

Modular multiplicative Inverse:

27-1 mod 392

392= 27(14)+14

27=14(1)+13

14=13(1)+1

1 =14+13(-1)------1

13=27+14(-1)------2

14=392+27(-14)-----------3

According (1)

1= 14+13(-1)

1=14+[27+14(-1)](-1)

1=14+27(-1)+14

1=2(14)+27(-1)

1=2[392+27(-14)]+27(-1)

1=2.392+27(-28)+27(-1)

1=2.392+27(-29)

2.392+27(-29)=1 mod 392

27(-29)=1 mod 392 ======🡺392-29=363

27(363)=1 mod 392

363=1/27 mod 392

363=27-1 mod 392

Digital signature algorithm:

1.global parameters(p,q,g)

p-prime number,64 bits b/w 512 and 1024….2l-1 <p<2l

q-prime divisor of p-1, 160

g=h(p-1)/q mod p, 1<h<p-1

user’s private key:

x random integer where 0<x<q

user’s public key

y=gx mod p

user’s per message secret number

k=random integer 0<k<q

signing algorithm:

r=(gk mod p) mod q

s=[k-1 (h(m)+xr)] mod q

signature(r,s)

verification:

w=(s’)-1 mod q

a=[h(m’)\*w] mod q

b=r’ wmod q

v=[ga yb mod p] mod q

test: v=r’

example:

p=7 , q=3, H(M)=3 h=2 k=2 X(private key)=5

p-1 mod q=0

6 mod 3=0

g=h(p-1)/q mod p

=26/3 mod 7= 4

Y=gx mod p=2

Signing algorithm:

R=[gk mod p]mod q

R=2

S=k-1[h(m)+xr] mod q

=2-1[3+(5\*2)] mod 3

=2-1[13]mod 3=====26 mod 13

s=2

signing algorithm(r,s)-----(2,2)

verification:

t=h(m)s-1 mod q]mod q

=(3\*2-1 mod 3) mod 3

=(3\*2)mod 3

=6 mod 3

t=0

U=[rs-1 mod q]mod q

=[2\*2-1 mod 3] mod 3

=2\*2 mod 3

=4 mod 3

U=1

V=[gt yu mod p] mod q

=[40 21 mod 7]mod 3

v=2

v=2 r=2

v=r

Symmetric and Asymmetric key distribution