Digital siginature

→ Digital siginature is Asymetric key cryptography.

→ It uses both Public and Private key.

→ Incase of encryption Private key is used.

→ Incase of decryption Public key is used.

→ It Provides Authentacation and also non-repodation.

→ signature means Proof of identify is it from correct sender (or) not.

→ They are two algo Digital signature Generation algo.

→ This Algo takes Private key and message and generates digital signature.

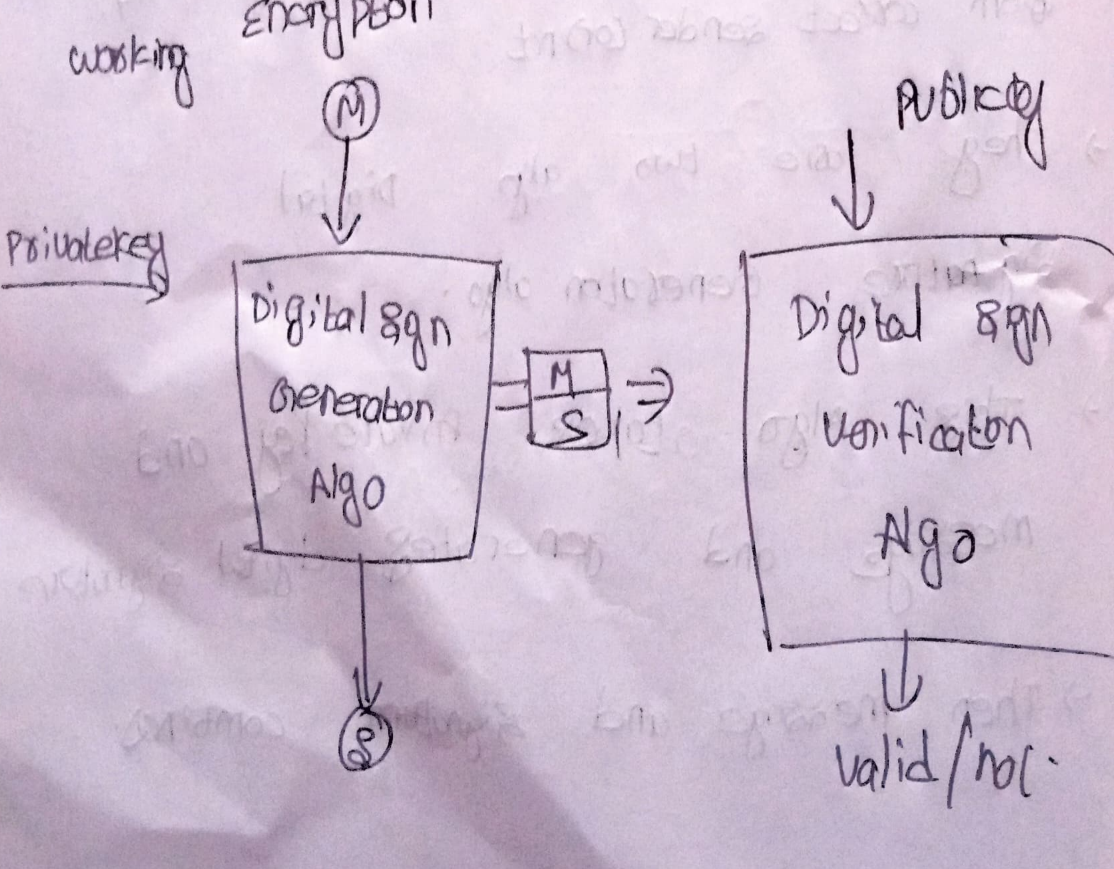
→ Then message and signature combines.

→ The combined Message and signature is sent as Input for Public key.

→ using Public key and Digital signature verification Algo.

→ It verifies produces the output whether it's valid (or) not.

working



→ If msg matches then it is vala

→ else it is not valid

Advantages of digital signatur.

① Authenaction

② non-repudation

③ Intergity

④ Digital certificate.

Applications of DS

① online transaction

② Email security

③ Document Authencation