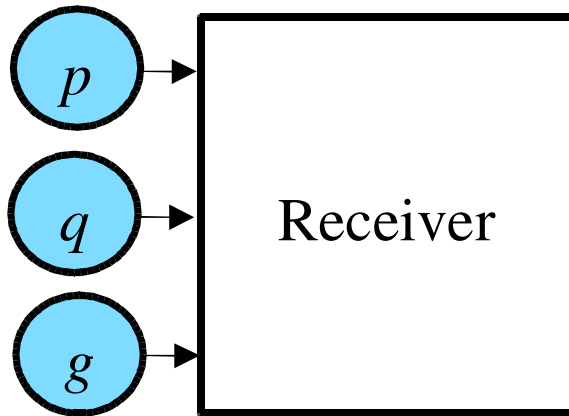


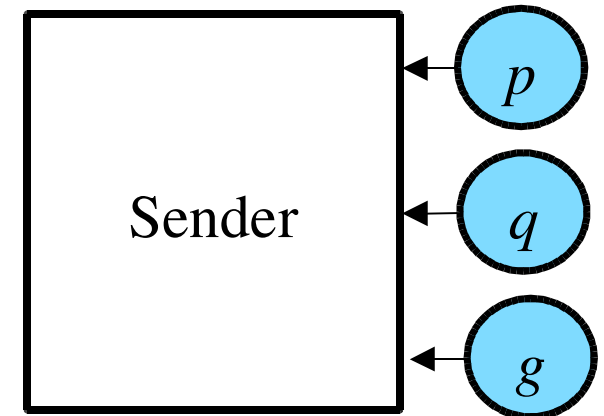
Digital Signature Standard

Digital Signature Standard

Setup



$\langle T, S \rangle$



$\langle T, S \rangle$

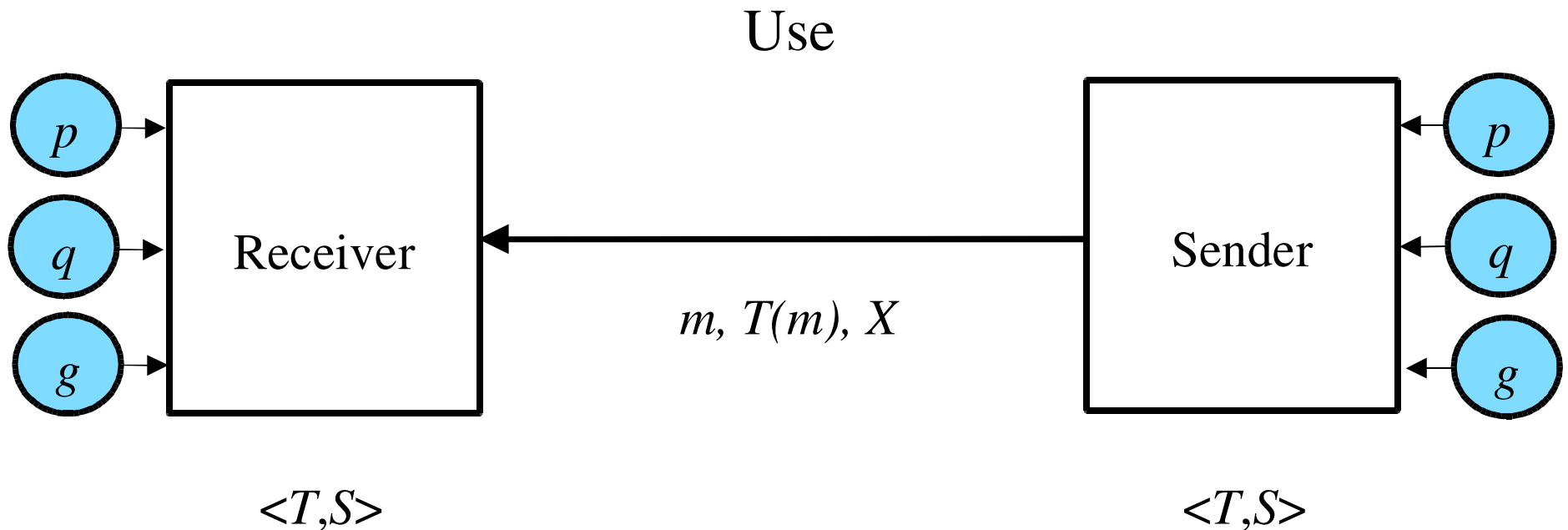
Generate p and q , both prime and public.

q has 160 bits, p has 512 bits and $p = kq + 1$.

Find g such that $g^q = 1 \pmod p$

Choose $S < q$ and $T^S = g \pmod p$. (long term key pair – T public)

Digital Signature Standard



Choose $S(m)$ and $T(m) = ((g^{S(m)} \bmod p) \bmod q)$ (per message key)

Compute $S(m)^{-1} \bmod q$

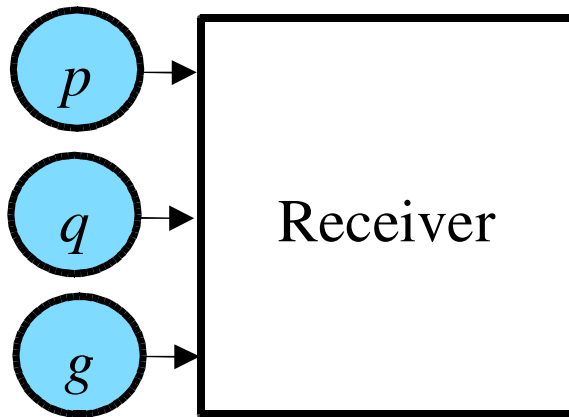
Calculate message digest $d(m)$ of the message using SHS.

Compute signature $X = S(m)^{-1} (d(m) + ST(m)) \bmod q$.

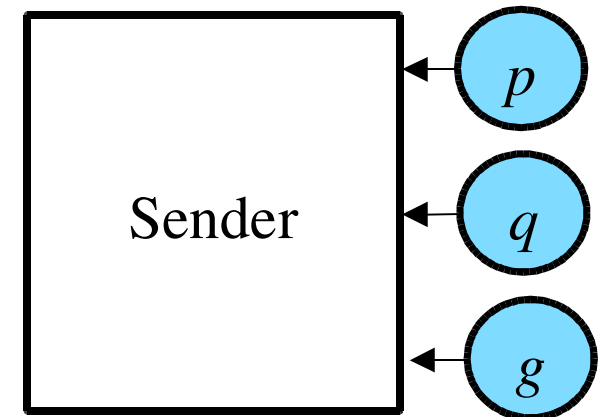
Transmit message m , per-message public number $T(m)$, X

Digital Signature Standard

Verification



$\langle T, S \rangle$



$\langle T, S \rangle$

Calculate $X^{-1} = (S(m)^{-1} (d(m) + ST(m)))^{-1}$

Calculate $d(m)^{-1}$

Calculate $x = d(m) * X^{-1}$

Calculate $y = T(m) * X$

Calculate $z = (g^x * T^y \text{ mod } p) \text{ mod } q$

Check that $z == T(m)$

Signing Properties

1. Signing something should not divulge the secret S
2. Nobody should be able to generate a signature without knowing S
3. Nobody should be able to generate a message that matches a signature
4. Nobody should be able to modify a signed message in a way that keeps the same signature valid