- **Compare the performance of AES and DES?**

AES	DES
Key length varies from 128 bits, 192 bits to 256 bits.	Key length is of 64 bits.
AES can encrypt 128 bits of plain text.	DES can encrypt 64 bits of plain text.
AES structure is based on substitution-permutation network.	DES structure is based on Feistal network.
Rounds per key length: 128 bits - 10 192 bits - 12 256 bits - 14	16 rounds of identical operations.
The operation rounds involved in AES encryption are Byte Substitution, Shift Row, Mix Column, and Key Addition.	Expansion, XOR operation with round key, Substitution, and Permutation are the rounds used in DES encryption
No known attacks.	Brute-force, Linear crypt-analysis and Differential crypt-analysis.
Because DES uses a smaller key, it is ***less secure.***	Because AES uses a large secret key, it is ***more secure.***

- **Is AES a Feistel cipher? Justify your answer?**

  No, AES is not a feistel cipher.

  AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant, with a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. Most AES calculations are done in a particular finite field. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

- **Is there any difference between message digest and message authentication code? Justify your answer.**

  Yes, there is a difference between digest and message authentication code.

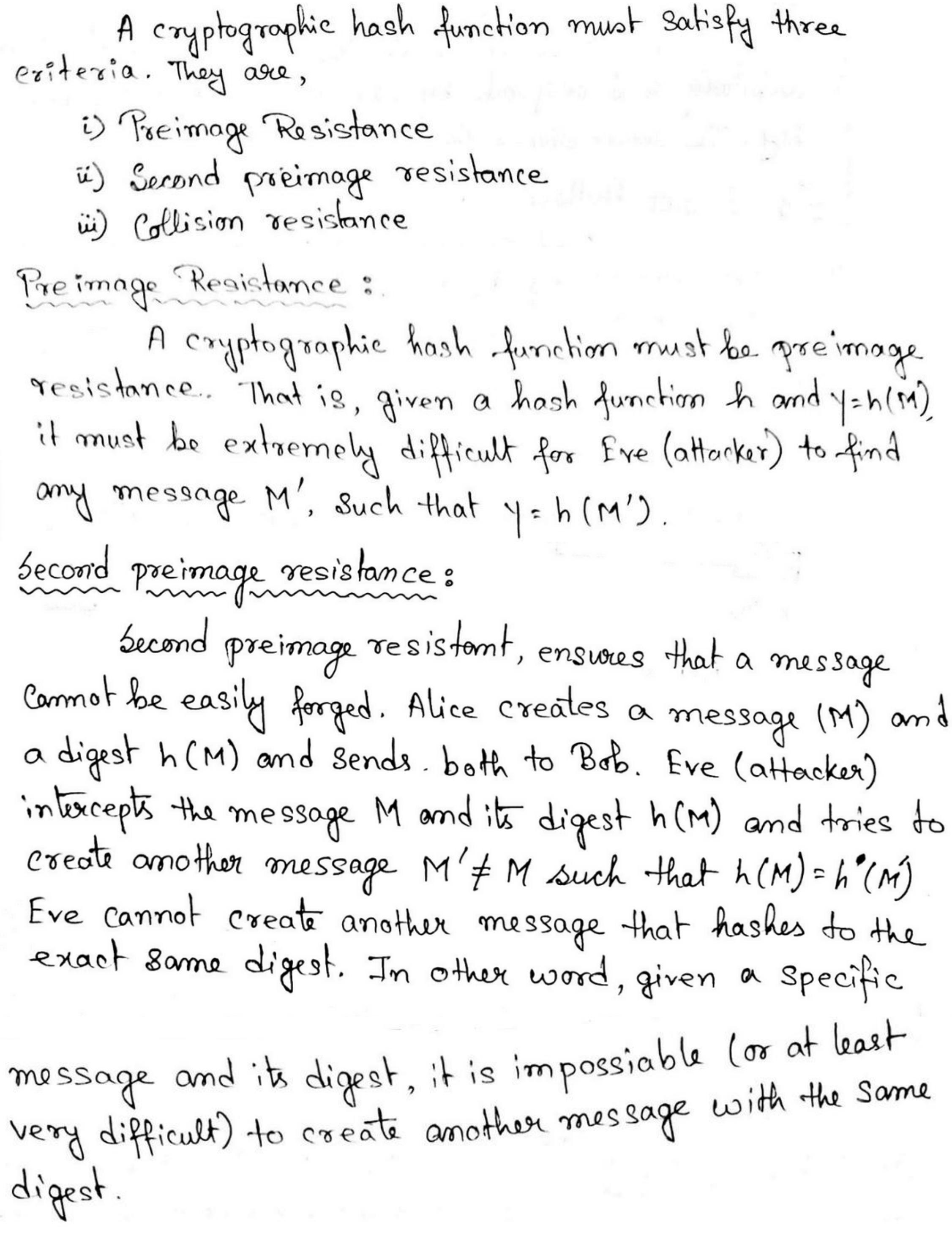
  A **message digest algorithm** takes a single input, like a message and produces a message digest which helps us to verify and check the integrity of the message. Any change in the input message, results in different hash being generated. An attacker has no clue about the message, once a hash is generated.

  A **message authentication code algorithm** takes two inputs, one is a message and another is a secret key which produces a MAC, that allows us to verify and check the integrity and authentication of the message. Any change in the secret key, or the message, results in different MAC being generated. An attacker cannot identify and validate the correct MAC without the secret key

- **What do you mean by packet sniffing?**

  When any data has to be transmitted over the computer network, it is broken down into smaller units at the sender's node called data packets and reassembled at receiver's node in original format. Packet sniffing is the action of detecting, reading, and recording packets of data being sent across a network. Network administrators or cyber criminals engage in packet sniffing by using packet sniffers, which are either physical devices or software applications. Packet sniffing is used to capture data such as web browsing histories, usernames and passwords, bandwidth usage, and much more.

- **State the conditions that a hash function should satisfy?**



A cryptographic hash function must satisfy three criteria. They are,

i) Preimage Resistance
ii) Second preimage resistance
iii) Collision resistance

Preimage Resistance :

A cryptographic hash function must be preimage resistance. That is, given a hash function h and $y = h(M)$, it must be extremely difficult for Eve (attacker) to find any message M′, such that $y = h(M')$.

Second preimage resistance :

Second preimage resistant, ensures that a message Cannot be easily forged. Alice creates a message (M) and a digest h(M) and sends both to Bob. Eve (attacker) intercepts the message M and its digest h(M) and tries to create another message $M' \neq M$ such that $h(M) = h(M')$. Eve cannot create another message that hashes to the exact same digest. In other word, given a specific message and its digest, it is impossiable (or at least very difficult) to create another message with the same digest.

Collision Resistance :

Collision resistance ensures that Eve (attacker) Cannot find two messages that hash to the Same value. Collision of a hash function is the event when two message M and M' such that $M \neq M'$ hashes to the Same value that is $h(M) = h(M')$. A given hash function is said to be collision resistance when it is difficult for Eve (attacker) to find collision.

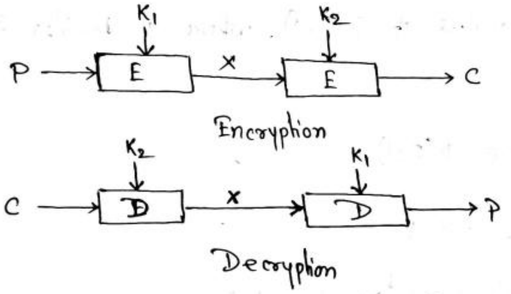
- **"Meet-in-the-middle attack is a specific attack for 2-DES" – Explain?**

The use of double DES results in a mapping that is not equivalent to a single DES encryption. But there is a way to attack this scheme, the algorithm is known as a meet-in-the middle attack. It is on the observation that if we have,

$$C = E(K_2, E(K_1, P))$$

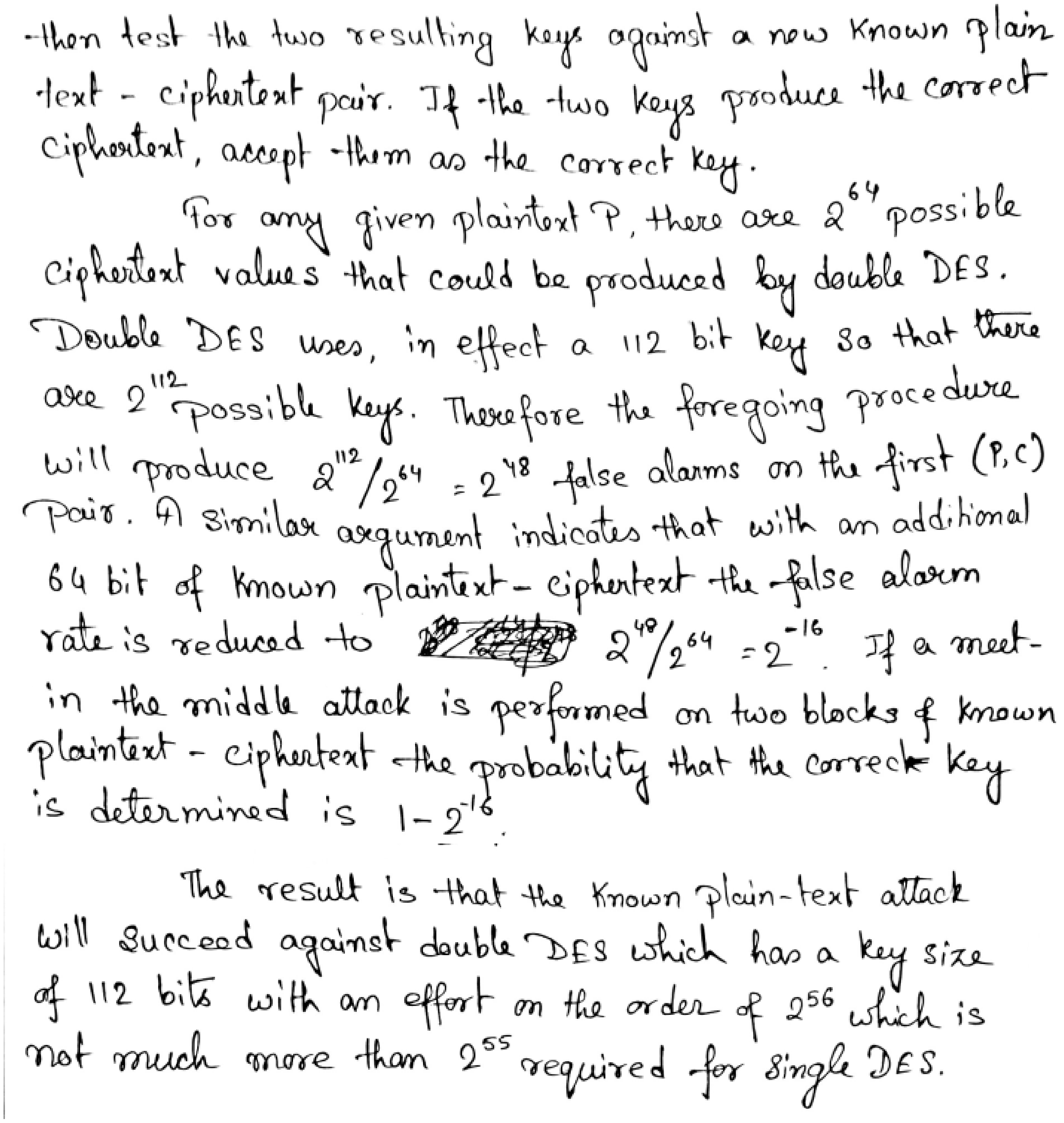
then,

$$X = E(K_1, P) = D(K_2, C).$$



$$P = D(K_1, D(K_2, C))$$

Given a pair (P, C) the attack proceeds as follows, First encrypt P for all 2^{56} possiable values of the key (K_1). Since these results in a table and then sort the table by the value of X. Next decrypt C using all 2^{56} possiable valu of key (K_2). As each decryption is produced check the result against the table for a match. If a match occurs



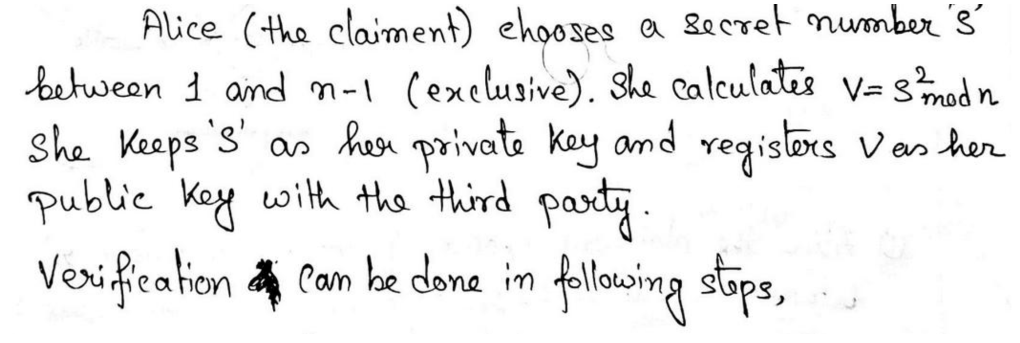
then test the two resulting keys against a new known plain text - ciphertext pair. If the two keys produce the correct ciphertext, accept them as the correct key.

For any given plaintext P, there are 2^{64} possible ciphertext values that could be produced by double DES. Double DES uses, in effect a 112 bit key so that there are 2^{112} possible keys. Therefore the foregoing procedure will produce $2^{112}/2^{64} = 2^{48}$ false alarms on the first (P, C) Pair. A similar argument indicates that with an additional 64 bit of known plaintext - ciphertext the false alarm rate is reduced to $2^{48}/2^{64} = 2^{-16}$. If a meet-in the middle attack is performed on two blocks of known plaintext - ciphertext the probability that the correct key is determined is $1-2^{-16}$.

The result is that the known plain-text attack will succeed against double DES which has a key size of 112 bits with an effort on the order of 2^{56} which is not much more than 2^{55} required for single DES.

- **State the principle of zero knowledge authentications?**

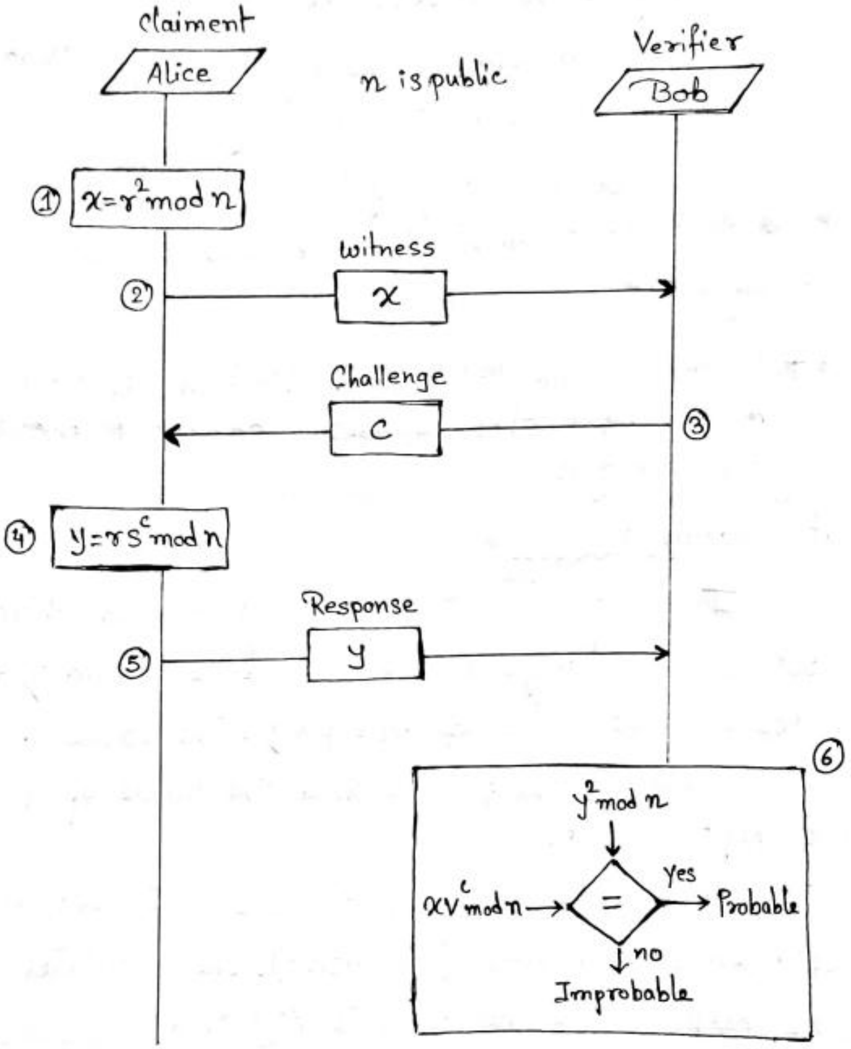
Alice chooses two large prime numbers p and q, and calculates the value n = p X q.



Alice (the claiment) chooses a secret number 'S' between 1 and n-1 (exclusive). She calculates $V = S^2 \bmod n$ She keeps 'S' as her private key and registers V as her public key with the third party.

Verification can be done in following steps,

s: Alice's private key
v: Alice's public Key
r: Random number



① Alice the claimant, chooses a random number 'r' between 0 and $n-1$. She then calculates the value of,

$$x = r^2 \bmod n$$

x is called the witness.

② Alice sends x to Bob as the witness

③ Bob, the verifier, sends the challenge c to Alice. The value of c is either 0 or 1.

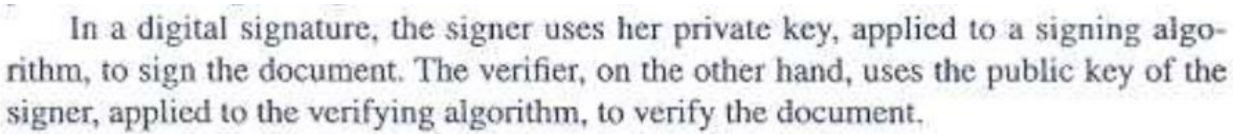
④ Alice calculate the response $y = rs^c$. Note that 'r' is the random number selected by Alice in the first step. 'S' is Alice's private key and 'c' is the challenge.

⑤ Alice sends the response to Bob to show that ~~shes~~ She knows the value of her private key 'S'. She claims to be Alice.

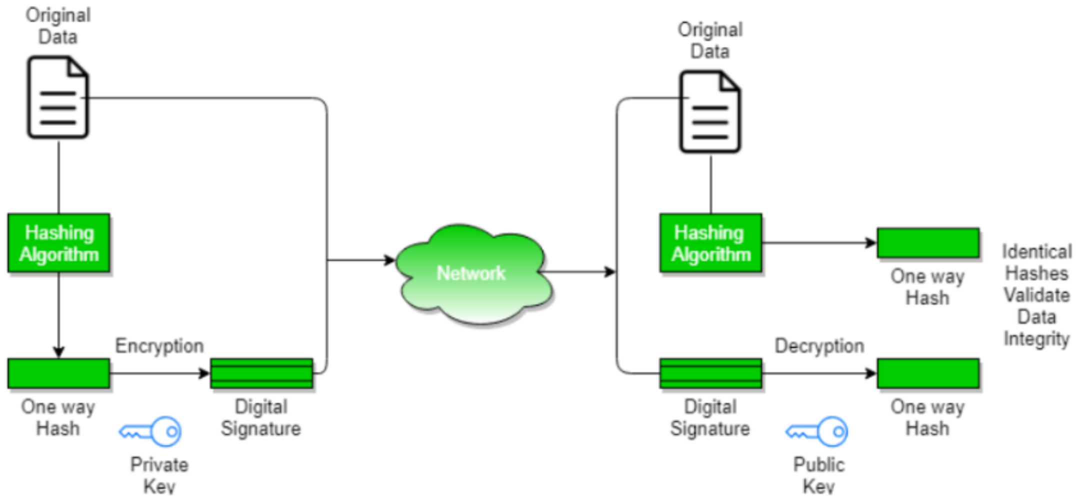
⑥ Bob Calculates y^2 and xv^c. If those two values are Congruent, then Alice either knows the value of s or she has calculated the value of y in some other ways (dishonest), because we can easily prove that y^2 is the Same as xv^c in modulo n arithmatic.

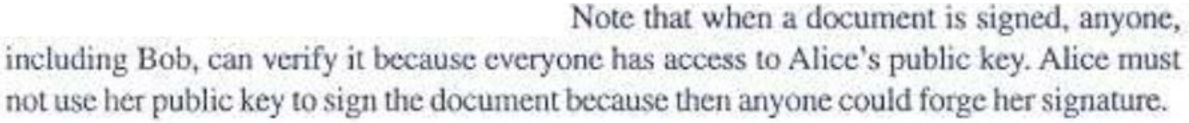
- **What do you mean by digital signature?**

  A digital signature is a mathematical technique used to validate the authenticity and integrity of a digital document, message or software. Digital signatures are the public-key primitives of message authentication.



In a digital signature, the signer uses her private key, applied to a signing algorithm, to sign the document. The verifier, on the other hand, uses the public key of the signer, applied to the verifying algorithm, to verify the document.





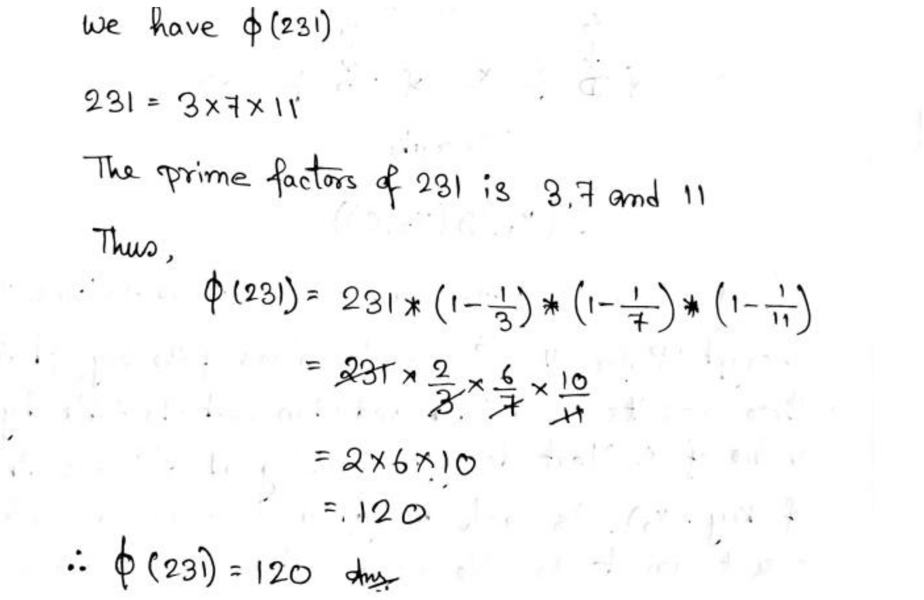
Note that when a document is signed, anyone, including Bob, can verify it because everyone has access to Alice's public key. Alice must not use her public key to sign the document because then anyone could forge her signature.

- **What is euler totient function? Compute the value of Φ(231).**

  Euler's totient function is the mathematical multiplicative function that counts the positive integers up to the given integer, generally called 'n,' which is a prime number (co-prime) to 'n.' One may use the function to know the number of prime numbers that exist up to the given integer 'n.'

  $$\varphi(n) = \mid \{a \in N \mid 0 \leq a < n : gcd(a,n) = 1\} \mid$$

  The value of Φ(231) can be calculated as,



we have $\phi(231)$

$231 = 3 \times 7 \times 11$

The prime factors of 231 is 3,7 and 11

Thus,

$$\phi(231) = 231 * (1-\frac{1}{3}) * (1-\frac{1}{7}) * (1-\frac{1}{11})$$

$$= \cancel{231} \times \frac{2}{\cancel{3}} \times \frac{6}{\cancel{7}} \times \frac{10}{\cancel{11}}$$

$$= 2 \times 6 \times 10$$

$$= 120$$

$\therefore \phi(231) = 120$ Ans.

- **State the difference between http and https protocols?**

  The difference between http and https protocols are given as follows,

Http	Https
The HTTP transmits the data over port number 80.	The HTTPS transmits the data over port number 443.
It is unsecured as the plain text is sent, which can be accessible by the hackers.	It is secure as it sends the encrypted data which hackers cannot understand.
It does not use SSL.	It uses SSL that provides the encryption of the data.
It is an application layer protocol.	It is a transport layer protocol.
It is mainly used for those websites that provide information like blog writing.	It is a secure protocol, so it is used for those websites that require to transmit the bank account details or credit card numbers.
The full form of HTTP is the Hypertext Transfer Protocol.	The full form of HTTPS is Hypertext Transfer Protocol Secure.

- **Prove that the difficulty of an alternative collision attack is proportional to $2^{\frac{n}{2}}$?**

  To find the probability of an alternative collision attack we use the fourth birthday problem.

  The 4th birthday Problem is:

We have two classes, each with K students. What is the minimum value of K so that it is likely that atleast one student from the first classroom has the Same birthday as a student from the second classroom.

The probability of success in fourth birthday problem is, $P = 1 - e^{-k^2/N}$

If EVE needs to be atleast 50% successful, then the size of 'k' is,

We know the value of 'k' by the fourth birthday problem,

$$K = \{\ln[1/(1-P)]\}^{1/2} \times N^{1/2}$$

$$K = 0.83 \times N^{1/2}$$

$$\text{or } K = 0.83 \times 2^{n/2}$$

In other word for Eve to be successful more than 50% of times, she needs to create a list of digests that is proportional to $2^{n/2}$

Note: The difficulty of an alternative collision attack is proportional to 2^n