Other public key cryptosystems

Public-key encryption

Discrete Logarithm

Definition

• Let $p$ be a prime, $q$ a prime divisor of $p-1$ and $g \in [1, p-1]$ has order $q$

• Let $x$ be the private key selected at random from $[1, q-1]$

• Let $y$ be the corresponding public key $y = g^x \mod p$

• Discrete Logarithm Problem (DLP). Given $(p, q, g)$ and $y$, determine $x$
ElGamal encryption scheme

• Encryption (2 exp)
  – select \( k \) randomly
  – \( c_1 = g^k \mod p \), \( c_2 = m \times y^k \mod p \)
  – send \((c_1, c_2)\) to recipient

• Decryption (1 exp)
  – \( c_1^x = g^{kx} \mod p = y^k \mod p \)
  – \( m = c_2 \times y^{-k} \mod p \)

• Security
  – An adversary needs \( y^k \mod p \). The task of calculating \( y^k \mod p \) from \((g, p, q)\) and \( y \) is equivalent to DHP and thus based on DLP in \( \mathbb{Z}_p \)

ElGamal in practice

• Prime \( p \) and generator \( g \) can be common system-wide

• Prime \( p \) size
  – 512-bit: marginal
  – 768-bit: recommended
  – 1024-bit or larger: long-term

• Efficiency
  – Encryption requires two modular exponentiations
  – Message expansion by a factor of 2

• Security
  – Different random integers \( k \) must be used for different messages
Elliptic Curve Cryptography

- Let $p$ and $\in \mathbb{F}_p$
- Let $E$ be an elliptic curve defined by $y^2 = x^3 + ax + b \pmod{p}$ where $a, b \in \mathbb{F}_p$ and $4a^3 + 27b^2 = 0$
- Example. $E: y^2 = x^3 + 2x + 4 \pmod{p}$
- The set of points $E(\mathbb{F}_p)$ with point at infinity $\infty$ forms an additive Abelian group

Elliptic curves: geometrical approach
Elliptic Cryptography (ECC)

- **Algebraic Approach**
  - Elliptic curves defined on finite field define an Abelian finite field

- **Elliptic curve discrete logarithm problem**
  - Given points $G$ and $Q$ such that $Q = kG$, find the integer $k$
  - No sub-exponential algorithm to solve it is known

- **ECC keys are smaller than RSA ones**

---

**Elliptic Curve Cryptography**

- Let $P$ have order $n$ then the cyclic subgroup generated by $P$ is $G = \langle P, 2P, \ldots, (n - 1)P \rangle$

- Parameters $P$ and $n$ are the **public parameters**

- **Private key** $d$ is selected at random in $[1, n - 1]$

- **Public key** $Q = dP$
Ellyptic Curve Cryptography

• **Encryption**
  – A message \( m \) is represented as a point \( M \)
  – \( C_1 = kP; \ C_2 = M + kQ \)
  – send \( (C_1; \ C_2) \) to recipient

• **Decryption**
  – \( dC_1 = d(kP) = kQ \)
  – \( M = C_2 - dC_1 \)

• **Security**
  – The task of computing \( kQ \) from the domain parameters, \( Q \), and \( C_1 = kP \), is the **ECDHP**

\[
\begin{array}{|c|c|c|c|c|}
\hline
& 80 & 112 & 128 & 192 & 256 \\
\hline
\text{EC parameter n} & 160 & 224 & 256 & 384 & 512 \\
\text{RSA modulus n} & 1024 & 2048 & 3072 & 8192 & 15360 \\
\text{DL modulus p} & & & & & \\
\hline
\end{array}
\]

Comparison among crypto-systems

• Private key operations are more efficient in EC than in DL or RSA
• Public key operations are more efficient in RSA than EC or DL if small exponent \( e \) is selected for RSA
## Comparison among crypto-systems

<table>
<thead>
<tr>
<th>Security level (bits)</th>
<th>DL parameter q (EC parameter n)</th>
<th>RSA modulus n (DL modulus p)</th>
</tr>
</thead>
<tbody>
<tr>
<td>80 (SKIPJACK)</td>
<td>160</td>
<td>1024</td>
</tr>
<tr>
<td>112 (3DES)</td>
<td>224</td>
<td>2048</td>
</tr>
<tr>
<td>128 (AES small)</td>
<td>256</td>
<td>3072</td>
</tr>
<tr>
<td>192 (AES medium)</td>
<td>384</td>
<td>8192</td>
</tr>
<tr>
<td>256 (AES large)</td>
<td>512</td>
<td>15360</td>
</tr>
</tbody>
</table>

- Private key operations are more efficient in EC than in DL or RSA.
- Public key operations are more efficient in RSA than EC or DL if small exponent $e$ is selected for RSA.

**Other PK cryptosystems**