VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

BCSE309L-Cryptography and Network Security

Continuous Assessment Test-II - October 2024

B1 Slot

Answer Key

1) Mr. Akash, Mr. Balu, and Mr. Chand would like to initiate a secret chat between them for the defense consultancy work they had obtained from DRDO. They need a common secret key that can be used in AES algorithm for their encrypted chat communication. Help them to generate the common secret key using the Diffie-Hellman algorithm using the following parameters. Q=17, α= the second primitive root in the pool of primitive roots of q. The private key of Mr. Akash, Mr. Balu, and Mr. Chand are 5,6,7 respectively.

Solution:

Q=17, α= the second primitive root in the pool of primitive roots of q {3, 5, 6, 7, 10, 11, 12, 14}

The private key of Mr.Akash,Mr.Balu and Mr.Chand are 5,6,7 respectively. The common key computed as follows:

$X_a=5$ $Y_a= 5^5 \bmod 17 = 14$	$X_b=6$ $Y_b= 5^6 \bmod 17 = 2$	$X_c=7$ $Y_c= 5^7 \bmod 17 = 10$
$X_a=5$ $Y_{ac}= 10^5 \bmod 17 = 6$	$X_b=6$ $Y_{ab}= 14^6 \bmod 17 = 15$	$X_c=7$ $Y_{bc}= 2^7 \bmod 17 = 9$
$K=9^5 \bmod 17 = 8$	**$K=6^6 \bmod 8$**	**$K=15^7 \bmod 17 =8$**

2) Suppose Anu and Binu use an ElGamal scheme with a common prime number p=67, generator or primitive root g=7, private key x=13, and random number k=9.
   a) Compute the public key. **[2 Marks]**
   b) Encrypt the message, M=20. **[3 Marks]**
   c) Use the shared secret to recover the original message, M. **[3 Marks]**
   d) If k is compromised, explain how an attacker could decrypt the message. What steps can be taken to prevent this? **[2 Marks]**

Solution:

a. The public key consists of (p,g,y) where $y=g^x \bmod p=7^{13} \bmod 67=63$
b. The ciphertext C consists of two values: C_1 and C_2.

$C_1=g^k \bmod p =7^9 \bmod 67=43$

$C_2=M \cdot y^k \bmod p = 20 \cdot (63^9 \bmod 67) =4$

c. $s=C_1^x \bmod p=43^{13} \bmod 67=27$; $s^{-1} \bmod 67=5$
$M=C_2 \cdot s^{-1} \bmod p=4 \cdot 5 \bmod 67=20$

d. In ElGamal encryption, k must be unique and random for each encryption. If the same k is reused, an attacker can link multiple ciphertexts and deduce relationships between them. This can lead to discovering the private key x, breaking the encryption scheme. Therefore, it is crucial to choose a different k for each encryption to maintain the security of the cryptosystem.

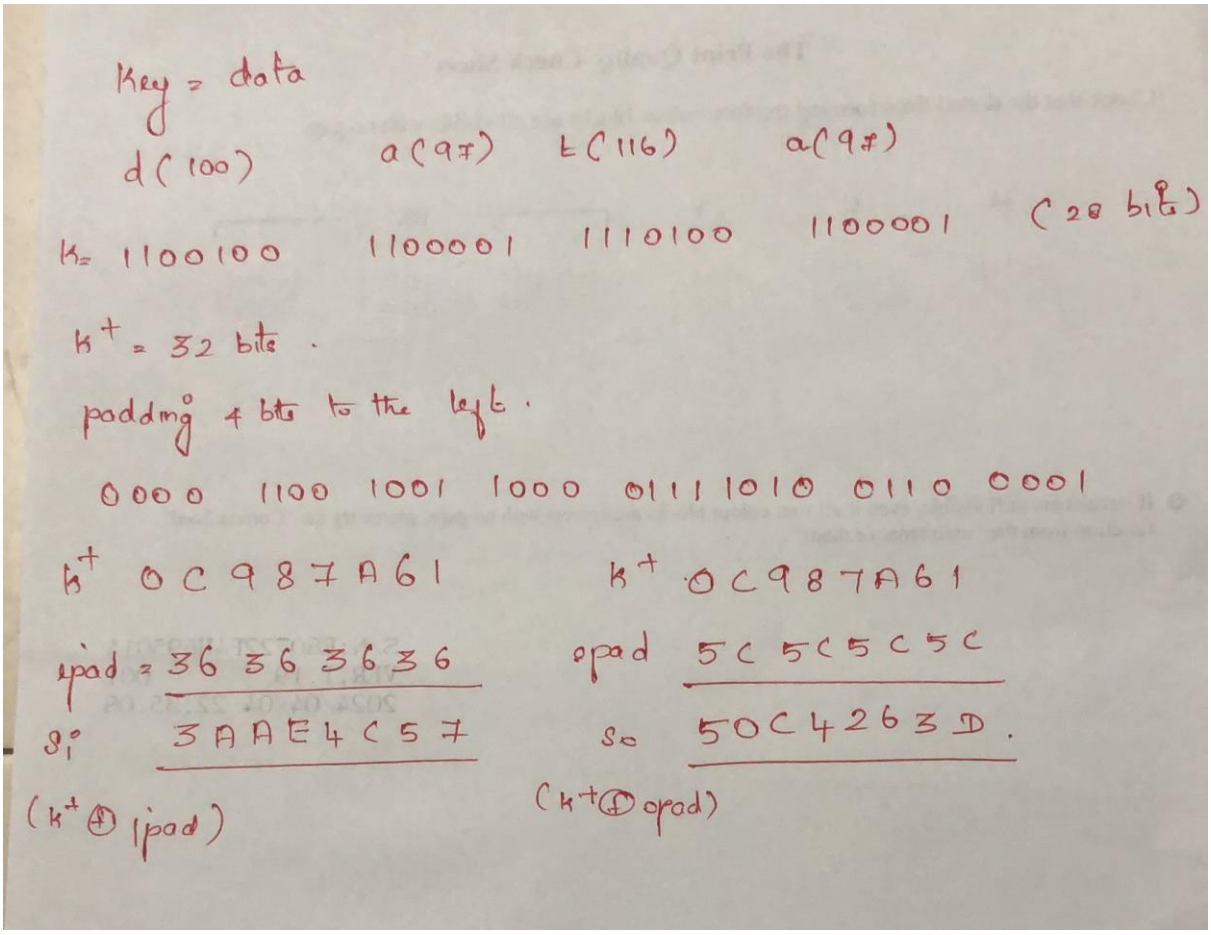
3) Arjun, a software engineer is developing a secure messaging application that allows users to communicate privately. To ensure the authenticity and integrity of the messages exchanged within the app, he decided to use Hash-based Message Authentication Code with a shared secret key "data". Each character in the key is represented using its ASCII value of 7 bits, and the block size is set to 32 bits. Since Arjun plans to implement this feature across multiple user sessions, he aims to optimize the authentication process by precomputing the values of K^+, S_i, and S_o.

a) Assist Arjun in calculating the precomputed values of K^+, S_i, and S_o and present them in hexadecimal format. **[7 Marks]**

b) Discuss the potential vulnerabilities of precomputing the values of K^+, S_i, and S_o. **[3 Marks]**

Solution:

a)



c) Key Exposure, replay attacks, lack of key rotation

4) Anil wants to sign a message using the RSA digital signature algorithm. She generates a key pair as follows: Public key: n=55, e=3, Private key: n=55, d=27. He wants to sign the message "VIT University". The hash function works as follows:
   - Each letter is assigned a number based on its position in the English alphabet: A=1, B=2, C=3, ..., Z=26.
   - The hash is the sum of the position values of the characters, and then we take the result modulo 7 to keep the output small.

   Answer the following after hashing the message:
   a) How does Anil sign the message? **[5 Marks]**
   b) How does Ballie verify Anil's signature? **[5 Marks]**

Solution:

a.Message Signing (By Anil)

Find Hash value using Hash function

Step 1: Assign Position Values to Each Letter

- We will ignore spaces and treat only the letters. Here's the position of each letter in the alphabet:
- 'V' = 22
- 'I' = 9
- 'T' = 20
- 'U' = 21
- 'N' = 14
- 'I' = 9
- 'V' = 22
- 'E' = 5
- 'R' = 18
- 'S' = 19
- 'I' = 9
- 'T' = 20
- 'Y' = 25

Step 2: Sum the Position Values

- 22+9+20+21+14+9+22+5+18+19+9+20+25=21322 + 9 + 20 + 21 + 14 + 9 + 22 + 5 + 18 + 19 + 9 + 20 + 25 = 21322+9+20+21+14+9+22+5+18+19+9+20+25=213

Step 3: Apply Modulo 7

- 213 mod 7=3
- So, the hash value of "VIT University" using our simple hash function is **3**.

Anil needs to sign the hash of the message using her private key d.

- Private Key: (n=55,d=27)

Step 1: Compute the signature S:

To create the signature, Alice raises the hash value H(M) to the power of d, then takes modulo n:

$S=H(M)^d \bmod n$

$S=3^{27} \bmod 55$

S=42

So, the **signature S is** 42

b. Message Verification (By Bob)

Balle receives the original message "VIT University " and the signature S=42. He also knows Anil's public key (n=55,e=3) and will use it to verify the signature.

Step 1: Hash the received message:

The hash of " VIT University " is H(M)=3 (already given).

Step 2: Verify the signature:

To verify the signature,

Signature S=42

- Public Key: e=3,n=55

Now, Bob calculates:

$S^e \bmod n = m$

$42^3 \bmod 55 = 3$

The result of $S^e \bmod n=3$ which matches the hash H(M). Therefore, the signature is **valid**.

5) A government agency, "National Health Service" (NHS), wants to implement a secure online portal for patients to access their medical records and communicate with healthcare providers. The portal will be used by 10 million patients and 50,000 healthcare providers across the country. To ensure the security and integrity of the portal, NHS wants to implement a Public Key Infrastructure (PKI) to authenticate and authorize users. Each patient and healthcare provider needs a digital certificate to access the portal. The digital certificates should be valid for 5 years. Each healthcare provider should have its own Certificate Authority (CA) to issue digital certificates to its patients and staff. Design a PKI architecture that meets the following requirements:

a) The number and type of CAs required. **[2 Marks]**
b) The role of each CA in the federation. **[2 Marks]**
c) The process for issuing and revoking digital certificates. **[2 Marks]**
d) The benefits of the proposed PKI architecture. **[2 Marks]**
e) How the proposed architecture addresses the security and scalability requirements of the NHS portal? **[2 Marks]**

Solution:

To meet NHS's requirements, a federated PKI architecture with multiple Certificate Authorities (CAs) should be implemented. The proposed architecture is as follows:

- **Root Certificate Authority (CA):**
  - One Root CA is required, which will be the top-most authority in the federation.
  - The Root CA will be responsible for issuing digital certificates to the healthcare provider CAs.
  - The Root CA's digital certificate will be self-signed, meaning it will sign its own certificate.
- **Healthcare Provider Certificate Authorities (CAs):**
  - Each healthcare provider will have its own CA, which will be responsible for issuing digital certificates to its patients and staff.
  - The number of healthcare provider CAs required is 50,000, one for each healthcare provider.
  - Each healthcare provider CA will be issued a digital certificate by the Root CA.

- **Digital Certificate Issuance:**
    - When a patient or healthcare provider registers for the portal, the healthcare provider CA will issue a digital certificate to the user.
    - The digital certificate will contain the user's public key, identity information, and other relevant details.
    - The digital certificate will be valid for 5 years, as per the agency's requirement.
- **Digital Certificate Revocation:**
    - When a patient or healthcare provider's status changes (e.g., a patient moves to a different healthcare provider), the healthcare provider CA will revoke the user's digital certificate immediately.
    - The revoked certificate will be added to a Certificate Revocation List (CRL), which will be maintained by the Root CA.
    - The CRL will be updated regularly and made available to all healthcare providers, ensuring that revoked certificates are not accepted by the portal.

Benefits of the Proposed PKI Architecture:

- **Scalability:** The federated architecture allows for easy scalability, as new healthcare providers can be added by simply installing a new CA.
- **Decentralized Management:** Each healthcare provider has its own CA, which reduces the management burden on the central IT department.
- **Improved Security:** The use of digital certificates and a federated PKI architecture ensures strong authentication and authorization of users, reducing the risk of unauthorized access to the portal.
- **Flexibility:** The proposed architecture allows for easy revocation of digital certificates, ensuring that users who are no longer authorized to access the portal are denied access.

Addressing Security and Scalability Requirements:

- **Security:** The proposed architecture ensures strong authentication and authorization of users through the use of digital certificates and a federated PKI structure. This reduces the risk of unauthorized access to the portal and protects sensitive patient information.
- **Scalability:** The federated architecture allows for easy scalability, as new healthcare providers can be added by simply installing a new CA. This ensures that the PKI system can handle the large number of users (10 million patients and 50,000 healthcare providers) and can scale to meet future growth.

*****