1. In an IoT ecosystem, a trust model is implemented to establish trust

between IoT devices and a central server. The trust model uses a

reputation-based system, where each device accumulates trust points

based on its behavior over time. Device A currently has 500 trust points,

and Device B has 750 trust points. The trust model allows devices to

establish connections with other devices if their combined trust points

exceed a certain threshold of 1000 points. a) Will Device A and Device B

be able to establish a connection based on the trust models threshold?

b) If the trust threshold is increased to 1200 points, will they be able to

establish a connection? c) What is the minimum trust points Device C

should have to establish a connection with Device A, assuming Device A

maintains its XXX trust points?

Also In an IoT ecosystem, a trust model is implemented to establish trust

between IoT devices and a central server. The trust model uses a

reputation-based system, where each device accumulates trust points

based on its behavior over time. Device A currently has 500 trust points,

and Device B has 750 trust points. The trust model allows devices to

establish connections with other devices if their combined trust points

exceed a certain threshold of 1000 points. a) Will Device A and Device B

be able to establish a connection based on the trust model&#39;s threshold?

b) If the trust threshold is increased to 1200 points, will they be able to

establish a connection? c) What is the minimum trust points Device C

should have to establish a connection with Device A, assuming Device A

maintains its 500 trust points?

1. In an IoT network, a system is using a symmetric encryption algorithm to

secure its communications. The system generates a new random

symmetric encryption key for each session. The key size is XXX bits.

Calculate the total number of possible keys that can be generated using

this key size. Also, if the system generates a new key for every hour,

calculate how long it would take for an attacker to exhaust all possible

keys through a brute-force attack if they can try 1 million keys per

second.

Also In an IoT network, a system is using a symmetric encryption algorithm to

secure its communications. The system generates a new random

symmetric encryption key for each session. The key size is 256 bits.

Calculate the total number of possible keys that can be generated using

this key size. Also, if the system generates a new key for every hour,

calculate how long it would take for an attacker to exhaust all possible keys through a brute-force attack if they can try 1 million keys per

second.

1. If encrypted text PIPAF UIT is decrypted as NINAD SIR; with key = 2 , the find what

should be decrypted text if the encrypted text is “PIPAF UIT YAU VOWGJ”

with key = 2 and If key is ceil(XXX/100) then what will be new encryption

1. Suppose you are designing a secure IoT system that uses encryption to

protect sensor data during transmission. You decide to use Advanced

Encryption Standard (AES) with a XXX-bit key for encryption and

decryption. Calculate the total number of possible keys in this AES

encryption scheme. Explain why using a longer key might be more secure.

1. If the 1 bit left shift operation was carried out on the data and then all the

bits are reversed and again 1 bit right shift operation is carried out then

what will be final number generated at the output? Data=

11001100101010010101 Also use same IOT encryption to send current time HHMM as per your watch

1. You have a fleet of XXX IoT sensors (1 year old) to be deployed in an

industrial setting, What will be the cost of implementing cloud security

measures for these devices for entire year. Given following details 1.

\*Device Authentication\*: Cost per device certificate: INR10 2. \*Data

Encryption\*: Cost of encryption key management system: INR 200/month

3. \*Access Control\*: Cost of access control system: INR 300/month 4.

\*Intrusion Detection\*: Cost of intrusion detection service: INR 50/month

per device 5. \*Firmware Updates\*: Cost of firmware update service: INR

100/device/year 6. \*Data Privacy\*: Cost of data anonymization service:

INR 5/device/month 7. \*Backup and Recovery\*: Cost of backup and

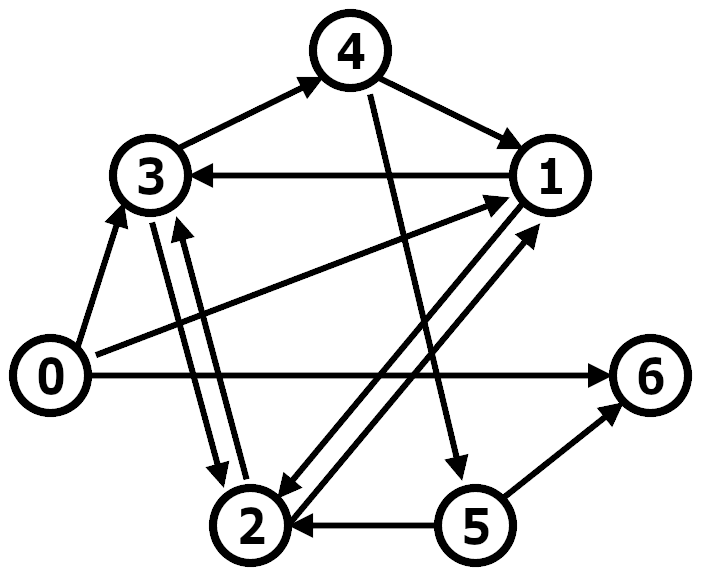
recovery service: INR 500/month 8. \*Incident Response\*: Cost of incident

response plan implementation: INR 2,000 - Cost of incident response

team per hour: INR 100/hour - Total response time for the year: 30

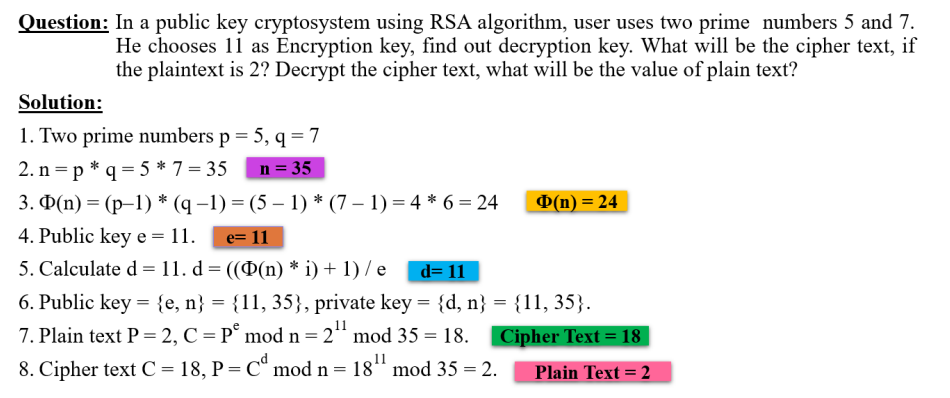
minutes/year 9. \*Third-Party Audits\*: Cost of third-party security audit:

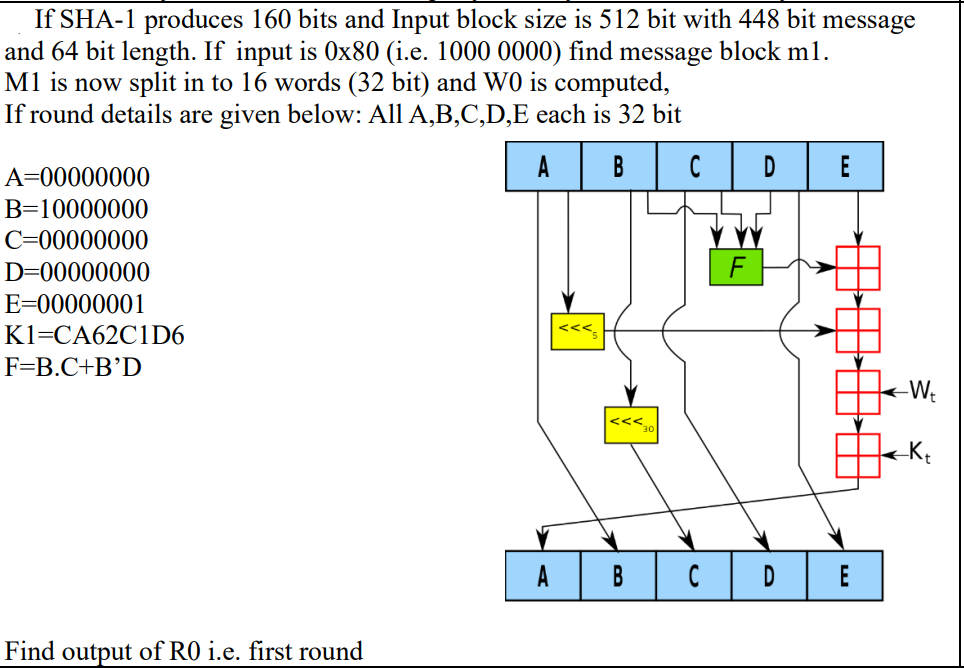
INR 5,000/year

1. If H(k) = floor(m\*((K\*A) mod 2)) and m=11 Slot= k mod m where K=5534 and A=0.XXX In which slot the particular function will map to?
2. For the given graph find all possible Hamilton paths:

If the mapping is X1 to X3, X3 to X5 and so on similarly X2 to X4 and so on find final updated connection matrix

1. Refer solved problem below and use ceil(XXX/10) instead of 11



1. 

XXX --- 3 digit of roll number