Euclidean algorithm

$r_1 = a$; $r_2 = b$; (initialization)

while(r_2 >0)

{

$q = r_1 / r_2$

$r = r_1 - q \times r_2$;

$r_1 = r_2$; $r_2 = r$;

}

gcd(a,b)= r_1

- Eve chooses a random integer X in Z_n*.
- Eve calculates $Y=C * X^e \bmod n$.
- Eve sends Y to B for decrypton and get $Z=Y^d$ mod
- Eve can only find P

Extended Euclidean algorithm

it finds the multiplicative inverses of b in Z_n when gcd(n,b)=1

$r_1 = n$; $r_2 = b$;

$t_1=0$; $t_2=1$;

while($r_2 > 0$)

{

$q = r_1 / r_2$

$r = r_1 - q \times r_2$;

$r_1 = r_2$; $r_2 = r$;

$t = t_1 - q \times t_2$;

$t_1 = t_2$; $t_2 = t$;

}

If ($r_1 = 1$) then $b^{-1} = t_1$

Example

- Finding Multiplicative inverse of 11 in Z_{26}

The gcd(26,11)=1,which means that the multiplicative inverse of 11 exists.The EE algorithm gives $t_{1=}$-7.

The multiplicative inverse is(-7) mod 26=**19**;