Digital Signature scheme: RSA

I Select two large Prime Nos.
p & q

II Compute $n = p * q$

III Compute $\phi(n)$
$\therefore \phi(n) = \phi(p) * \phi(q)$
$\phi(n) = (p-1) * (q-1)$

IV Now select the public key e such that
1. $0 \leq e \leq \phi(n)$
2. $GCD(e, \phi(n)) = 1$

V Now calculate the private key d
$d \equiv e \bmod \phi(n)$
$d e^{-1} \bmod \phi(n) = 1$

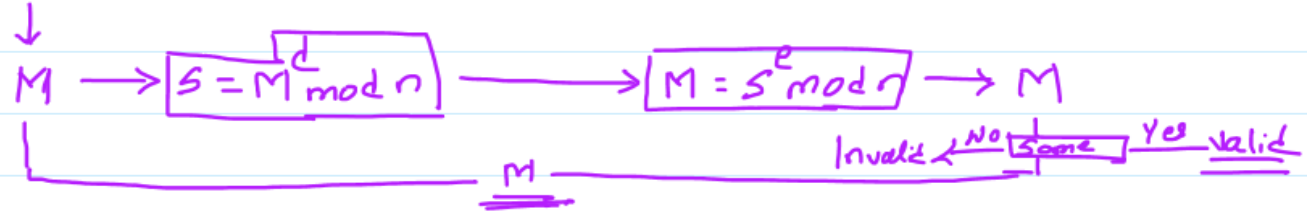
VI Public key (e, n)
Private key (d, n)

VII Create a signature
$S = M^d \bmod n$

VIII Send S & M to Receiver.

IX Perform verification at Receiver side.
$M' = S^e \bmod n$
if $(M == M')$
M & S is valid. (Keep).
else
invalid (ID card)

Block Dig:



Rx