B.Sc. Engg. CSE 7th Semester 08 December 2022

# ISLAMIC UNIVERSITY OF TECHNOLOGY (IUT)
## ORGANISATION OF ISLAMIC COOPERATION (OIC)
## Department of Computer Science and Engineering (CSE)

**SEMESTER FINAL EXAMINATION** **WINTER SEMESTER, 2021-2022**

**DURATION: 3 HOURS** **FULL MARKS: 150**

## CSE 4743: Cryptography and Network Security

**Programmable calculators are not allowed. Do not write anything on the question paper.**

Answer **all 6 (six)** questions. Marks of each question and corresponding CO and PO are written in the right margin with brackets.

---

1. a) Which security mechanism(s) is/are provided in each of the following cases? 5×2 (CO1) (PO1, PO2)
   i. A school demands student identification and a password to let students log into the school server.
   ii. A school server disconnects a student if she is logged into the system for more than two hours.
   iii. A professor refuses to send students their grades by e-mail unless they provide student identification they were preassigned by the professor.
   iv. A bank requires the customer's signature for a withdrawal.
   v. A student uses Rabin-Karp hash algorithm to perform the string-matching task.

   b) Satoru obtained a cipher text "***EKF HUSF 66 C8L7U5***" and wants to decrypt it. He also found: 10 (CO2) (PO1, PO2)
   i. the key, $k = 23$
   ii. the plaintext was made of letters **(a to z)** and digits **(0 to 9)**
   iii. the encryption algorithm was Multiplicative cipher

   Help Satoru by uncovering (decrypting) the secret message.

   c) The encryption key in a transposition cipher is (3, 2, 6, 1, 5, 4). Compute the decryption key. 5 (CO2) (PO1, PO2)

2. a) Encrypt the message "***We live in an insecure world***" using Hill cipher with the following key. 10 (CO2) (PO1, PO2)

$$K = \begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$$

   Use '**z**' as the bogus character.

   b) Use Playfair Cipher to encipher the message "***mecha kawai des ne***". The secret key can be made by filling the first and part of the second row with the word "**PLAYFAIR**" and filling the rest of the matrix with the rest of the alphabet sequentially. (Use **x** as the bogus character) 8 (CO2) (PO1, PO2)

   c) Modern Block Ciphers have two properties, Diffusion and Confusion. Show how these traits are upheld by the Product Ciphers. 7 (CO1) (PO1, PO2)

3. a) "Symmetric-key exchange is better than Asymmetric-key exchange." – Analyse this statement with valid arguments and examples. 5 (CO2) (PO1, PO2)

b) Amano wants to send Erika a message ***"Section A is better"*** using on RSA cryptosystems. In this system, the prime-product is n and the public key is e. (Ignore the spaces while encrypting) 7+7+1 (CO2) (PO1, PO2)

i. Given n = 12091 and e = 3. Encrypt the message and find the private key, d for Erika so that she can decrypt the message.

ii. Given n = 100 and e = 3. Encrypt the message and find the private key, d for Erika so that she can decrypt the message.

iii. Determine which cryptosystem works in a real-life scenario.

c) Max argues that the hashing algorithm MD-5 is better than SHA-1. Lewis disagrees and states the opposite. However, both agree that these algorithms require padding of input bits even if they are a multiple of 512 bits. 5 (CO1) (PO1, PO2)

Identify why padding is required in this circumstance and elucidate the security goal associated with these hashing algorithms.

4. a) The Needham-Schroder protocol is susceptible to the *Replay Attack* as depicted in Figure 1. 10 (CO3) (PO1, PO2)

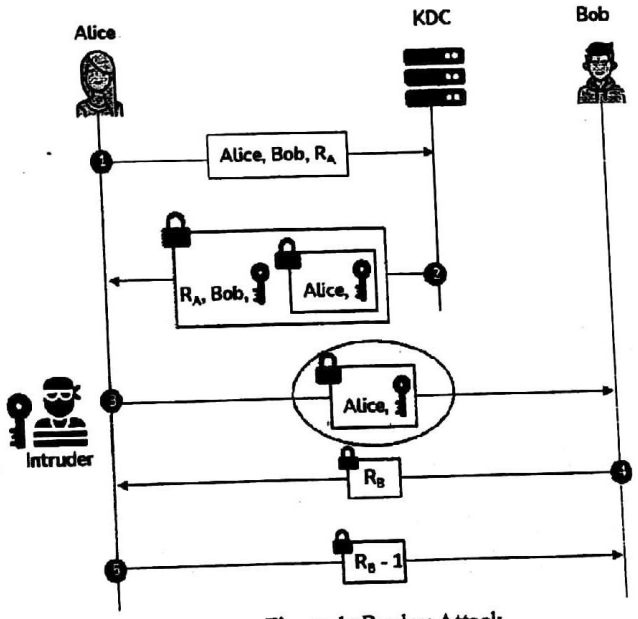


Figure 1: Replay Attack

Analyse the cause for this vulnerability. Identify the mechanism to circumvent this vulnerability with appropriate diagrams.

b) Illustrate a variant of Kerberos with diagrams which adheres to the following guidelines and answer the following questions. 7.5×2 (CO3) (PO1, PO2)

i) The workstation generates a Ticket Granting Ticket (TGT). The TGT will be encrypted with the user's master key rather than the KDC's master key.

ii) Compare this design with standard Kerberos in terms of efficiency and security? What happens in each scheme if the user changes her password during a login session?

5. a) The IPSec IKE Phase – I exchanges keys via the Diffie-Hellman technique. However, this technique is susceptible to Man-in-the-Middle (MITM) attack as illustrated in Figure 2. 3+7 (CO3) (PO1, PO2)

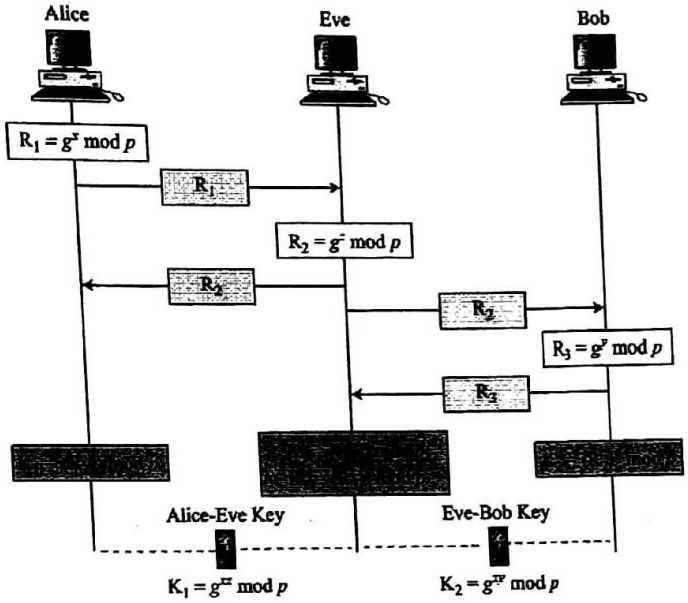


Figure 2: MITM Attack in IKE Phase – I

Now, answer the following questions.

i. Analyse how the MITM attack can be thwarted.

ii. Eve launches another attack by sending several half-keys to Bob (Server), masquerading herself as if these keys are from multiple sources. Determine with appropriate diagrams how this attack can be prevented.

b) IPSec provides a service against Replay Attacks as demonstrated in Figure 3. 10 (CO3) (PO1, PO2)

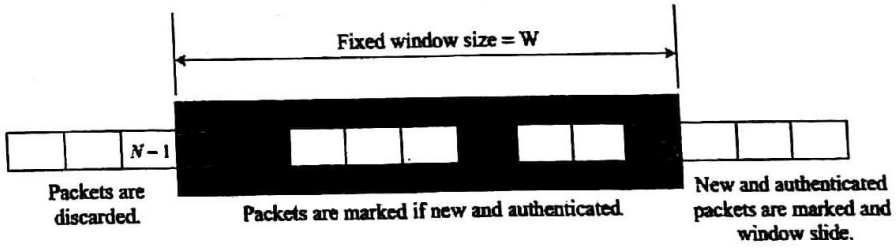


Figure 3: Replay Attack Protection

A host receives authenticated packets with the sequence numbers 181, 192, 224, 264, and 333. The replay window has a default size of 64, currently starting from sequence number 200.
What will the host do with the packets? What is the window span after each event?

c) Ayanokoji-kun wants to send a secret message to Karuizawa using the Cipher Feedback (CFB) operation. Determine the ciphertext for the first block if the original message is $(CE2F\ 7DF6\ B1A5\ 42C3)_{16}$ and the encrypted Initialization Vector (IV) is $(AD25\ EF96\ CFB3\ 4D7F)_{16}$. Consider each ciphertext block size is 8 bits. 5 (CO2) (PO1, PO2)

6. a) When a session is resumed with a new connection, SSL does not require the full handshaking process. Examine and illustrate the messages that need to be exchanged in a partial handshaking. Use diagrams, if necessary. — 7 (CO3) (PO1, PO2)

b) Compare and contrast the protocols defined in SSL and TLS. Deduce the goals of each protocol in SSL and TLS. — 8 (CO3) (PO1, PO2)

c) Security at the Transport layer employs multiple key-exchange algorithms. Answer the following questions. — 5×2 (CO3) (PO1, PO2)

   i. Assess the key exchange algorithms in SSL/TLS and judge which algorithms are more or less immune to malicious attacks.

   ii. "If an adversary reverse-engineers to find the encryption key, then the entire client-server connection is compromised" – Justify this statement.