1. El-Gamal Digital Signature

- PP: prime p, generator g in $\mathbb{Z}_p^*$
- KeyGen: $x \leftarrow \{0, 1, \cdots, p-2\}$ $\quad sk = x$

  $y = g^x \bmod p \in \mathbb{Z}_p^*$ $\quad pk = y$
- Sign(PP, sk, m):

  Compute $h(m) \in \mathbb{Z}_{p-1}$

  Choose $k \leftarrow \mathbb{Z}_{p-1}^*$

  Compute $r = g^k \pmod p$

  Compute $A = \frac{h(m) - rx}{k} \pmod{p-1}$.

  $\sigma(m) = (r, A)$
- Verify(PP, pk, m, σ):

  Check that $0 < r < p$

  Check that $y^r \cdot r^A = g^{h(m)} \pmod p$.

Correctness: $y^r \cdot r^A = g^{xr} \cdot g^{k(\frac{h(m)-rx}{k})} = g^{h(m)}$

Security: ① not secure if h = identity

Choose $e \leftarrow \mathbb{Z}_{p-1}$

Compute $r = g^e \cdot y \bmod p$.

$A = -r$

Then (r, A) is a valid signature of $m = -e \cdot r \pmod{p-1}$

$y^r \cdot r^A = y^r \cdot (g^e \cdot y)^{-r} = g^{-e \cdot r} = g^m \pmod{p-1}$

② What about security in ROM?

Not know how to reduce to DL problem.

Pointcheval - Stern '1996: modified version

- Sign: $k \leftarrow \mathbb{Z}_{p-1}^*$

  $r = g^k \pmod p$

  $A = \frac{h(m \| r) - rx}{k} \pmod{p-1}$

Verify: Check $0<r<p$ and $y^r \cdot r^A = g^{h(m\|r)}$

Security: Modified El-Gamal is existentially unforgeable against adaptive chosen message attacks. in ROM, assuming DLP is hard.

2. Digital Signature Standard (DSS - NIST '91).

- PP: q prime. $|q| = 160$ bits.
  $p = nq+1$ prime $|p| = 1024$ bits.
  g_0 generators of $\mathbb{Z}_p^*$
  $g = g_0^n$ generators subgroup of $\mathbb{Z}_p^*$ (order q).
- KeyGen: Choose $x \leftarrow \mathbb{Z}_q$ $sk = x$ 160 bits.
  $y = g^x \bmod p$ $pk = y$ 1024 bits.
- Sign: $k \leftarrow \mathbb{Z}_q^*$
  $r = g^k \pmod p \pmod q$ 160 bits.
  $A = \frac{h(m)+rx}{k} \pmod q$ 160 bits.
  redo if $r=0$ or $A=0$
- Verify: Check $0<r, A<q$
  Check $y^{r/A} \cdot g^{h(m)/A} \pmod p \pmod q = r$

Correctness. $y^{r/A} \cdot g^{h(m)/A} = g^{\frac{xr+h(m)}{A}} = g^k = r \pmod p \pmod q$

Security: insecure if h = identity.
Provably secure if $h(m)$ is replaced with $h(m\|r)$

3. ECDSA

- PP: curve. g generator of order n.
- KeyGen: $x \leftarrow \{1, \cdots, n-1\}$. $y = xg$
  $sk = x$ $pk = y$
- Sign. Choose $k \leftarrow \{1, \cdots, n-1\}$
  Compute $(u, v) = kg$.

$r = u \bmod n$.

$A = \frac{h(m) + rx}{k} \pmod n$.

redo if $r = 0$ or $A = 0$.

- Verify: Check $0 < r, A < n$.

  Compute $(\alpha, \beta) = \frac{h(m)}{A} g + \frac{r}{A} y$

  Check $\alpha = r \pmod n$.

Correctness. $\frac{h(m)}{A} g + \frac{r}{A} y = \frac{h(m) + xr}{A} g = kg$