RSA DIGITAL SIGNATURE

- **Let *A* want to send a signed intelligible message *a* to *B* via the Internet.**
- **Two semiprimes: *m=p*q* (A) and *n=r*s* (B)**
- **Let { *m*, e} and { *n*, *h* } be public keys of A and B users;**
- **Let *d* and *g* be private keys of A and B respectively.**
- ***d* and *e* are modular inverse to each other; and**
- ***g* and *h* are modular inverse to each other.**

In other words,

1. Let m = pq (p and q are primes)

2. Let $\varphi(m)$ = (p-1)(q-1)

3. Choose a small number e, coprime to $\varphi(m)$

4. Find d, such that d*e mod $\varphi(m)$ = 1

Repeat the same procedure for n =rs (r and s are primes)

Signing and Encryption

{Sender's actions}:

1. $x := a^d \bmod m$**; (private d) - sign**

2. $y := x^h \bmod n$**; (public h) - encrypt**

3. *A* sends *y* to receiver *B* via the Internet;

Decryption and Verification

{Receiver's *B* actions}:

4. $z := y^g \bmod n$ **(private g) - decrypt**

5. $u := z^e \bmod m$ **(public e) - verify**

6. If *u* is an intelligible message, then receiver accepts it

7. In addition, the receiver accepts that *u=a.*