Chapter Four

Digital Signature

Digital signature

Concept has come from handwritten signature.

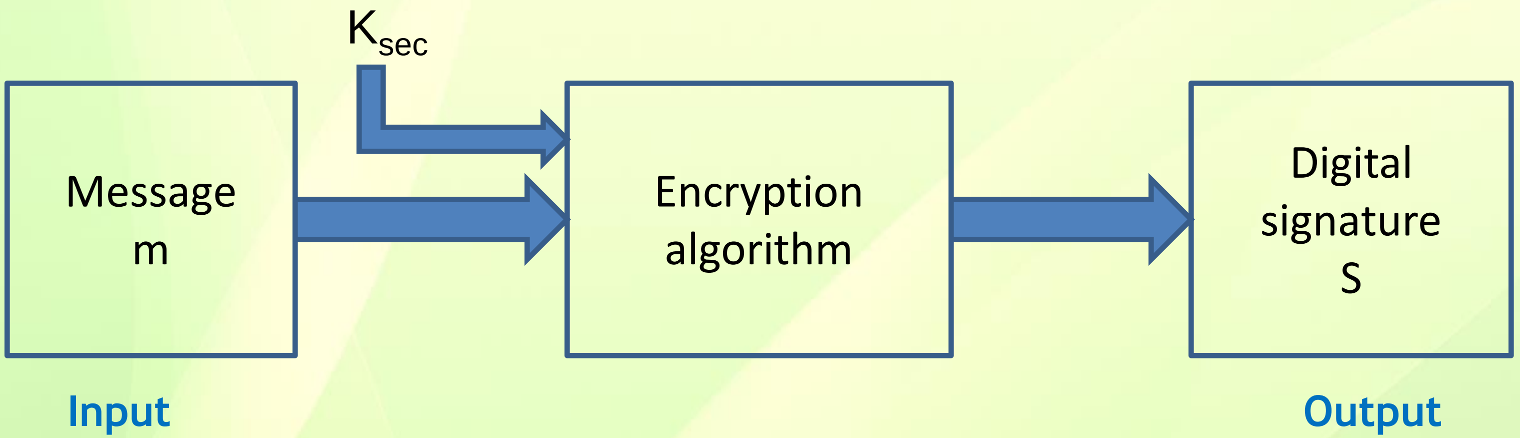
Cryptographic technique.

Public key cryptosystem is used in digital signature method.

unforgivable: means **only the originator** should be able to produce/ compute the signature value.

Verifiable: means others should be able to check that the signature has come from the **originator.**

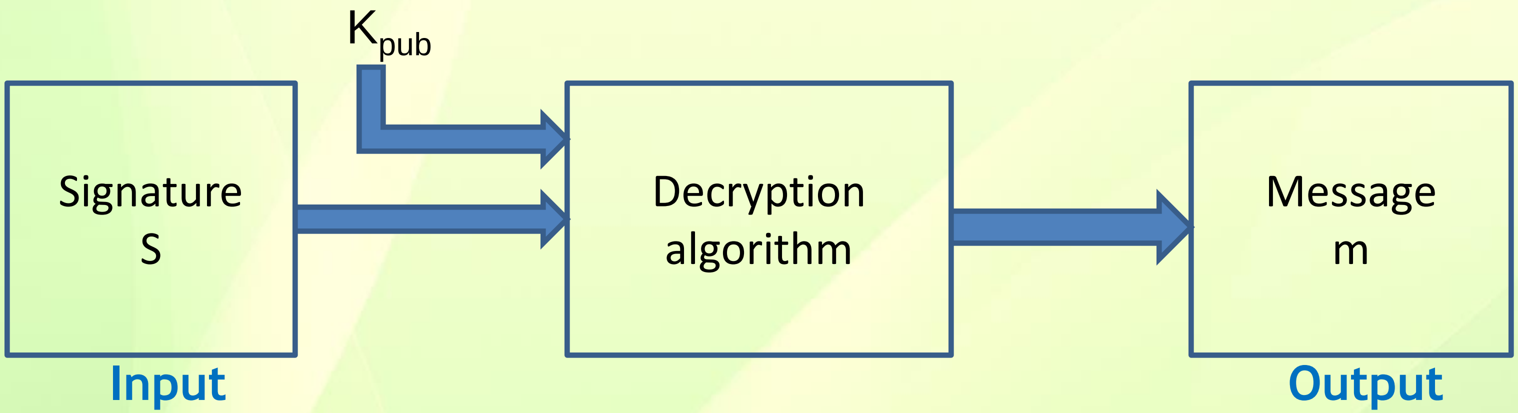
Simple digital signature



Signature creation process

Message is encrypted using private key (K_{sec}) of the creator or originator.

Signature verification



Verification process

Signature is decrypted using public key (K_{pub}) of the originator.

Signature verification

Suppose that *A* wants to send a signed message to *B*. Then,

1) *A* uses his private key $K_{sec, A}$ to produce signature and sends it to *B*.

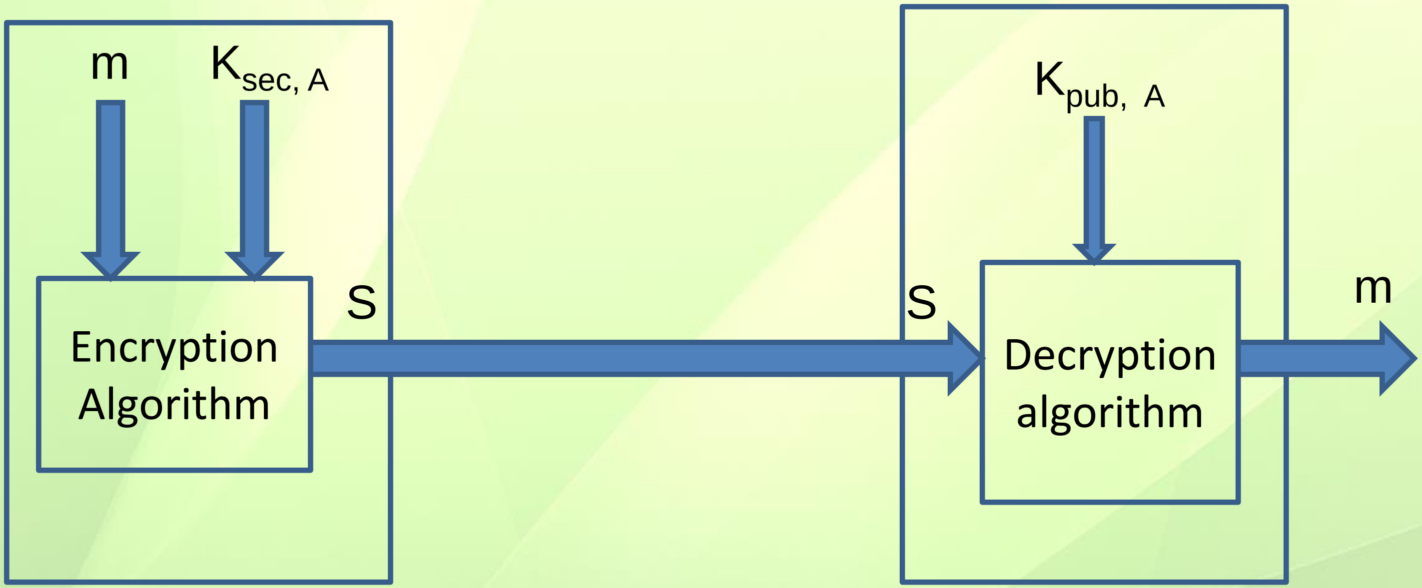
   $S = E\,(m, K_{sec, A})$.

2) After receiving the signed message *B* will verify the signature as follows:

   $D(S, K_{pub, A}) = m$.

Digital signature at a glance

For *A*:   For *B*:



Sending end:
Signature creation

Receiving end:
Signature verification

Signature verification

A sends signature to *B*, thus B verifies that:

A signed *m* (since *A*'s public key is matched).

No one else signed *m* (since only *A* must have the private or secret key).

A signed *m* and not *m'* (since *S* can be produced only from *m* not from *m')*.

Non-repudiation:

There is no way to deny that *A* has signed m. In other words *A* can not say that he does not produce *S*.

Encrypted signature

Suppose that A sends message and B receives it.

1) *A* produces signature *S* using his secret key:

$$S = E(K_{sec,\ A}, m).$$

2) Now *A* enciphers (encrypts) *S* using *B's* public key:

$$C = E(K_{pub,\ B}, S).$$

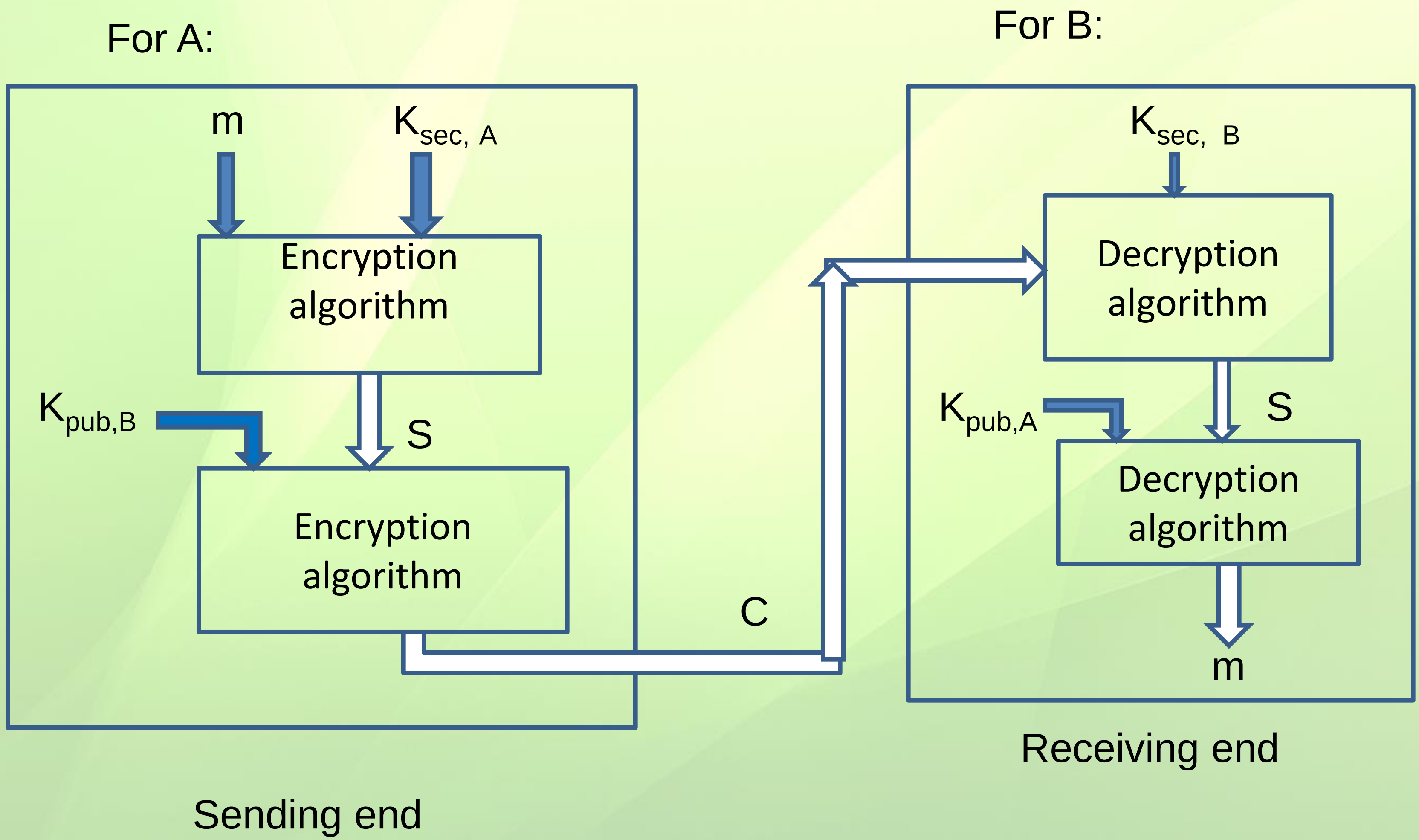
3) *B* receives *C* and deciphers it:

$$S = D(K_{sec,\ B}, C).$$

4) *B* verifies that *A* signed m:

$$m = D(K_{pub,\ A}, S).$$

Encrypted signature at a glance



Digital Signature Scheme

El Gamal Algorithm

Key generation:

1. Choose a prime p and two integers, c and x, such that $c < p$ and $x < p$.
2. Calculate $y = c^x \bmod p$.
3. Compute q that is a prime factor of (p –1), that means p should be chosen so that (p-1) has a large prime factor, q.
4. x is the private key and (p, c, y)is the public key.

El Gamal Algorithm

Signature Creation:

1. Compute a random integer k, $0 < k < p-1$, which is relatively prime to $(p-1)$ and which has not been used before. Suppose $z = p - 1$, then $gcd(k, z) = 1$

2. *Compute:*

$$i)\ t = c^k \bmod p$$

$$ii)\ s = b(m - xt) \bmod z;$$

where b is the m-inv of k and z, so

$$\boldsymbol{kb \bmod z = 1.}$$

The message signature is then (s, t).

El Gamal Algorithm

Signature verification:

A recipient receives (s, t). He uses the public key (p, c, y) and compute:

i) $v_1 = y^t.t^s \bmod p$ and

ii) $v_2 = c^m \bmod p$

If $v_1 = v_2$, the recipient can accept the signature.

Example of El Gamal Algorithm

Key Generation:

1. Let p = 17, c = 11 and x = 5 ($c < p$ and $x < p$)

2 compute:

$$y = c^x \bmod p = 11^5 \bmod 17 = 10$$

Then 5 is the private key and (17, 11, 10) is the public key.

Example [cont..]

Signature Generation: public key (p, c, y) = (17, 11, 10)

1. *Choose* $z = p\text{-}1 = 17 - 1 = 16$
2. *Choose* $k = 7$ ($k < z$) and gcd (k, z) = gcd (7, 16) = 1
3. *Compute* $t = c^k \bmod p = 11^7 \bmod 17 = 3$;
4. $kb \bmod z = 1$, $7b \bmod 16 = 1$, $b = 7$ [Extended Euclidian algorithm]
5. $s = b (m - xt) \bmod z$ *[use of private key x]*
6. suppose the message, $m = 19$
7. $s = 7 (19 - 5 \times 3) \bmod 16 = 12$

- The message signature is (s, t) = (12, 3)

Example[cont..]

Verification:

Compute:

$$v_1 = y^t . t^s \text{ mod } p = 10^3 . 3^{12} \text{ mod } 17 = 5$$

$$v_2 = c^m \text{ mod } p = 11^{19} \text{ mod } 17 = 5$$

- Since $v_1 = v_2$, the signature is verified.

15

Thank You.