UNIVERSITY OF RUHUNA

Faculty of Engineering

End-Semester 8 Examination in Engineering: July 2022

Module Number: EE8209 **Module Name: Information Security**

[Three Hours]

[Answer **all questions**, each question carries 10 marks.]

Q1 a) i) Explain the difference between information security and cyber security.

[1 Mark]

ii) State two (2) basic assumptions used in cryptography.

[1 Mark]

iii) Briefly explain confidentiality, integrity and availability (CIA triad) concepts.

[1.5 Marks]

b) i) Use Double Transposition Cipher to decrypt the following cipher text. The matrix size is 4x4 and the key is [1324], [2143].

"EBIGNUDTxNOCWOxN"

[2 Marks]

ii) Given the cipher text is "EPRSPATCO", the key is "RTCASCEOP", and the encryption algorithm is One Time Pad (OTP), find out the plaintext. Refer to Table Q1-f).

[2.5 Marks]

Table Q1-f)

Letter	A	C	E	O	P	R	S	T
Code	000	001	010	011	100	101	110	111

iii) What is the 'depth issue' associated with One Time Pad (OTP)?

[1 Mark]

iv) A good cipher system needs to achieve both confusion and diffusion. State which properties are achieved by Double Transposition Cipher and One Time Pad (OTP).

[1 Mark]

Q2 a) i) Explain how Stream Ciphers work and state two (2) commonly used Stream Ciphers.

[1 Mark]

ii) Explain the operations of expansion, permutation, substitution, and XOR.

[2 Marks]

b) Consider the following Feistel cipher design with three rounds and the plain text, $P = (L_0, R_0)$.

Encryption:

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

where F is the round function and K_i is the subkey for round i.

i) What is the ciphertext C, if the round function, $F(R_{i-1}, K_i) = R_{i-1}$?

[2 Marks]

ii) Comment on the security of the above encryption scheme.

[1 Mark]

c) In cryptography, encryption is modelled as C = E(P, K) and decryption is modelled as P = D(C, K), where C is the cipher text, P is the plaintext, K is the key, E denotes encryption, and D denotes decryption. Write the corresponding model equation for the encryption process in Triple DES, when two keys, K1 and K2, are used.

[1 Mark]

d) i) Explain two (2) drawbacks of Electronic Code Book (ECB) mode.

[1 Mark]

ii) Let's consider a security system where Cipher Block Chaining (CBC) mode is used. When the cipher text C_i is transmitted over a channel, if an error occurs resulting in C_i being changed to G, analyse using notations how the system recovers from such a transmission error.

Formula for encryption in CBC mode is $C_i = E(P_i \oplus C_{i-1}, K)$

Formula for decryption in CBC mode is $P_i = D(C_i, K) \oplus C_{i-1}$

[2 Marks]

Q3 a) i) What is the main difference between symmetric key cryptography and asymmetric key cryptography?

[0.5 Marks]

ii) Public key cryptography is based on a one-way trap door function. Explain with examples.

[1 Mark]

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

[1 Mark]

b) Following are the steps executed in the RSA encryption algorithm.

- Two prime numbers are selected as p and q
- $N = pq$
- Compute the totient function, $\emptyset(N) = (p-1)(q-1)$
- Select e such that, e is relatively prime with $\emptyset(N)$. i.e., $gcd[e, \emptyset(N)] = 1$
- $d = e^{-1} \ mod \ \emptyset(N)$
- Encryption: $C = M^e \ mod \ N$
- Decryption: $M = C^d \ mod \ N$

i) Identify the private key and public key from the given parameters.

[1 Mark]

ii) Find the cipher text, C for the following parameters.

$p = 5, q = 3, M = 7$

Hint: Select the lowest value for e, which is relatively prime with $\emptyset(N)$.

[3 Marks]

iii) If cipher text, C, is 8, find the corresponding plaintext for the same security parameters used in part (ii) above.

[1 Mark]

c) Why is it difficult for an intruder to figure out the shared secret key in Diffie-Hellman key exchanging algorithm? Explain using notations.

[1 Mark]

d) Consider a scenario, where Alice first signs a message and then encrypt it before sending to Bob.

i) Write the format of the message using public key notations.

[0.5 Marks]

ii) Briefly explain one (1) advantage and one (1) disadvantage of this method.

[1 Mark]

Q4 a) i) What is the difference between Authentication and Authorization?

[1 Mark]

ii) Explain three-factor authentication with one (1) example per each factor.

[1.5 Marks]

iii) Explain how the dictionary attack works and what modifications should be made in storing of passwords to prevent such an attack.

[2 Marks]

b) Design a simple authentication protocol for two parties to be authenticated (two-way). You may explain the protocol using a simple diagram.

[2 Marks]

c) i) Consider the following use case.

"Shawn and Peter are two employees at an accounting firm. Shawn is the accounting manager and Peter is the in-house software engineer. An

accounting program is developed by Peter to read and make necessary changes to the accounting data that the firm has. Peter has access to read, write and execute the accounting program and Shawn can only read and execute it. Both employees can read accounting data."

Draw the Lampson's Access Control matrix for the above use case.

[2 Marks]

ii) Explain how Access Control Lists (ACLs) are different from Capability Lists (C-Lists) and state one (1) use case for each list.

[1.5 Marks]

Q5 a) i) List four (4) properties of a hash function.

[1 Mark]

ii) List two (2) hash algorithms.

[0.5 Marks]

iii) What is "Avalanche effect"?

[0.5 Marks]

iv) State two (2) applications of Hash functions and explain one (1) of them.

[1.5 Marks]

b) Using a flow diagram, explain how you would use Hash based Message Authentication Code (HMAC) to ensure the integrity of the message.

[2 Marks]

c) i) Explain one (1) example use case of Watermark in detecting acts of misuse.

[1 Mark]

ii) Explain how images can be used in steganography.

[1 Mark]

d) i) State one (1) main difference between a virus and a worm.

[0.5 Marks]

ii) Consider the following botnet attack stage detection framework.

Step 1: First, the normal profiles of the network devices are created.
Step 2: Any deviations from the normal profiles are detected as anomalies.
Step 3: These anomalies are mined to extract possible attack patterns.
Step 4: Attack patterns are used as identifiers to detect botnet attack stages.

Identify the type(s) of detections (i.e., signature-based, change-based, and anomaly-based) in the above framework and justify your answers.

[2 Marks]