## * Digital Signature:

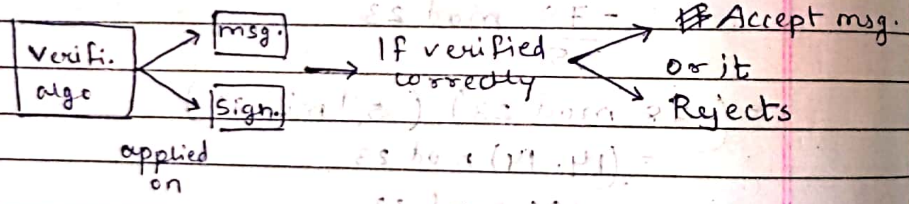
### (1) Inclusion:

→ Conventional signature is included in the document, it is a part of the document wherein digital signature there are two separate documents, a message and a sign.

→ The recipient recieves both documents and verifies that signature belongs to the supposed sender.

### (2) Verification method:

→ Sign. on the document is verified with the sign. stored on the file.



→ Don't have copy of signature, hence we apply verification algorithm.

### (3) Relationship:

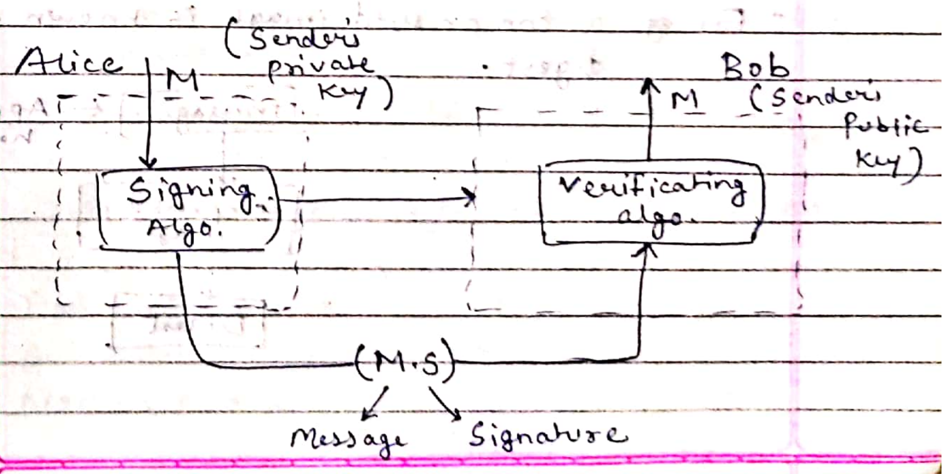
| One to Many (conventional) | One to One (Digital) |
|---|---|
| → One sign. will be okay for many documents. | → One sign. will be ~~okay~~ for only one document. |

### (4) Duplicity:

→ A copy of sign document can be distinguish from the signature on original document

→ In digital, there is no such stored reference unless there is a factor of time (Timestamp)

• Digital Signature : Process:



→ The message and signature are sent to the reciever, the reciever recieves ~~the~~ signature and message and applies verification algorithm on message & signature both.

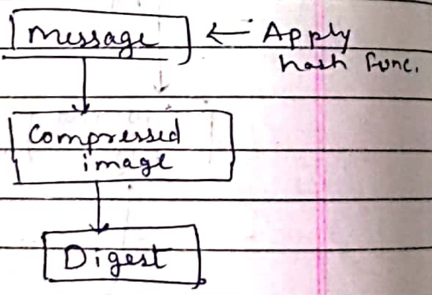
→ If verified correctly, bob will accept the message else will reject the message.

→ Here, user uses private key to sign the document on the other hand, reciever will use sender's public key for verification.

- Signing the Digest:

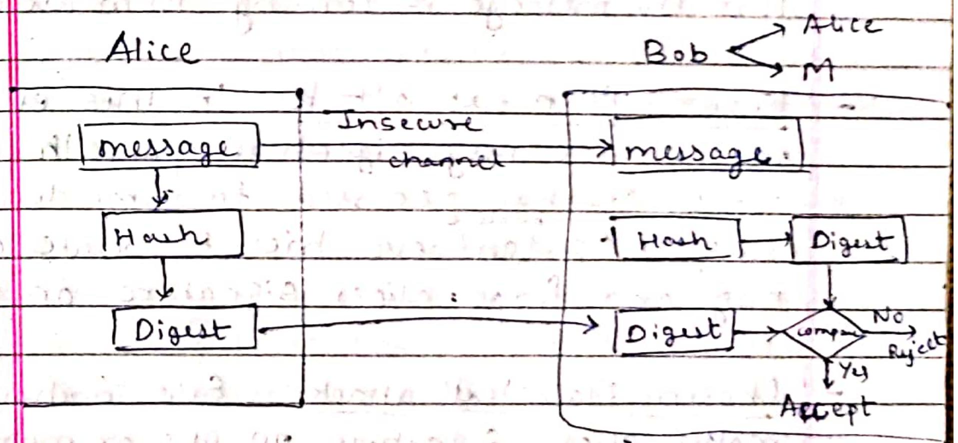
→ Hash functions
-It is an one way function.

→ Digest
- For eg: a compressed image is known as digest.



- Hash function - A mathematical function that converts an input value into a compressed numerical value which is known as a hash or hash value.

- Message digest - It is used to ensure the integrity of the message transmitted over an insecured channel, message is passed through the hash function. Function creates compressed image of image called as digest.



- Services provided by Digital signature :

→ Data integrity
→ Authentication of sender
→ Non-repudiation

- Attacks on digital signature:

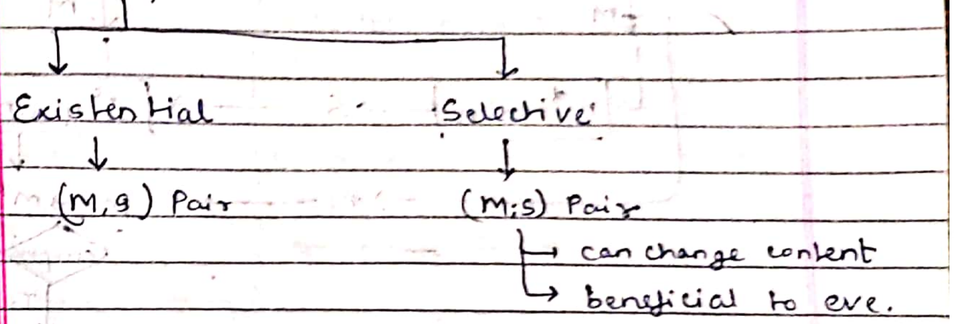
- Key only attack
- Chosen Plain text attack
- ~~Chosen~~ Known Plain text attack.

- Key only attack: Eve (→ attacker.) has access only to the public information release by alice. To forge the message eve needs to create alice's signature in order to convince bob that the message is coming Bom alice.

- Known Plain text attack: In this eve has one or more msg. signature pair. In other words, she has accessed to some documents previously signed by alice and eve tries to create another msg. and forge alice's signature on it.

- Chosen Plain text attack: Eve somehow makes alice's signature on one or more message, eve now has chosen message signature pair. Eve can create another msg. with the content he wants

- Forgery → If attack is successful



- RSA – Digital signature Scheme:

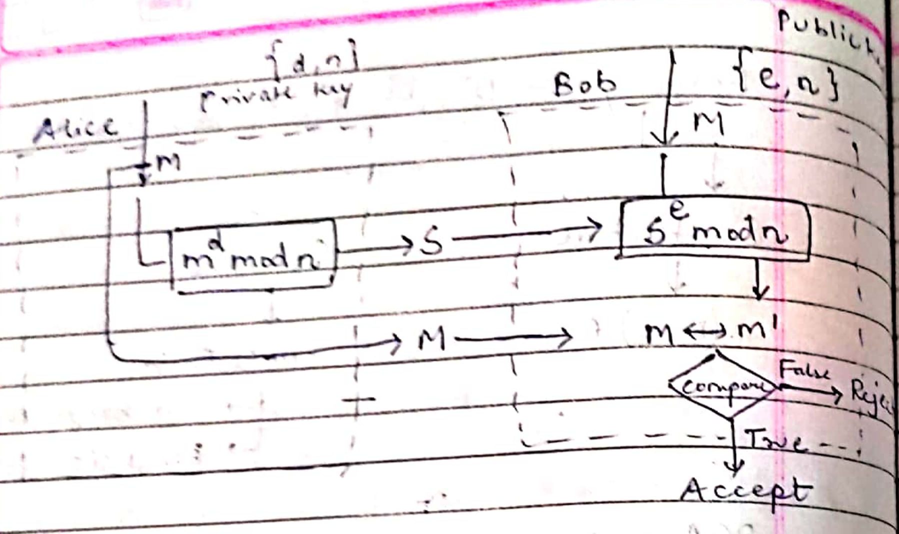
→ RSA algorithm can be used to sign and verify a msg., in this case it is called RSA digital signature scheme.

→ The digital signature scheme changes the roles of public and private key.

→ Private and public key of sender is used in which sender's private key is used to sign the msg. and sender's public key is used to verify the message.

→ Key generation is same as RSA encrypt... decrypt

e → public key of sender
d → private key of recieve



Alice has public RSA model, the values are as following, modulus n = 91, e = 5, & message = 7

(i) what is sign document ?.

(ii) Show bob's calculation that verifies that document is valid.

$$ed \equiv 1 \bmod n$$

$$5 \times d \equiv 1 \bmod 91$$

$$\therefore d = 18$$

$$m^d \bmod n$$

Now, $7^{18} \bmod 91$

$$\therefore 7^1 \bmod 91 = 7$$

$$\therefore 7^2 \bmod 91 = (7^1 \bmod 91 \times 7^1 \bmod 91) \bmod 91$$

$$= 49 \bmod 91$$

$$= 49$$

$$7^4 \bmod 91 = (49 \times 49) \bmod 91$$

$$= 2401 \bmod 91$$

$$= 35$$

$$7^8 \bmod 91 = (35 \times 35) \bmod 91$$

$$= 1225 \bmod 91$$

$$= \cancel{25}\ 42$$

$$7^{16} \bmod 91 = (\overset{42}{\cancel{25}} \times \overset{42}{\cancel{25}}) \bmod 91$$

$$= \overset{1764}{\cancel{625}} \bmod 91$$

$$= 82\ 35$$

$$\therefore 7^{18} \bmod 91 = (82 \times 49) \bmod 91$$

$$= 4018 \bmod 91$$

$$= 14$$

$$ed \equiv 1 \bmod \phi(n)$$

Here, $n = 91$

$$\therefore n = p \times q = 13 \times 7$$

$$\therefore p = 13,\ q = 7$$

$$\therefore \phi(n) = 12 \times 6$$

$$= 72$$

$\therefore ed \equiv 1 \bmod \phi(n)$

$\therefore 5 \times d \equiv 1 \bmod 72$

$\therefore d = 29$

Now, $S = M^d \bmod n$

$= 7^{29} \bmod n$

$= 7^{29} \bmod 91$

$\therefore 7^{29} \bmod 91 = (\overset{35}{\cancel{82}} \times \overset{42}{\cancel{25}} \times 35 \times 7) \bmod 91$

360150

$= \cancel{71,750} \bmod 91$

$S = \cancel{42}\ \boxed{63}$

Now, verification,

$V = S^e \bmod N$

$= 63^5 \bmod 91$

$63^1 \bmod 91 = 63$

$63^2 \bmod 91 = (63 \times 63) \bmod 91$

$= 3969 \bmod 91$

$= 56$

$63^4 \bmod 91 = (56 \times 56) \bmod 91$

$= 3136 \bmod 91$

$= 42$

$\therefore 63^5 \bmod 91 = (42 \times 63) \bmod 91$

$= 2646 \bmod 91$

$= \boxed{7}$

- <u>Elgamal Digital Scheme</u>:

→ It is the varient of digital signature algorithm.

→ The scheme is based on computing assumption of large elient ~~m~~numbers. Computationally it is very difficult to find $S_1$ and $S_2$.

Prime no. $q \longrightarrow \alpha$ (Primitive root of $q$)

Step 1: Key generation:

(i) Generate a random integer such that $X_A$ is $1 < X_A < (q-1)$

(ii) $Y_A = \alpha^{X_A} \bmod q$

(iii) A's private key $= X_A$

A's public key $= \{q, \alpha, Y_A\}$

Eg: $q = 19$, $\alpha = 10$

$\therefore 1 < X_A < (19-1)$

$\therefore 1 < X_A < 18$

Lets take $X_A$ as 16.

$\therefore Y_A = \alpha^{X_A} \bmod q$

$= 10^{16} \bmod 19$

$= (10^8 \bmod 19)(10^8 \bmod 19) \bmod 19$

$= (17 \times 17) \bmod 19$

$= 4$

$\therefore$ A's private key $= X_A = 16$

A's public key $= \{q, \alpha, Y_A\} = \{19, 10, 4\}$

Step 2 : Creating the digital signature.

(i) Choose random integer K such that

$1 \le K \le (q-1)$

and g.c.d. $(K, (q-1)) = 1$

$\therefore S_1 = \alpha^K \bmod q$

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

Eg: $K = 5$, $m = 14$

$\therefore S_1 = \alpha^K \bmod q$

$= 10^5 \bmod 19$

$S_1 = 3$

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

$= 5^{-1}(14 - 16(3)) \bmod 18$

$= 11(14 - 48) \bmod 18$

$= 18 - (374 \bmod 18)$

$\therefore S_2 = 4$

Verification

Eg: Calculate $V_1 = \alpha^m \bmod q$

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

$m = 14$

$\therefore V_1 = 10^{14} \bmod 19$

$= \underline{\underline{16}}$

$V_2 = 4^3 \cdot 3^4 \bmod 19$

$= \underline{\underline{16}}$