Topic..... Date.....

NAME - MOHAMMED SAAD

ROLL NO - 19BCS071

SUBJECT - NETWORK SECURITY

CODE - CEN-805

Teacher's Sign .....

Topic..... Date.....

Q1. Explain the following with respect to MD5:

i. If the size of the message is 1000 bits, what will be the size of padding bits?

Ans We need to add padding bits to make the length a multiple of 512 bits

$$(|M| + |P| + 64) = 0 \bmod 512$$

$$|P| = (-|M| - 64) \bmod 512$$

$$|P| = (-1000 - 64) \bmod 512 = -1064 \bmod 512$$
$$= 472$$

ii) Function to generate temporary constant

$$K_i = \text{abs}(\sin(1+1)) \times 2^{32}$$

$i \in [1, 64]$

1 to 16 are used in round 1 and successive rounds use successive 16 values

Teacher's Sign .....

Topic..... Date.....

ii) Values of Chaing variables

Since MD5 has 128 bit hash value 4 32 bits variables are initialised

A = 0x01234567 B = 0x89abcdef
C = 0xfedca98 D = 0x76543210

These are called chaing variables

iv) Compression Function

A 128 bit buffer (4 registers, 32 bit each) is used to hold the intermidiate and final result of hash function.

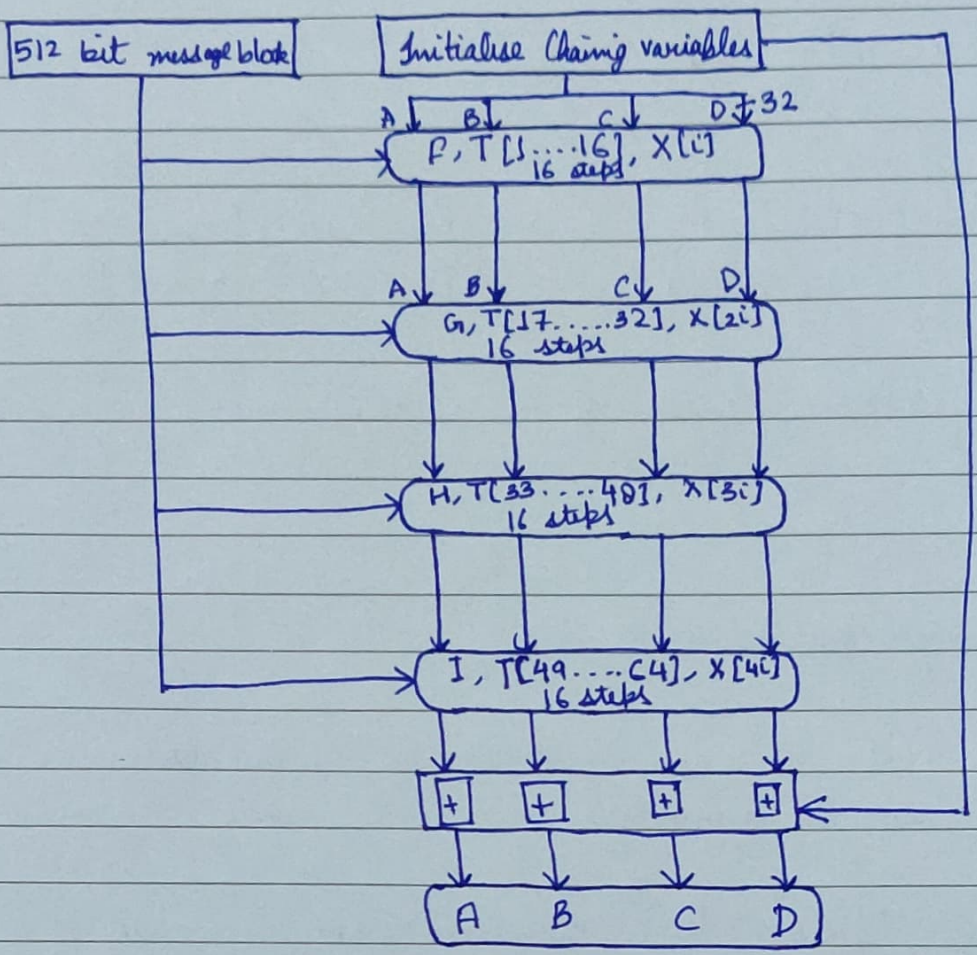
We define four auxillary functions that each take as input three-32-bit words and produce as output one 32-bit word.

F(X,Y,Z) = XY V not(X)Z
G(X,Y,Z) = XZ V Y not(Z)
H(X,Y,Z) = X xor Y xor Z
I(XY,Z) = Y xor (XV not(Z))

In each bit position F acts as a conditional: If X then Y else Z. Function F could use + instead of V since XY and not(X) Z will never have 1's in the same bit position.
Function G, H&I are bitwise parallel to the function F.

Teacher's Sign .....

Topic.....Date.....



compression function

Teacher's Sign .....

Topic..... Date.....

Q2 For what purpose the Message digest is used? Explain the process of padding and chaining variables used in SHA-I.

A message digest is a fixed size numeric representation of the contents of a message, computed by a hash function. It can be performed as a digital signature. Message digest guarantee the integrity of the message. It is used to ensure the integrity of a message transmitted over an insecure channel.

Padding in SHA-1

SHA-1 is used to compute a message digest for a message or data file that is provided a input. The purpose of message padding is to make the total length of a padded message a multiple of 512. The following specifies how padding shall be performed. A "1" followed by m "0"s followed by a 64-bit integer are appended to the end of the message to produce a padded message of length $512 * n$.

Chaining variables in SHA-1

A = 67452301
B = EFCDAB89
C = 98BADCFE
D = 10325476
E = C3D2E1F0

Teacher's Sign .....

Topic..... Date.....

Q3. For SHA-512.

i. Show the equation for the values of W_{60} and W_{64}.

$$W_{60} = W_{44} \oplus \text{RotShift}_{1\text{-}8\text{-}7}(W_{45}) \oplus W_{53} \oplus \text{RotShift}_{19\text{-}61\text{-}6}(W_{59})$$

$$W_{64} = W_{53} \oplus \text{RotShift}_{1\text{-}8\text{-}7}(W_{54}) \oplus W_{62} \oplus \text{RotShift}_{19\text{-}61\text{-}6}(W_{67})$$

(ii) Find the value of the padding field and the value of the length field if the length of the message is 2000 bits long.

$$|P| = (-|M| - 128) \bmod 1024$$

$$|P| = -2128 \bmod 1024$$

$$= 944 \text{ bits}$$

Length field is of 128 bits

$$(2000)_{10} = (700)_{16}$$

0000 0000 0000 0000 0700 0000 0000 0700

Teacher's Sign .....

Topic..... Date.....

Q4.

$|P| = (-24 \text{ mod } 1024)\ (-24 - 128) \bmod 1024$

$|P| = 872$

01100001 01100010 01100011
61 62 63

Total message = $|P| + |M| + 128$

$W_1 = 61\ 62\ 63\ 80\ 00\ 00\ 00\ 00$
$W_2 = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_3 = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_4 = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_5 = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_6 = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_7 = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_8 = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_9 = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_{10} = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_{11} = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_{12} = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_{13} = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_{14} = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_{15} = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_{16} = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 18$

Teacher's Sign .....

Topic.....Date.....

Q5. Explain about the functioning of one iteration and compression function used in SHA-512.

SHA-512 creates a digest of 512 bits from a multiple block message. Each block is 1024 bits in length.

Message preparation-
SHA-512 insists that the length of the original message be less than 2^{128} bits.

Length field and Padding
SHA-512 requires the addition of a 128 bit unsigned integer length field to the message that defines the length of the message in bit.

Word Expansion.
A block is made of 1024 bits or sixteen 64 bit words. Before processing each message block must be expanded! The 1024 bit block becomes the first 16 words, the rest of words come from already made words

Message Digest Initialization
The algorithm uses 8 constants for message digest initialization. They are called A0 to H0 to math with the word naming used for the digest.

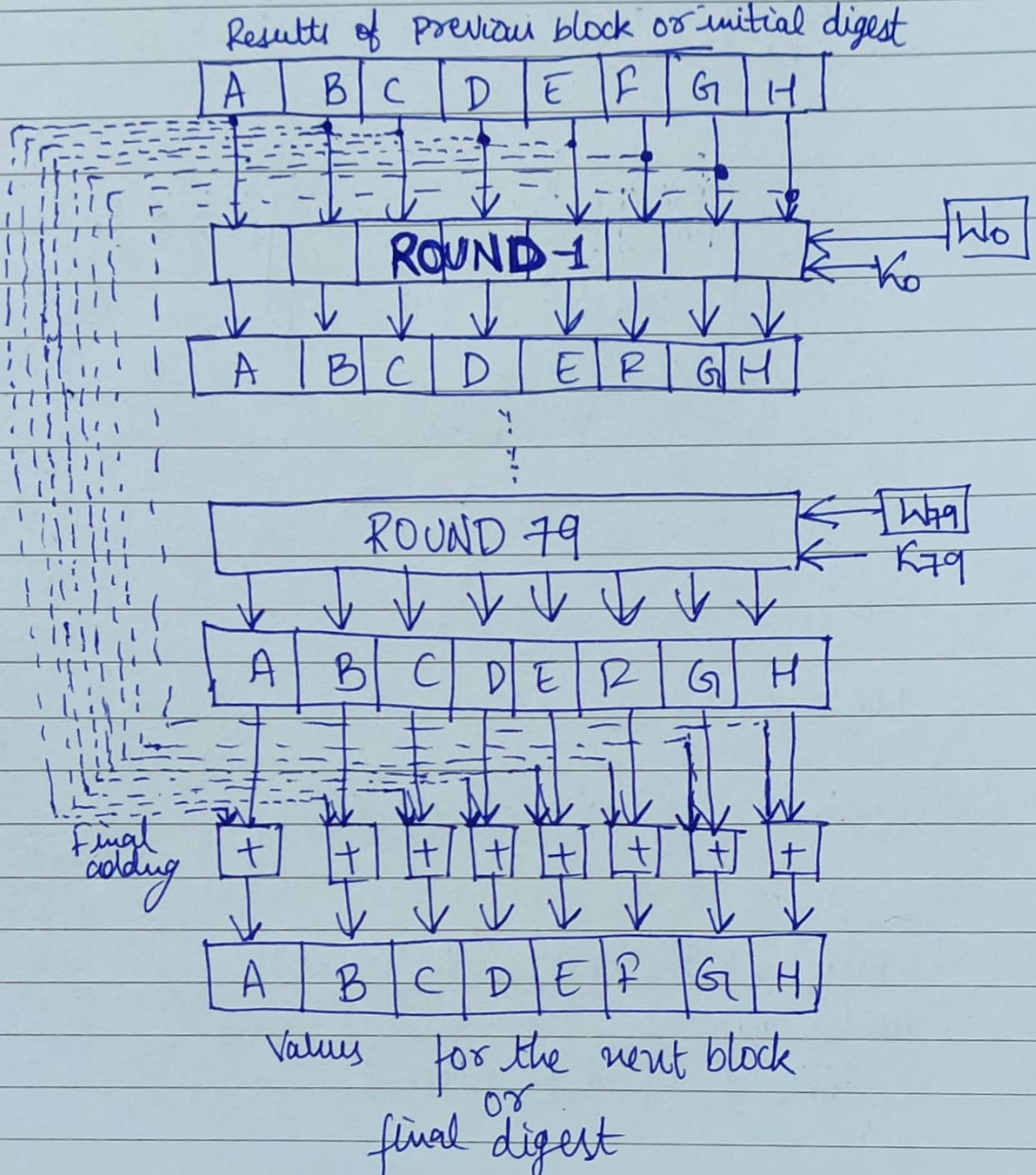
Teacher's Sign .....

Topic..... Date.....

Compression function

A message digest from a multiple block message where each block is 1024 bits. processing of each block requires 80 rounds.

At the beginning of processing the values of the eight buffers are saved into eight temporary variables. At the end of processing these values are added to the values ~~and~~ created from step 79.



Teacher's Sign .....

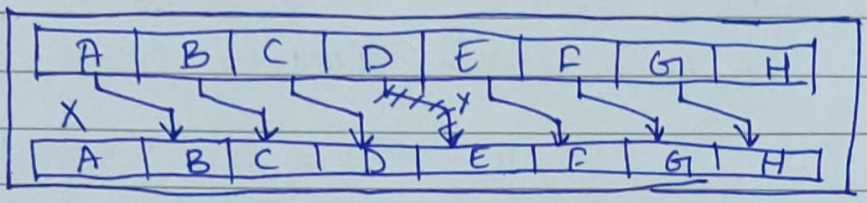
Topic..... Date.....

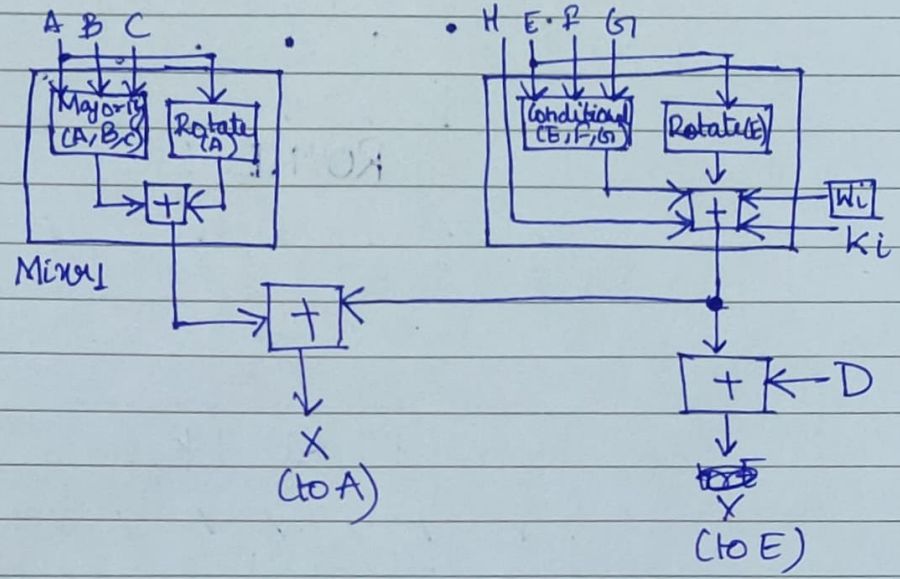
Structure of each Round

In each round eight new values for the 64 bit buffers are created from the values of previous round.

A → B B → C C → D D → E E → F

F → G G → H





Majority (x, y, z)

$(x \text{ AND } y) \oplus (y \text{ AND } z) \oplus (z \text{ AND } x)$

Rotate(x)

$RotR_{28}(x) \oplus RotR_{34}(x) \oplus RotR_{39}(x)$

conditional

$x \text{ AND } y \oplus (\text{NOT } x \text{ AND } z)$

$\boxplus$ addition modulo 2^{64}

RotRi(x) Right rotation of the argument x by i bits.

Teacher's Sign.....

Topic..... Date.....

Q6. If the ASCII Character "COMPUTERENGINEERING" is passed as a message to the SHA-512 as input, find the values in HEX assigned to the words $W_0, W_1, W_2 \ldots W_{15}$ for the defined message

C - 01000011 O - 01001111 M - 01001101
P - 01010000 U - 01010101 T - 01010100
E - 01000101 R - 0101 0010
E - 01000101 N - 01001110 G - 01000111
I - 01001001 N - 01001110 E - 01000101
E - 01000101 R - 0101 0010 I - 01001001
N - 01001110 G - 01000111

C - 43 O - 4F M - 4D P - 50 U - 55 T - 54 E - 45 R - 52
E - 45 N - 4E G - 47 I - 49 N - 4E E - 45 E - 45 R - 52
I - 49 N - 4E G - 47

$|M| = 152$ bits

Padding $= (-|M| - 128) \bmod 1024 = -152 - 128 \bmod 1024$
$= 744$ bits

$W_1 = 43\ 4F\ 4D\ 50\ 55\ 54\ 45\ 52$ $W_2 = 45\ 4E\ 47\ 49\ 4E\ 45\ 45\ 52$
$W_3 = 49\ 4E\ 47\ 80\ 00\ 00\ 00\ 00$ $W_4 = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_5 = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$ $W_6 = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_7 = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$ $W_8 = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_9 = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$ $W_{10} = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_{11} = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$ $W_{12} = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_{13} = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$ $W_{14} = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$W_{15} = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$ $W_{16} = 00\ 00\ 00\ 00\ 00\ 00\ 00\ 98$

Teacher's Sign .....

Topic..... Date.....

Q7 Using the El Gamal Digital signature scheme, let $p = 881$ and $d = 700$. Find the values for e1 and e2. Choose $r = 17$. Find the value of signature S1 and S2 if the message $M = 400$.

Sol We have $p = 881$ $d = 700$

$e_1 = 3$ $e_2 = 3^{700} \bmod 881 = 471$.

$S_1 = e_1^r \bmod p = 3^{17} \bmod 881 = 540$

$S_2 = (M - d \times S_1) r^{-1} \bmod (p-1) = (400 - 700 \times 540) 17^{-1} \bmod 88$

$= 720$

We can verify the signature because V_1 is congruent to V_2

$V_1 = e_1^M \bmod p = 3^{400} \bmod 881 = 186$

$V_2 = e_2^{S_1} \times S_2^{S_2} \bmod p = 471^{540} \times 540^{720} \bmod 881 = 186$

Q8. Alice chooses $q = 101$ and $p = 8081$. Alice selects $e_0 = 3$ and calculates $e1 = e_0^{(p-1)/q} \bmod p = 6968$. Alice chooses $d = 61$ as the private key and calculates $e_2 = e_1^d \bmod p = 2038$. Now Alice can send a message to Bob. Assume that hash of the message $h(M) = 5000$ and Alice chooses $r = 61$.

(i) Generate signature

$h(M) = 5000$ $r = 61$

$S_1 = (e_1^r \bmod p) \bmod q = 54$

$S_2 = ((h(M) + dS_1) r^{-1}) \bmod q = 40$

(ii) Verify signature

Alice sends M, S_1, and S_2 to Bob. Bob uses public key to calculate V.

$S_2^{-1} = 48 \bmod 101$

$V = [(6968^{5000 \times 48} \times 2038^{54 \times 48}) \bmod 8081] \bmod 101 = 54$

Because S_1 and V are congruent, Bob accepts the message.

Teacher's Sign .....

Topic..... Date.....

Q9. Using the RSA scheme, let $p = 809$, $q = 751$, and $d = 23$. Calculate the public key e. Then

(i) Sign and verify a message with $M_1 = 100$. Call the signature S_1.

We have $n = 809 \times 751 = 607559$

$\phi(n) = (809-1) \times (751-1) = 606000$

Since $d = 23$

We have $e = d^{-1} \bmod \phi(n) = 158087$

$S_1 = M_1^d \bmod n = 100^{23} \bmod 607559 = 223388$

$M_1 = S_1^e \bmod n = 223388^{158087} \bmod 607559 = 100$

(ii) Sign a verify a message with $M_2 = 50$. Call the signature S_2.

We have

$S_2 = M_2^d \bmod n = 50^{23} \bmod 607559 = 5627$

$M_2 = S_2^e \bmod n = 5627^{158087} \bmod 607559 = 50$

(iii) Show that if $M = M_1 \times M_2 = 5000$, then $S = S_1 \times S_2$

If $M = M_1 \times M_2 = 5000$, we have

$S = M^d \bmod n = 5000^{23} \bmod 607559 = 572264$

$S = (S_1 \times S_2) \bmod n = (223388 \times 5627) \bmod 607559 = 572264$

Teacher's Sign .....

Topic..... Date.....

Q10. Using the RSA digital signature scheme, let $p = 809$, $q = 751$ and $d = 23$. Calculate the set of public key and private key and then sign and verify a message with $M = 50$.

Sol Public key $e = d^{-1} \bmod \phi(n)$

$n = 809 \times 751 = 607559$ $\quad \phi(n) = (809-1)(751-1) = 606000$

$e = 23^{-1} \bmod 606000 = 158087$

$S = M^d \bmod n = 50^{23} \bmod 607559 = 5627$

$M = S^e \bmod n = 5627^{158087} \bmod 607559 = 50$

Q11. What is digital signature? Explain the mechanism of generation of digital signature using Schnorr digital signature technique.

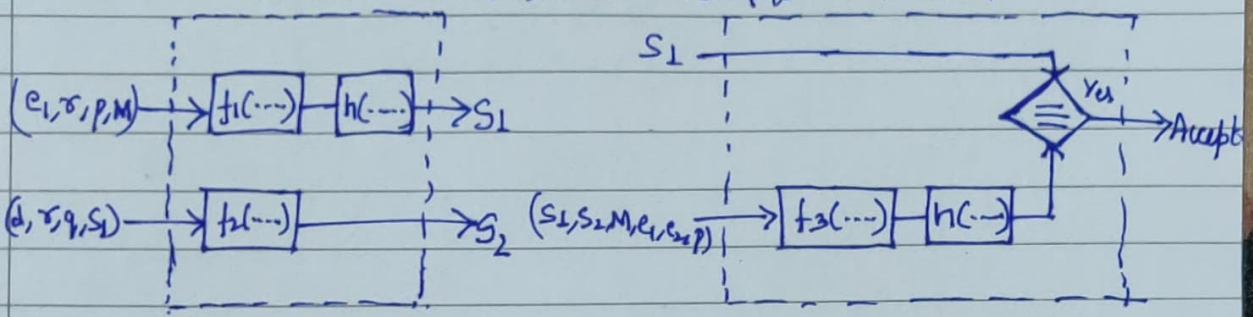
A digital signature is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature. The sender uses a process that involves showing that she owns a private key related to the public key that she has announced publicly. The receiver uses the sender's public key to prove that the message is indeed signed by the sender who claims to have sent the message.

Teacher's Sign .....

Topic..... Date.....

S_1, S_2: Signatures (d): Alice's private key
M: Message r: Random secret
(e_1, e_2, p, q): Alice's public key

General idea behind the Schnorr digital signature scheme



In the signing process, two functions create two signatures; in the verifying process, the output of one function is compared to the first signature for verification.

Key Generation

Before signing a message, Alice needs to generate keys and announce the public ones to the public.

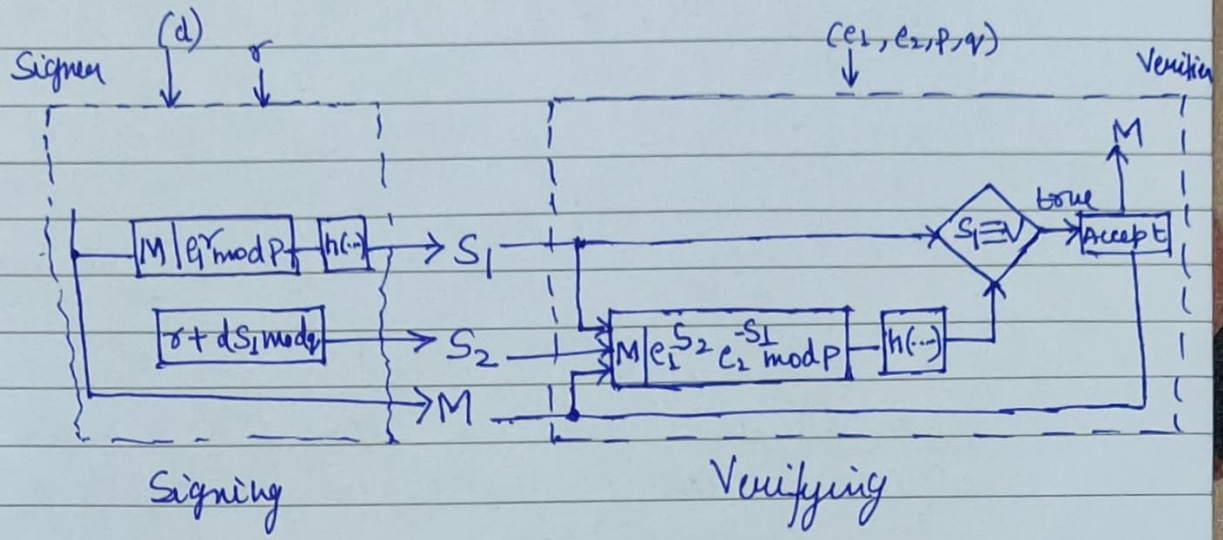
1. ~~Alice~~ selects a prime p, which is usually 1024 bits in length.
2. Select another prime q, the prime q needs to divide (p-1). In other words, $p-1 = 0 \bmod q$.
3. Choose e_1 to be the q^{th} root of 1 modulo p. To do so, choose a primitive element in Z_p, e_0 and calculate $e_1 = e_0^{(p-1)/q} \bmod p$.
4. Choose an integer d, as her private key.
5. Calculate $e_2 = e_1^d \bmod p$.
6. Public key is (e_1, e_2, p, q) private key is d.

Teacher's Sign .....

Topic..... Date.....

Signing and Verifying

M: Message — r: Random secret — | : Concatenation
S_1, S_2: Signatures — (d): private key — $h(\ldots)$: Hash algorithm
V: Verification — (e_1, e_2, P, q): Public key



Signing

1. Choose a random integer r. r needs to be changed each time a new message is being sent.
2. Calculate the first signature $S_1 = h(M | e_1^r \bmod p)$.
3. Calculate the second signature $S_2 = r + d \times S_1 \bmod q$.
4. Send M, S_1 and S_2.

Verifying Message

The receiver, receives M, S_1 and S_2.

1. Calculate $V = h(M | e_1^{S_2} e_2^{-S_1} \bmod p)$
2. If S_1 is congruent to V modulo p, message is accepted, otherwise, rejected.

Teacher's Sign .....

Topic..... Date.....

Q12. What is Blind Digital signature? Explain the blind digital signature detection generation and verification process using RSA.

A digital signature in which a document is required to be signed without revealing the contents of the document to the signer, is called a blind digital signature.
The main idea is as follows.

a. Create a message and blind it. Send the blinded message.
b. The blinded message is signed and returns the signature on blinded message.
c. Unblind the signature to obtain a signature on the original message.

Blind signature based on RSA scheme
Let us briefly describe a blind digital signature scheme. Blinding can be done using a variation of the RSA scheme. Select a random number, b, and calculate the blinded message $B = M \times b^e \bmod n$, in which e is Alice's public key and n is the modulus defined in the RSA digital signature scheme. The blinded message is then sent.
The blinded message is then signed using the signing algorithm defined in the RSA digital signatures $S_b = B^d \bmod n$, in which d is private key. S_b is the signature on the blind version of the message.
The multiplicative inverse of his random number b is used to remove the blind from the signature.

Teacher's Sign .....

Topic..... Date.....

The signature is $S = S_b b^{-1} \bmod n$.
It can be proved that S is the signature on the original message as defined in RSA digital signature scheme.

$$S \equiv S_b b^{-1} \equiv B^d b^{-1} \equiv (M \times b^e)^d b^{-1} \equiv M^d b^{ed} b^{-1} \equiv M^d b b^{-1} \equiv M^d$$

S is the signature