parameters given below. $p=7$, $q=11$ and $M_1=8$

ii) Prove the multiplicative homomorphic attribute of RSA algorithm by taking the second value to be encrypted as $M_2=6$.

iii) Comment on a flaw that might encounter in these encryption schemes with regard to cryptic parameters.

[5 Marks]

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

ii) Compare the key features in Secure Socket Layer (SSL), Internet Protocol Security (IPSec) and Kerberos security protocols.

[3 Marks]

b) Consider the mutual authentication and key establishment protocol shown in Figure Q3 b). This protocol uses a timestamp T and the 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.

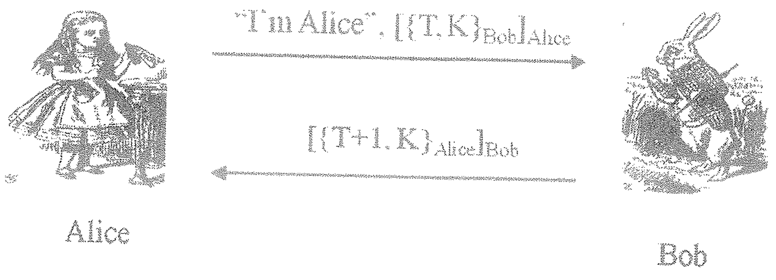
"I'm Alice", $[\{T, K\}_{Bob}]_{Alice}$
$[\{T+1, K\}_{Alice}]_{Bob}$
Alice
Bob

Figure Q3 b)

[2 Marks]

c) Vehicle to vehicle (V2V) communication concept comprises a wireless network where automobiles communicate each other for the purpose of reducing traffic congestions and avoiding accidents aided by extracted vehicular statistics such as speed, location, direction of travel, braking, and loss of stability. Moreover, each automobile could be connected to a monitoring server to form a vehicular network in which the vehicle condition and location is monitored by a concerned party. The Figure Q3 c) illustrates a vehicular network model in which the wireless communication ranges of vehicles C1 and C2 are indicated. In the V2V communication link between C1 and C2, the information being conveyed between the vehicular nodes should be secured and the anonymity of the car owner should be ensured. At the same time, each vehicular node is monitored by the monitoring server of their vehicular statistics in which anonymity is not a concern. But all the communication channels should be secured as the vehicles could be subjected to hacking, which results in unexpected devastating consequences. Propose a security protocol for the model given in Figure Q3 c). The model should have three secure communication channels as described below.

- V2V communication channel
- Channel for monitoring vehicular statistics
- Channel for compromising both V2V and monitoring network which requires when the range of a vehicular node fails to reach the nearest mobile node to connect with the monitoring server (as in C2)

[5 Marks]

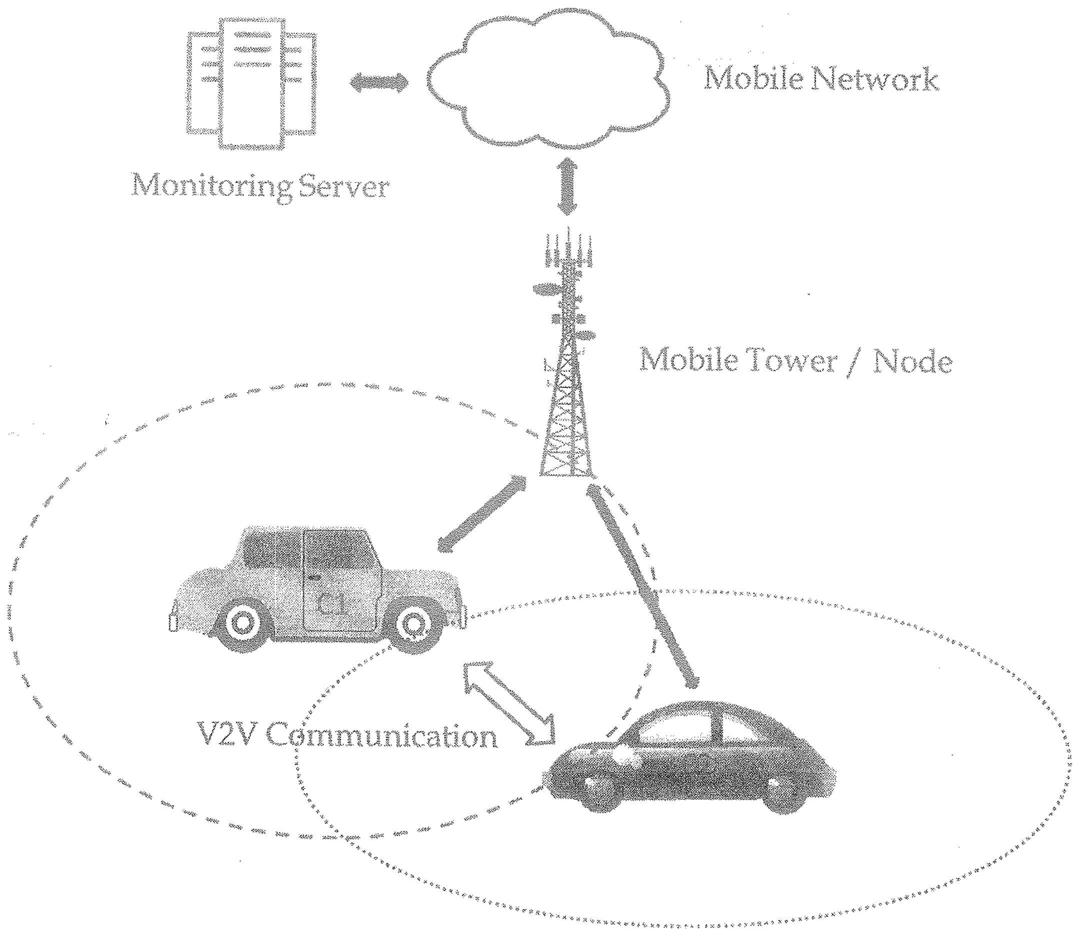
Monitoring Server
Mobile Network
Mobile Tower / Node
C1
V2V Communication

Figure Q3 c)