22 ELECTRONIC DIGITAL SIGNATURE ELGAMAL

Suppose that the base p and the generator g are public values chosen in some suitable way, and that each user who wishes to sign messages has a private signing key X and a public signature verification key $Y = g^X$. An ElGamal signature scheme works as follows. Choose a message key k at random, and form $r = g^k \pmod{p}$. Now form the signature s using a linear equation in k, r, the message M and the private key X. There are a number of equations that will do; the particular one that happens to be used in ElGamal signatures is

$$rX + sk = M$$

So s is computed as $s = (M - rX)/k$; this is done modulo $\phi(p)$. When both sides are passed through our one-way homomorphism $f(x) = g^x \bmod p$ we get:

$$g^{rX} g^{sk} \equiv g^M$$

or

$$Y^r r^s \equiv g^M$$

An ElGamal signature on the message M consists of the values r and s, and the recipient can verify it using the above equation.

To verify, the receiver checks that

$$Y^a a^b \bmod P = G^{m'} \bmod P. \tag{1}$$

Proof of correctness:

$$Y^a a^b \bmod P = \left(G^X\right)^a \left(G^K\right)^b \bmod P = G^{Xa+Kb} \bmod P. \tag{2}$$