20 Sep 2024

# Digital Signature Schemes based on DLP

## Digital Signature Algorithm (DSA)

**Key Generation for DSA**

1. Generate a prime $p$ with $2^{1023} < p < 2^{1024}$.
2. Find a prime divisor $q$ of $p-1$ with $2^{159} < q < 2^{160}$.
3. Find an element $\alpha$ with $\mathrm{ord}(\alpha) = q$, i.e., $\alpha$ generates the subgroup with $q$ elements.
4. Choose a random integer $d$ with $0 < d < q$.
5. Compute $\beta \equiv \alpha^d \bmod p$.

The keys are now:
$k_{pub} = (p, q, \alpha, \beta)$
$k_{pr} = (d)$

**DSA Signature Generation**

1. Choose an integer as random ephemeral key $k_E$ with $0 < k_E < q$.
2. Compute $r \equiv (\alpha^{k_E} \bmod p) \bmod q$.
3. Compute $s \equiv (SHA(x) + d \cdot r)\, {k_E}^{-1} \bmod q$.

**DSA Signature Verification**

1. Compute auxiliary value $w \equiv s^{-1} \bmod q$.
2. Compute auxiliary value $u_1 \equiv w \cdot SHA(x) \bmod q$.
3. Compute auxiliary value $u_2 \equiv w \cdot r \bmod q$.
4. Compute $v \equiv (\alpha^{u_1} \cdot \beta^{u_2} \bmod p) \bmod q$.
5. The verification $ver_{k_{pub}}(x, (r, s))$ follows from:

$$v \begin{cases} \equiv r \bmod q \Longrightarrow \text{valid signature} \\ \not\equiv r \bmod q \Longrightarrow \text{invalid signature} \end{cases}$$

**Key Generation for ECDSA**

1. Use an elliptic curve $E$ with
   - modulus $p$
   - coefficients $a$ and $b$
   - a point $A$ which generates a cyclic group of prime order $q$
2. Choose a random integer $d$ with $0 < d < q$.
3. Compute $B = dA$.

The keys are now:
$k_{pub} = (p, a, b, q, A, B)$
$k_{pr} = (d)$

**ECDSA Signature Generation**

1. Choose an integer as random ephemeral key $k_E$ with $0 < k_E < q$.
2. Compute $R = k_E A$.
3. Let $r = x_R$.
4. Compute $s \equiv (h(x) + d \cdot r)\, {k_E}^{-1} \bmod q$.

**ECDSA Signature Verification**

1. Compute auxiliary value $w \equiv s^{-1} \bmod q$.
2. Compute auxiliary value $u_1 \equiv w \cdot h(x) \bmod q$.
3. Compute auxiliary value $u_2 \equiv w \cdot r \bmod q$.
4. Compute $P = u_1 A + u_2 B$.
5. The verification $ver_{k_{pub}}(x, (r, s))$ follows from:

$$x_P \begin{cases} \equiv r \bmod q \Longrightarrow \text{valid signature} \\ \not\equiv r \bmod q \Longrightarrow \text{invalid signature} \end{cases}$$