## Digital Signature

**Def.** Digital signature consists of ($\mathsf{KeyGen}$, $\mathsf{Sign}$, $\mathsf{Verify}$):

- $(vk, sk) \leftarrow \mathsf{KeyGen}(1^\lambda)$;
  - Input: a security parameter $\lambda$
  - Output: a verification key $vk$ and a signing key $sk$
- $\sigma \leftarrow \mathsf{Sign}(m, sk)$;
  - Input: a message $m$ and a signing key $sk$
  - Output: a signature $\sigma$ of $m$
- $b \leftarrow \mathsf{Verify}(m, \sigma, vk)$;
  - Input: a message $m$, a signature $\sigma$ and a verification key $vk$
  - Output: a bit $b = 1$ when $\sigma$ is a valid siganture of $m$

## RSA Signature

- $\mathsf{KeyGen}(1^\lambda)$;
  - Choose two large primes $p$ and $q$ and $n := pq$
  - Choose $e$ such that $1 < e < \phi(n) = (p-1)(q-1)$ and $\gcd(e, \phi(n)) = 1$
  - Compute $d$ such that $ed \equiv 1 \bmod p$
  - Output $vk = \{e, n\}$ and $sk = \{d, p, q\}$
- $\mathsf{Sign}(m, sk)$;
  - Output $m^d \bmod n$
- $\mathsf{Verify}(m, \sigma, vk)$;
  - Compute $m' := \sigma^e \bmod n$
  - If $m = m'$, output 1
  - Otherwise, output 0

## ElGamal Signature

- $\mathsf{KeyGen}(1^\lambda)$;
  - Choose a large prime $p$ and $g \leftarrow \mathbb{Z}_p^*$
  - Choose a secret key $s \leftarrow \mathbb{Z}_p^*$
  - Compute $y := g^s \bmod p$.
  - Output $vk = \{p, g, y\}$ and $sk = \{s\}$
- $\mathsf{Sign}(m, sk)$;
  - Choose a random $r \leftarrow \mathbb{Z}_p^*$
  - Compute $\sigma_1 := g^r \bmod p$ and $\sigma_2 := r^{-1}(m - s \cdot \sigma_1) \bmod p - 1$
  - Output $\sigma = (\sigma_1, \sigma_2)$
- $\mathsf{Verify}(m, \sigma, vk)$;
  - Compute $g_1 := y^{\sigma_1} \sigma_1^{\sigma_2} \bmod p$

  - Compute $g_2 := g^m \bmod p$
  - If $g_1 \equiv g_2$, output 1
  - Otherwise, output 0

- A signed message $m$ is revealed.
- How to generate a signature while protecting a message?
  - use Blind signature which will be covered in the next time.
- If $m$ is long, use $(m, \sigma(H(m)))$ instead of $(m, \sigma(m))$ where $H$ is a cryptographic hash function.

## Digital Signature Algorithm (DSA)

- KeyGen$(1^\lambda)$;
  - Choose a prime $q$ and $p$ such that $q|p-1$.
  - Choose $g \leftarrow \mathbb{Z}_p^*$ and compute $y_1 := g^{\frac{p-1}{q}} \bmod p$
  - Choose a secret $s \leftarrow \mathbb{Z}_p^*$ and $y_2 = y_1^s$
  - Output $vk = \{p, g, y_1, y_2\}$ and $sk = \{s\}$
- Sign$(m, sk)$;
  - Choose a random $0 < r < q-1$.
  - Compute $\sigma_1 := y_1^r \bmod p \bmod q$
  - Compute $\sigma_2 := r^{-1}(m + s \cdot \sigma_1) \bmod q$
  - Output $(\sigma_1, \sigma_2)$
- Verify$(m, \sigma, vk)$;
  - Parse $\sigma$ as $(\sigma_1, \sigma_2)$.
  - Compute $u_1 \equiv \sigma_2^{-1} m \bmod q$
  - Compute $u_2 \equiv \sigma_2^{-1} \sigma_1 \bmod q$
  - Compute $v \equiv y_1^{u_1} y_2^{u_2} \bmod p \bmod q$
  - If $v = \sigma_1$, output 1.
  - Otherwise, output 0.

**Correctness**

Since $m \equiv -s\sigma_1 + r\sigma_2 \bmod q$, $\sigma_2^{-1} m \equiv -s\sigma_1\sigma_2^{-1} + r \bmod q$.

Then, $r \equiv \sigma_2^{-1} m + s\sigma_1\sigma_2^{-1} \equiv u_1 + su_2 \bmod q$

Therefore, $v \equiv y_1^r \equiv y_1^{u_1+su_2} \equiv y_1^{u_1} y_2^{u_2} \bmod p \bmod q$