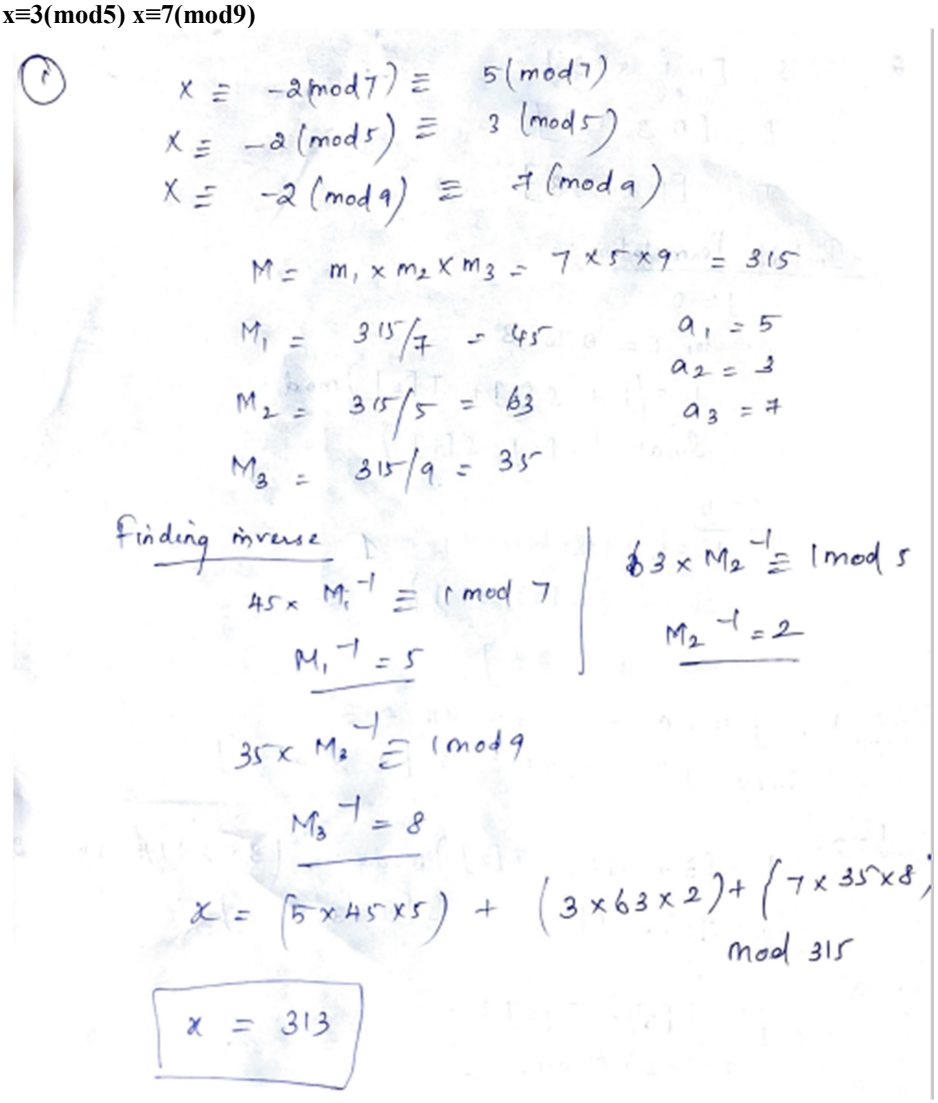
B1 SLOT

1. A logistics company uses three different types of delivery trucks: Type A, Type B, and Type C.
Each type of truck has a specific maintenance schedule:
Type A trucks are serviced every 7 days.
Type B trucks are serviced every 5 days.
Type C trucks are serviced every 9 days.
The company is planning a large maintenance day when all trucks will be serviced together. However, they realize that they already missed this by 2 days. They need to determine how many days from now they will have the next opportunity to service all trucks on the same day.
Determine the smallest positive integer x such that:
$x \equiv -2 \pmod 7$
$x \equiv -2 \pmod 5$
$x \equiv -2 \pmod 9$
$x \equiv 5 \pmod 7$ $x \equiv 3 \pmod 5$ $x \equiv 7 \pmod 9$



2. Alice and Bob decide to use a toy version of RC4 to securely communicate. Instead of the full 256-byte state array used in the standard RC4, they use a smaller version of 4x2 bits, to make things easier. So, they will operate on a 2 bits plaintext as S can take values from 0 to 3. They use a 2x2 key K = [1, 2] and plaintext P = [0, 3, 1, 2].

a) **Perform the initial permutation. (5)**
b) **Determine the ciphertext. (5)**

2. S : [0 1 2 3]

P : [0 3 1 2]

T : [1 2 1 2]

Initial Permutation:

j = 0

for i = 0 to 3

j = (j + S[i] + T[i]) mod 4

Swap (S[i], S[j])

i = 0

j = (0+0+1) mod 4 = 1

Swap (S[0], S[1])

S : [1 0 2 3]

i = 1 ; j = 1 + 0 + 2 = 3 mod 4 = 3

Swap S[1] & S[3] : S [1 3 2 0]

i = 2

j = (3 + S[2] + T[2]) mod 4 = (3 + 2 + 1) mod 4 =

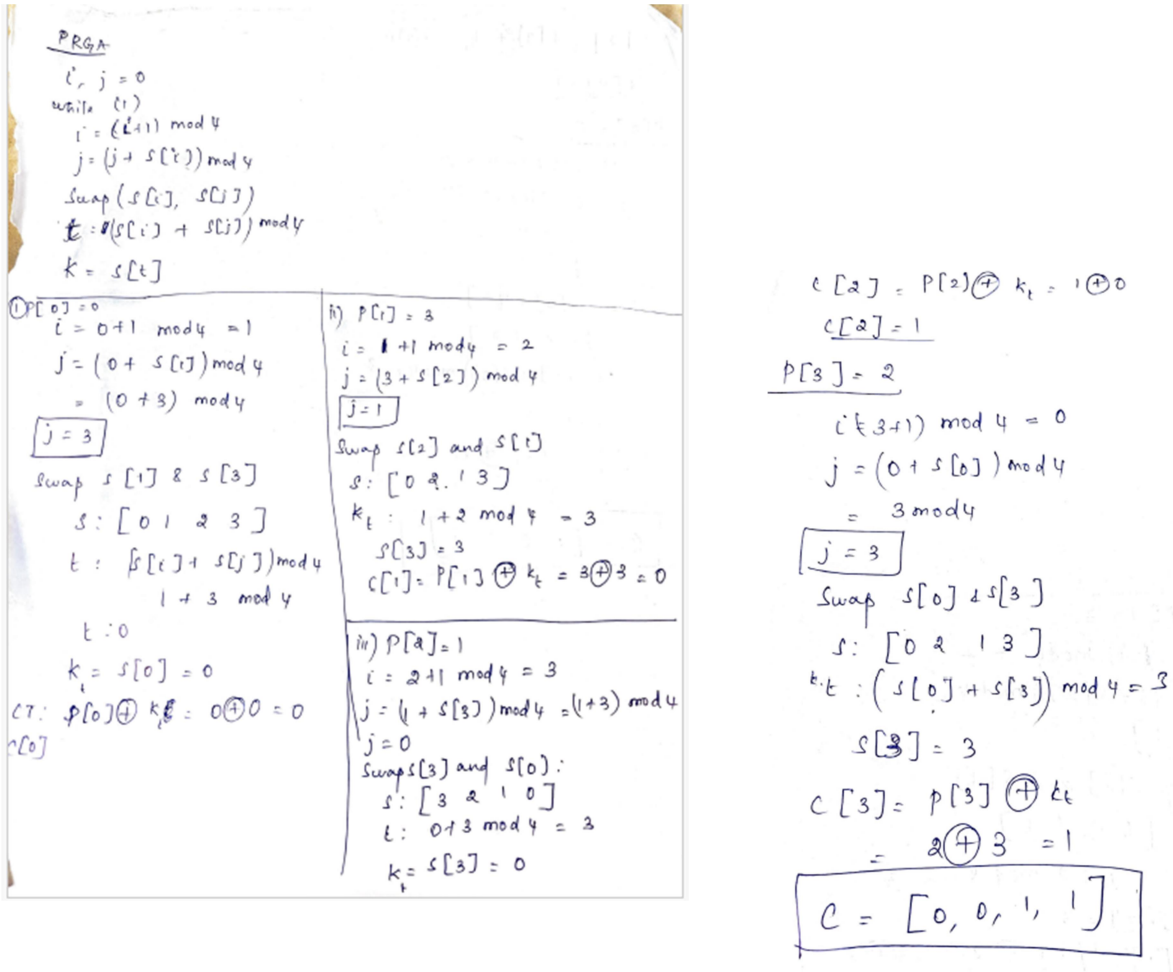
Swap S[2] & S[2] : S [1 3 2 0]

i = 3

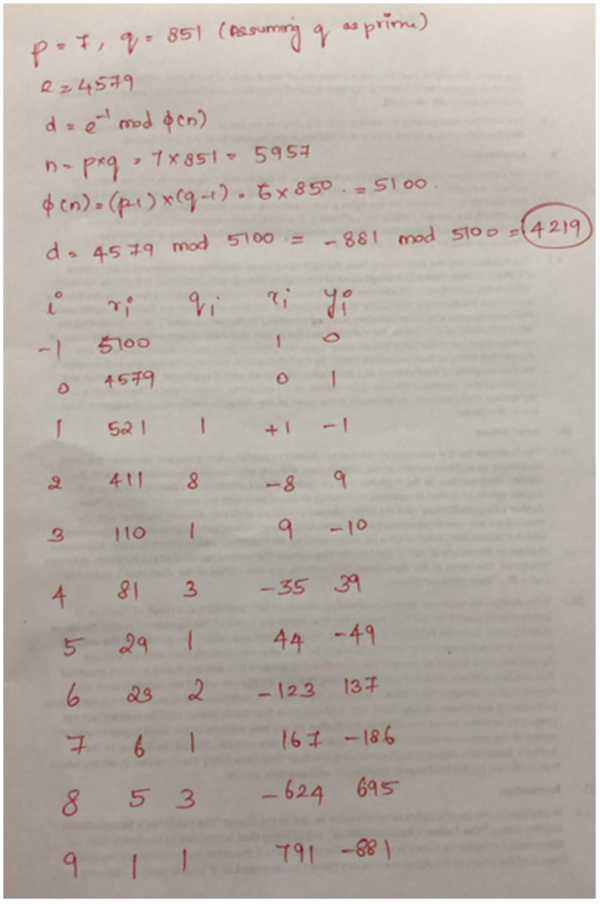
j = (2 + S[3] + T[3]) mod 4

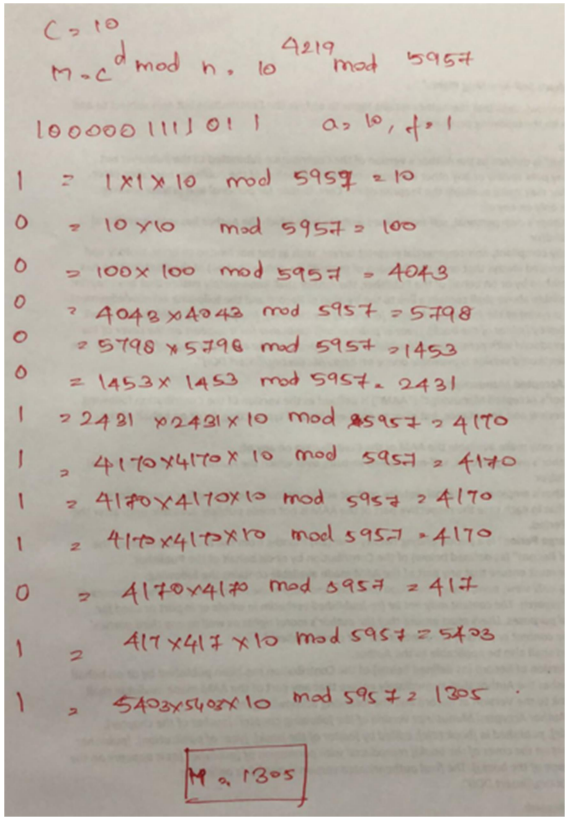
= (2+0+2) mod 4 = 0

S[3] and S[0] : S [0 3 2 1]

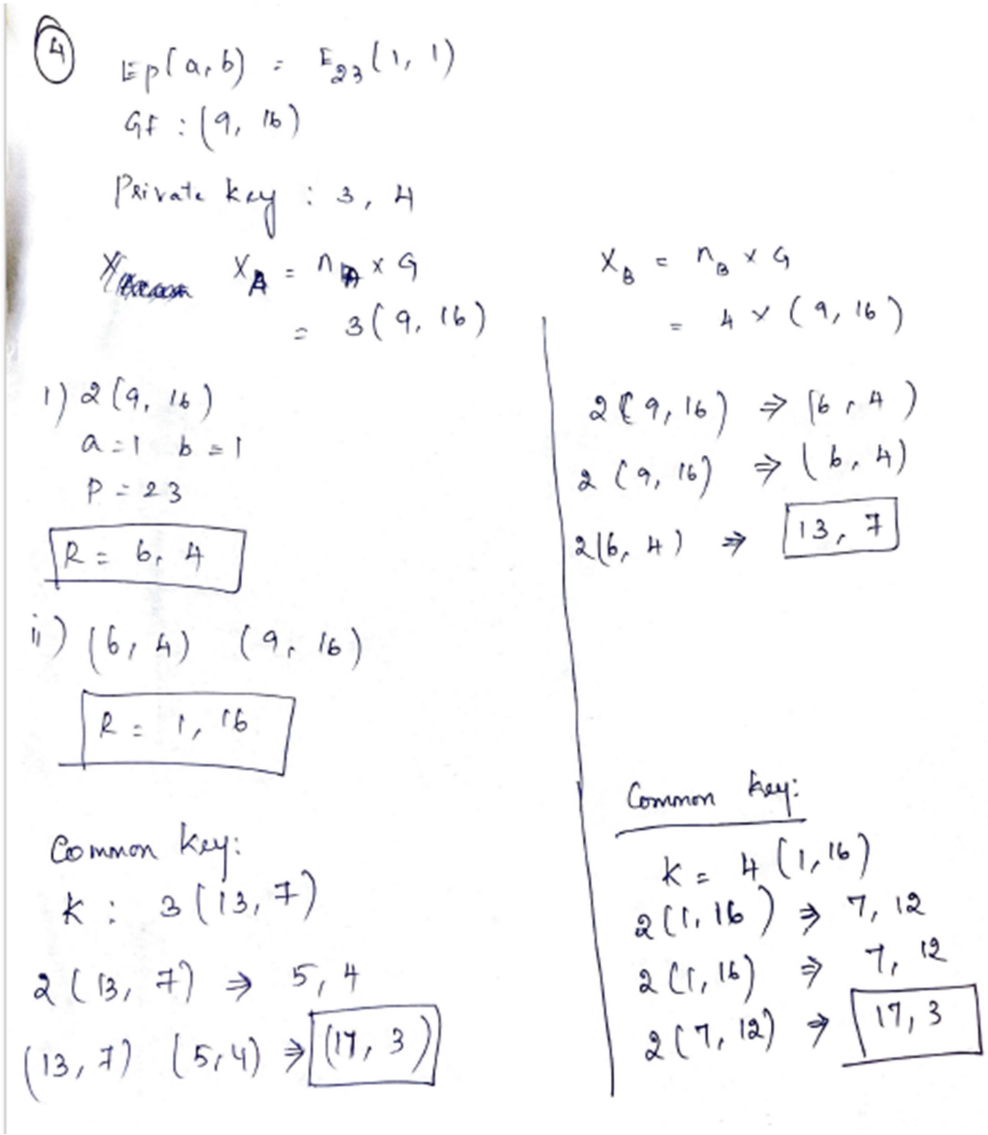


3. Given the RSA modulus with two prime numbers p =7 and q =851 Compute the value of Euler's totient function ϕ(n). If the public key exponent e=4579, calculate the private key exponent d . Suppose you intercept a ciphertext C=10 sent to a user whose public key is (e, n). Determine the plaintext M using the RSA algorithm.





4. Mr. Akash and Mr.Balu 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 which can be used in AES algorithm for their encrypted chat communication. Help them to generate the common secret key using Elliptic Curve Cryptography algorithm using the following parameters. Ep(a,b)= E_{23}(1,1), The private key of Mr.Akash and Mr.Balu are 3 and 4 respectively. GF point is (9,16)



5. Mr. Balu is exploring the MD5 algorithm and wants to evaluate the buffer values after one operation of round 2. He is working with the following values: Message M = 7A6FBCD2, Key K = A8304613, No of shifts S = 9 bits, A = 5A827999, B = C3D2E1F0, C = 8F1BBCDC, D = 6A09E667. Compute the resulting buffer values after completing one operation sequence of this round. [10 Marks]

Solution:

Step 1: Evaluate G Function

G(B, C, D) = (B ∧ D) ∨ (C ∧ ¬D) = C520F1F8

Step 2: Compute the sum

A+G(B, C, D)+M+K = EED52E26

Step 3: Perform left rotation

Left rotate EED52E26 by 9 bits = D52E26F4

Step 4: Add the result to B

C3D2E1F0 + D52E26F4 = 98FFF8E4

Final Buffer Values:

A=6A09E667

B=98FFF8E4

C=C3D2E1F0

D=8F1BBCDC

6. The software update distribution system uses a prime number q=73 and α = 41, which is a primitive root of 73, to ensure that updates are both authentic and unmodified before being applied to devices. Software Provider A is responsible for generating and distributing software updates and selects a private key X_A=25. It sends the software update with a hash value of 45 and generates the signature using a chosen integer K=7. Device B is a client device with its own private key X_B = 32 that receives the updates and wants to verify the authenticity of the received software update. Use the appropriate algorithm to generate and verify the authenticity of the update.

$q = 73, \alpha = 41, X_A = 25, X_B = 32, K = 7$

$H(M) = m = 45$

Signing

$S_1 = \alpha^K \bmod q = 41^7 \bmod 73 = 36$

$K^{-1} \bmod (q-1) = 7^{-1} \bmod 72 = 31$

$S_2 = K^{-1}(m - X_A S_1) \bmod (q-1)$

$= 31(45 - (25 \cdot 36)) \bmod 72$

$= 31(-855) \bmod 72 = -26505 \bmod 72 = -9 \bmod 72$

$= 63$

$(S_1, S_2) = (36, 63)$

Verification

$V_1 = \alpha^m \bmod q = 41^{45} \bmod 72 = 72$

$V_2 = (Y_A)^{S_1} (S_1)^{S_2} \bmod q = 36^{36} \cdot 36^{63} \bmod 73$

$= 1.72 \bmod 73 = 72$

$\boxed{V_1 = V_2}$

7. Mr.Prem is running a Cyber Café, which cater the needs of the following services to his customers: File Service, E-mail Service, Print Service, Web Service etc. He would like to construct a secure system which enables the users to authenticate themselves once per login session/type of service/service session to avail those services. With a neat sketch design a suitable ticketing gatekeeper/ticketing mechanism in Mr.Prem's prototype and discuss the dialogue that occurs between various entities/stack holders in his system for the successful user authentication to avail various above said services.

Once per user logon session:

(1) C → AS: $ID_C \| ID_{tgs}$

(2) AS → C: $E(K_c, Ticket_{tgs})$

Once per type of service:

(3) C → TGS: $ID_C \| ID_V \| Ticket_{tgs}$

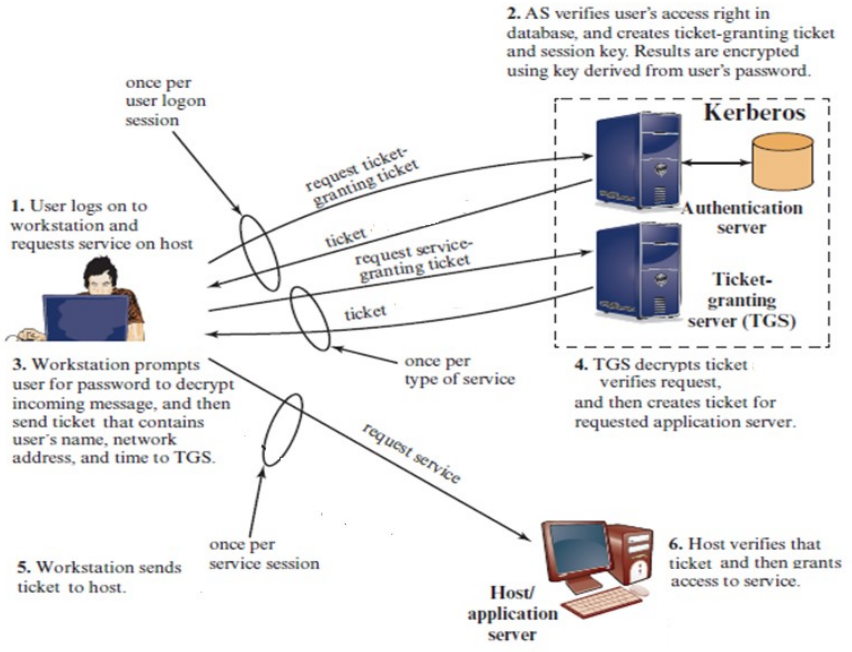
(4) $TGS \rightarrow C$: $Ticket_v$

Once per service session:

(5) C → V: $ID_C \| Ticket_v$

$Ticket_{tgs} = E(K_{tgs}, [ID_C \| AD_C \| ID_{tgs} \| TS_1 \| Lifetime_1])$

$Ticket_v = E(K_v, [ID_C \| AD_C \| ID_v \| TS_2 \| Lifetime_2])$



8. Imagine a large organization with two branches A and B, that need to securely communicate over the internet. The IT team is implementing IPsec to protect the data exchanged between the entire networks of A and B. During the deployment, they need to decide which mode of IPsec would be more appropriate for securing the communication. Explain which IPsec mode is better suited for securing communication between these entire networks, and describe how the two modes differ in terms of functionality and application in this context.

Tunnel Mode (Appropriate for Entire Networks)

 Functionality: Tunnel mode encapsulates the entire original IP packet (both the payload and the header) inside a new IPsec packet. A new outer IP header is created, and the entire packet is encrypted and

authenticated. This mode is designed for secure communication between two networks, where routers or gateways at each branch office handle encryption and decryption.

 Application: In this scenario, where both branches need to communicate securely over the internet, Tunnel mode is ideal. The routers or gateways at Office A and Office B will encapsulate and encrypt the traffic coming from any device within their respective networks, protecting all data as it traverses the insecure internet. The outer IP header routes the packet between the gateways, while the original IP packet remains hidden and protected inside.

 Use Case: Tunnel mode is commonly used for site-to-site VPNs or network-to-network communication, where multiple devices within one network need to securely connect to devices in another network.

Transport Mode (For Host-to-Host Communication)

 Functionality: Transport mode encrypts only the payload of the IP packet, leaving the original IP header intact. Only the data being transmitted (the payload) is protected, while the routing information remains visible. This mode is typically used for direct communication between two individual hosts.

 Application: In this context, Transport mode would not be appropriate, as it is designed for securing end-to-end communication between two individual devices (such as two computers) rather than between two entire networks. Each device would have to handle the encryption and decryption on its own, which is less practical when securing communication between large networks.

 Use Case: Transport mode is more suitable for host-to-host communication, such as securing data between two individual servers or workstations.

9. (i) Explain the five main services offered by PGP (Pretty Good Privacy) to enhance digital communication security? [5 Marks]

PGP enhances digital communication security through:

1. Confidentiality: Protects data from unauthorized access.
2. Authentication: Verifies the sender's identity.
3. Integrity: Ensures the message remains unchanged.
4. Non-Repudiation: Prevents the sender from denying their involvement.
5. Compression: Optimizes data transmission and storage.

These services make PGP a robust tool for secure communication and data protection.

(ii) The first 16 bits of the message digest in a PGP signature are exposed in plaintext.

a) To what extent does this compromise the security of the hash algorithm? (2 Marks)

Revealing the first 16 bits of the hash digest in a PGP signature has a **minor impact** on the security of the hash algorithm, provided the algorithm is cryptographically strong (e.g., SHA-256 or better). The primary security properties (pre-image resistance and collision resistance) remain largely intact. However:

- The reduced search space slightly weakens brute-force protection.
- For older or weaker hash algorithms (e.g., MD5, SHA-1), this exposure may exacerbate known vulnerabilities.

It is important to use modern, robust hash functions to minimize any potential risks.

b) To what extent does this serve its intended function, specifically helping to verify if the correct RSA key was used to decrypt the digest? (3 Marks)

Revealing the first 16 bits of the hash digest serves its intended function effectively by acting as a quick checksum to verify if the correct RSA private key was used to decrypt the signature. Here's how and why:

1. **Verification of Key Usage**:
    - The first 16 bits of the decrypted hash are compared with the plaintext-exposed value.
    - If they match, it confirms that the RSA decryption likely used the correct private key.
2. **Efficiency in Verification**:
    - This allows early detection of incorrect keys without needing to recompute or verify the entire hash digest, saving computational resources.
3. **Minimizing Overhead**:
    - By verifying only the first 16 bits first, the system reduces unnecessary cryptographic operations, especially if multiple keys need to be tested.
4. **No Security Impact on RSA**:
    - This does not compromise the RSA encryption itself because the verification process only works if the private key is valid.
5. **Conclusion**:
    - The exposure of the first 16 bits is a practical design choice that balances efficiency with security, ensuring the RSA key was correctly used without revealing significant information about the hash or message.

10. You have recently joined the security team of a mid-sized company that is expanding its IT infrastructure to support online services, remote work, and cloud-based applications. As part of this expansion, the Chief Information Security Officer (CISO) has tasked you with assessing the current state of the network security and recommending an appropriate solution for deployment. Currently, the company lacks a formal solution, relying only on firewall rules and antivirus software for security. With the increasing volume of network traffic and sensitive customer data being handled, the CISO is concerned about potential threats, including insider threats, zero-day attacks, and advanced persistent threats (APTs). The company has diverse needs, including protecting its internal network from insider threats, monitoring web traffic for potential vulnerabilities, securing its cloud infrastructure, and identifying anomalous behaviour that could indicate malware infections or data exfiltration. The company also anticipates rapid growth. Explain the types of systems that you would consider for the company's needs.

Types of Intrusion Detection

Host based

Network based

Application based