Key Generation

Choose a big enough prime number p and a primitive root g:

$$g \in \mathbb{Z}_p ,\ p \textit{ is prime}$$

Select an α at random

$$\alpha \in \{1,2, \ldots, p-2\}$$

and compute A with

$$A \equiv_p g^{\alpha}$$

The private key is the exponent α, whereas the tripel *(p,g,A)* represents the public key.

Signature

$M \in \{0,1\}^{*}$:= the to be signed message.

$h: M \rightarrow \{1,2, \ldots, p-2\}$:= a cryptographic hash function.

Select a k by chance

$$k \in \{1,2, \ldots, p-2\} \textit{ with } gcd(k, p-1)=1$$

and compute the signature *(r,s)* of the message M

$$r \equiv_p g^k \ ,\ \ s \equiv_{(p-1)} k^{-1}(h(M)-\alpha r)$$

Verification

Verify that $1 \leq r \leq p-1$ and $A^r r^s \equiv_p g^{h(m)}$ holds.

Correctness

$$A^r r^s \equiv_p g^{\alpha r} g^{k s} \equiv_p g^{\alpha r} g^{k(k^{-1}(h(M)-\alpha r) mod (p-1))}$$

$$A^r r^s \equiv_p g^{h(m)} \textit{ with } h(m) \in \{1,2, \ldots, p-2\}$$

In case $A^r r^s \equiv_p g^{h(m)}$ is fulfilled for a certain tuple *(r,s)* and furthermore $r \equiv_p g^k$ holds, it follows

$$g^{\alpha r + k s} \equiv_p g^{h(m)}$$

Besides we know

$$g^y \equiv_p g^x \Leftrightarrow x \equiv_{(p-1)} y$$

$$\alpha r + k s \equiv_{(p-1)} h(m)$$

$$k s \equiv_{(p-1)} h(m) - \alpha r$$

$$s \equiv_{(p-1)} k^{-1}(h(m) - \alpha r)$$