UNIVERSITY OF RUHUNA

Faculty of Engineering

End-Semester 8 Examination in Engineering: December 2015

Module Number: EE8257 **Module Name: Information Security**

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

PART- B

Q1. a) i) A Virtual Private Network (VPN) is a private network access method where the connection is extended across the internet. Explain how the VPNs ensure the information security concepts.

[2.5 Marks]

ii) State the Kerckhoffs's principle in cryptography.

[0.5 Marks]

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

1st phase :

Encoded with Caesar's cipher.

2nd phase :

'Double transposition' with a 3×6 matrix. Key : [2,1,3] [4,2,3,6,1,5]

If the encrypted text is 'UZBPKFLDKXFOFYIVUV', determine the plaintext by decrypting this cipher.

[5 Marks]

c) Mention the types of attacks that are feasible on information systems and state their significance.

[2 Marks]

Q2. a) i) Describe the uses and the vulnerabilities of 'Sign-and-Encrypt' and 'Encrypt-and Sign' approaches in asymmetric key encryption schemes.

[1 Mark]

ii) Explain the difference between ephemeral Diffie-Hellman (DH) and static DH encryption schemes.

[1 Mark]

b) The Data Encryption Standard (DES) algorithm round function is mentioned 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.

[1 Mark]

ii) Integrity violations in the Cipher Block Chaining (CBC) mode of symmetric key encryption schemes can be detected. Explain how CBC works and errors are detected.

[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 which, 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, $Decryption[Encryption(x_1) \otimes Encryption(x_2)] = x_1 \otimes x_2$. If an encryption algorithm is adhering to above mentioned concept for every mathematical operation (addition, multiplication, division,.....etc.), such an algorithm is named as Fully Homomorphic Encryption (FHE) scheme. Eventhough 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 attribute for Multiplicative homomorphism. The RSA encryption algorithm is given below.

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

i) Verify the RSA encryption algorithm from the parameters given below.
$p = 5,\ q = 7,\ M_1 = 5$

[3 Marks]

ii) Prove the multiplicative homomorphic attribute of RSA algorithm by taking the second value to be encrypted as $M_2 = 4$.

[2 Marks]

Q3. a) i) List the best practices followed to enhance the security in password based authentication systems.

[1 Mark]

ii) Would the methods mentioned in i) are capable of securing the system against dictionary attacks?

[1 Mark]

iii) State the requirements for an ideal biometric scheme.

[1 Mark]

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

[2 Marks]

c) Man in the Middle (MiM) attack in Secure Socket Layer (SSL) protocol is failing. Explicate the reason using proper illustrations.

[2 Marks]

d) Consider the diagram given in Figure Q3.1 of IPSec protocol Internet Key Exchange (IKE) Phase 1 Main Mode (MM) of one of the key options.

i) Identify the key option of this MM.

[0.5 Marks]

ii) What is the purpose of proof $_A$ and proof $_B$?

[0.5 Marks]

iii) Mention the significance of the Aggressive Mode (AM) of this key option compared to the other main modes.

[1 Mark]

iv) Plausible deniability is a weakness in this key option. Explain.

[1 Mark]

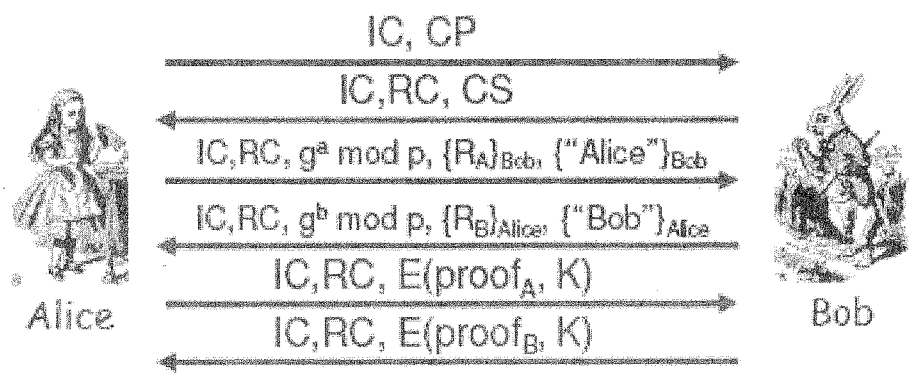

Figure Q3.1