PA2: Digital Signatures

v3

Digital Signature Algorithms

DSA (Digital Signature Algorithms)

Public parameters:

- p, q: large primes. $p > q, q|(p-1)$
- g: generator: $1 < g < p$. $g^q \equiv 1 (\mathrm{mod}\ p)$. $g^e \not\equiv 1 (\mathrm{mod}\ p)$ for $e \in \{1, 2, \ldots, q-1\}$.

p, q, g are fixed and provided in this assignment.

Generate Key

- secret signing key x: choose random $x \in \{1, 2, \ldots, q-1\}$
- public verification key y: $y = g^x (\mathrm{mod}\ p)$. $y \in [2, p-1]$

Signing

Given message $m : string$, secret key x.

- Choose random k from $\{1, 2, q-1\}$
- Compute: $r = (g^k \bmod p) \bmod q$
- Compute: $z = Number :: Hash(m)$
- Compute: $s = (k^{-1}(z + xr)) \bmod q$.
- If r or s is 0, choose different k.
- (r, s) is the signature.

Note: $ki = k^{-1}(\text{mod } q)$ is the unique element in $\{1, 2, \ldots, q-1\}$ $s.t.\ (ki \cdot k) \equiv 1(\text{mod } q)$. The computation is provided in $Number :: Inv()$.

Verification

Given message $m : string$, public key y, signature (r, s).

- Check that both r and s are in $\{1, 2, \ldots, q-1\}$. If not, return false.
- Compute: $w = s^{-1} \bmod q$
- Compute: $z = Number :: Hash(m)$
- Compute: $u_1 = (zw) \bmod q$
- Compute: $u_2 = (rw) \bmod q$
- If $(g^{u_1} y^{u_2} \bmod p) \bmod q = r$, return true. Else, return false.

Schnorr

Public parameters:

- p, q: large primes. $p > q, q|(p-1)$
- g: generator: $1 < g < p$. $g^q \equiv 1(\text{mod } p)$. $g^e \not\equiv 1(\text{mod } p)$ for $e \in \{1, 2, \ldots, q-1\}$.

p, q, g are fixed and provided in this assignment.

Generate Key

- secret signing key x: choose random $x \in \{1, 2, \ldots, q-1\}$
- public verification key y: $y = g^x(\text{mod } p)$. $y \in [2, p-1]$

Signing

Given message $m : string$, secret key x.

- Choose random k from $\{1, 2, q-1\}$
- Compute: $r = (g^k \bmod p)$

- Compute: $e = Number :: Hash(r, m) \bmod q$
- Compute: $s = (k - xe) \bmod q$.
- If s or e is 0, choose different k.
- (s, e) is the signature.

Verification

Given message $m : string$, public key y, signature (s, e).

- Check that both s and e are in $\{1, 2, \ldots, q - 1\}$. If not, return false.
- Compute: $r_v = (g^s y^e) \bmod p$
- Compute: $e_v = Number :: Hash(r_v, m) \bmod q$
- If $e_v = e$, return true. Else, return false.