→ Digital signature:-

Message authentication protects two parties who exchange the message from an third party. however it doesn't protect each other to solve the dispute between them. the digital signature requirments are:-

1- it must be a bit pattern that depend on the message being signed.
2- the signature must use some unique information to the sender to prevent bothe forgery & denial.

* various types of digital signature

1- Direct digital signature:-

→ in this method the sender attaches the signature with the msg. the receiver can verify the

digital signature for authentication purpose

2. arbitrated digital signature.

the problem with direct D.S can be solved with the help of the third party known as arbitrator.

there are 3 techniques in generation arbitrated signature

1- conventional cryptography, arbitar can see the msg.

X → A : M || EKxA [IDx || H(M)]

A → Y : EKAY [IDx || M || EKxA[IDx || H(M)]]

X : generates the msg along with the signature, but the signature Encrypted by using shared key between X & A.

the arbiter will decrypt the signature & generates anew msg which is Encrypted by using shared key between A & Y.

→ the receiver y will accept the msg without verifying the signature because the msg has been received from trusted party. arbiter.

~~→ In this Case~~

In Case of dispute occure the arbitor will resolve the problem by using signature.

(2) Conventional cryptography arbitar doesn't see message.

$X \rightarrow A : ID_x' : E_{kxy}[M] : : E_{kxa}[ID_x' : : H(E_{xy}(M)]$.

$A \rightarrow Y : E_{kay}[ID_x' : : E_{kxy}(M) : : E_{kxA}[ID_x' : : H(E_{kxy}(M)]]$.

(3) public key encryption arbitar doesn't see the msg :-

$X \rightarrow A$; ID_X ; $E_{KR_X}[ID_X ; E_{KU_Y}[E_{KR_X}(M)]]$.

$A \rightarrow Y$; $E_{KR_A}[ID_X ; E_{KU_Y}(E_{KR_X}(M))]$?

(public key of Y)

here x will Encrypt the msg by using his private key and again Encrypt with public key of y.

thus both authentication and privacy can be acheived and along with identity Encryption with private key of x and sends the message to arbitar.

→ arbitar will decrypt the message with public key of x and checks whether message contain signature or not.

if the msg contain signature he will Encrypt the msg with his private key and send it to y. then y accept the msg base on trust.