El Gamal's Digital Signature

Key generation

1. Select prime *p* and a generator *g*;
2. Sender *S* selects a random integer ***r*** (secret key) such that
   $0 < r < p - 1$ and calculates

$$K=(g^r)(\text{mod} p);$$

***K*, *g* and *p* are in public domain;**

Signing

1. To authenticate message *M*, the sender selects another random integer *R* ($0 < R < p - 1$) and $\gcd(R,p\text{-}1)=1$ and computes

$$X=(g^R)(\text{mod} p);$$

2. The sender finds *Y* such that $M=rX+RY \bmod (p\text{-}1)$;

(X,Y) is the signature of *M*:

$$M=rX+RY \bmod (p\text{-}1)$$

$Y = ? \bmod (p\text{-}1)$

$RY = (M - rX) \bmod (p\text{-}1)$

$Y = (M - rX)\, R^{-1} \bmod (p\text{-}1)$

Verification

1. The receiver *B* gets (*M*, *X*, *Y*) and computes

$$A=(K^X)(X^Y)\bmod p;$$

(X,Y) is called the authenticator.

2. *B* accepts *M* if and only if $A=g^M(\mathrm{mod}\,p)$.

Prove the correctness:

$(K^X)(X^Y)\bmod p = (g^r)^X\ (g^R)^Y \bmod p = g^{rX}\ g^{RY} \bmod p = g^{rX+RY} \bmod p = g^{(rX+RY) \bmod (p-1)} \bmod p = g^M \bmod p$

Example

1. $p=11$; $g=2$;

2. $2^0=1(\mathrm{mod}11)$; $2^1=2(\mathrm{mod}11)$;

$2^2=4(\mathrm{mod}11)$; $2^3=8(\mathrm{mod}11)$;

$2^4=5(\mathrm{mod}11)$; $2^5=10(\mathrm{mod}11)$;

$2^6=9(\mathrm{mod}11)$; $2^7=7(\mathrm{mod}11)$;

$2^8=3(\mathrm{mod}11)$; $2^9=6(\mathrm{mod}11)$;

2^{10}=1(mod11);

3. Let r=8; K=g^r=2^8 mod11=3.

4. Then sender sends to B (K,g,p)=(3,2,11).

   Signing

5. Let M=5; then select R=9: gcd(R,p-1)=1;

6. X=g^R=2^9=6(mod11);

7. Sender S finds Y=3 and sends (M, X, Y)=(5,6,3);

8. The receiver computes

   (K^X)(X^Y)(mod$p$)=(3^6)(6^3)=10(mod11)=10;

9. g^M(mod$p$)=2^5(mod11)=10;

10. Since these two numbers are the same, the receiver accepts the message *M*.