UNIVERSITY OF RUHUNA

Faculty of Engineering

End-Semester 8 Examination in Engineering: September 2023

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

[Three Hours]

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

Q1 a) What is Kerckhoffs's principle in information security?

[1.0 Mark]

b) From a bank's perspective, which is usually more important, the integrity of its customers' data or the confidentiality of the data? From the perspective of the bank's customer, which is more important? Discuss your answers.

[2.0 Marks]

c) Caesar's cipher is one of the simple substitution ciphers.

i) Decrypt the following cipher text using Caesar's cipher.
Hint: Caesar's cipher uses a shift of 3.
Cipher text: "ODVW HADP"

[2.0 Marks]

ii) Explain one cryptanalysis method that can be used to break down the above Caesar's cipher.

[1.0 Mark]

d) Use Double Transposition Cipher to decrypt the following cipher text. The matrix size is 3x5 and the key is [231], [41352].
Cipher text: "xxAVLAITxSTHSAA"

[2.0 Marks]

e) What is confusion and diffusion in cryptography, and which is/are achieved by the simple substitution cipher and double transposition cipher?

[2.0 Marks]

Q2 a) Explain the difference between stream ciphers and block ciphers.

[1.0 Mark]

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

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

The cipher text is the resulting text at the end of three rounds, i.e., $C = (L_3, R_3)$. Here, F is the round function and K_i is the subkey for round i.

Given, P = 1101 0110, K_1 = 1010, K_2 = 1100, and K_3 = 0011, compute the final cipher text if $F(R_{i-1}, K_i) = K_i$.

[2.0 Marks]

c) RC4 is one of the stream ciphers invented by Ron Rivest. Initialization algorithm of RC4 is shown in Listing Q2 in pseudo-code.

Listing Q2: Initialization algorithm of RC4

```
for i = 0 to 3
        S[i] = i
        K[i] = key[i mod N]   //N is the size of the key

j = 0
for i = 0 to 3
        j = (j + S[i] + K[i]) mod 4
        swap(S[i], S[j])        ///swap the elements of S in positions i and j
```

Here, key = [3 2] and N is the size of the key.

i) Calculate the array S, after the initialization steps.

[2.5 Marks]

ii) Give two (2) examples of RC4 uses.

[1.0 Mark]

d) 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 equations for the encryption process in both logical approach and actual approach of Triple DES. Why is the latter strategy used in practice?

[1.5 Marks]

e) Message Authentication Code (MAC) is used to check integrity of messages in symmetric key cryptography. Explain using equations how the MAC received at the receiver side and the MAC computed at the receiver side will be different, if a **ciphertext** block is changed by an intruder.

[2.0 Marks]

Q3 a) Give an example of a pro and a con of public key cryptography.

[1.0 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: $C = M^e \ mod \ N$

i) For p = 11 and q = 17, calculate the private and public key values.
Hint: Select the lowest value for e, which is relatively prime with $\emptyset(N)$.

[2.0 Marks]

ii) Find the cipher text, C, given that M=6.

[2.0 Marks]

c) What is the role of Certificate Authority (CA) in public key cryptography?

[1.0 Mark]

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

i) Use public key notation to specify the message's format.

[0.5 Marks]

ii) Describe one security flow in this method.

[1.0 Mark]

e) Design a hybrid crypto system to communicate between two parties that utilizes the advantages of both symmetric key and public key crypto systems. Use a diagram and standard notations to explain the communication protocol.

[2.5 Marks]

Q4 a) What is Cyclic Redundancy Check (CRC) and why is it not suited in cryptographic systems?

[1.0 Mark]

b) Describe how online bidding system can employ hashing.

[1.0 Mark]

c) A Hash-based Message Authentication Code (HMAC) is a crucial cryptographic technique used in information security to verify the integrity of messages or data.

i) Why is it important to send the message along with the hashed message in HMAC to ensure integrity?

[1.0 Mark]

ii) How can an intruder attack the communication discussed above, and what can be done to prevent it?

[1.5 Marks]

d) Figure Q4 shows the public key encryption mode used in IPSec protocol. Analyze the security of the protocol and identify any potential security issues.

[3.0 Marks]

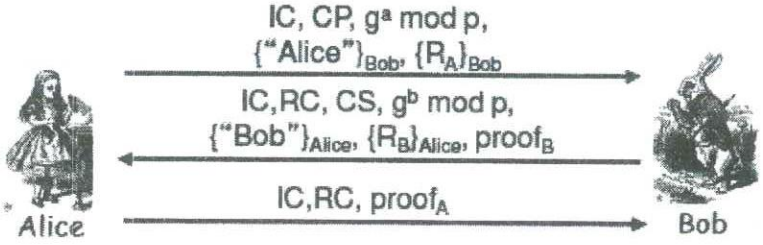

Figure Q4: Public key encryption in IPSec protocol

e) Give two (2) examples of visible and invisible watermarks, respectively.

[1.0 Mark]

f) How is steganography different from cryptography? State two (2) applications of steganography.

[1.5 Marks]

Q5 a) Consider the simple authentication protocol shown in Figure Q5. Examine the protocol and explain what Trudy can do to break this authentication and extract the key, K.

Note: T is the time stamp, K is the key, and the messages are first *encrypted* and then *signed*.

[2.0 Marks]

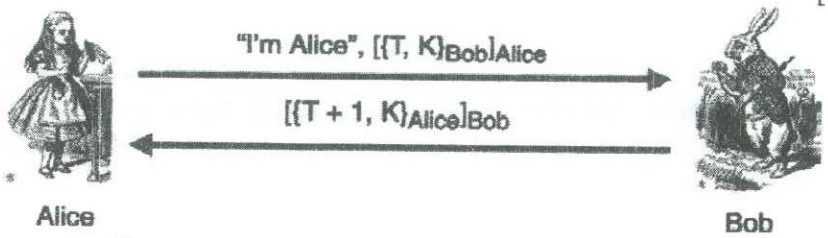

Figure Q5: A simple authentication protocol

b) State four (4) types of biometrics used in authentication.

[1.0 Mark]

c) Draw the design of an encrypted virus and discuss why it is challenging to identify them.

[1.0 Mark]

d) Most of the tech companies still primarily depend on signature-based intrusion detection systems. Explain the reasons behind and discuss potential threats of such practices.

[1.5 Marks]

e) Many websites require users to register to access information. Suppose that you register at such a website, but when you return later, you've forgotten your password. The website then asks you to enter your e-mail address and, if the address matches any e-mail address in the website's database, the corresponding password is e-mailed to that address. Discuss two (2) main security concerns with this approach in dealing with forgotten passwords.

[2.0 Marks]

f) Consider the following use case.

Alice, Bob, Carol and Trudy are four employees of a firm. Alice is the inhouse software developer, Bob is the HR manager, Carol is the accountant, and Trudy is a clerk. All the data in the firm can only be *modified* by a software system developed by Alice. Bob can read only employee data, Carol can read only accounting data, Trudy can read only customer data. All the employees except Trudy can execute the software system.

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

[2.5 Marks]