Cryptography – BCS 3
Public-Key Cryptography – Cyclic Group and Elliptic Curves

Pierre-Alain Fouque
Université de Rennes 1
September, 29 2020
Agenda

1. Cyclic Groups
2. Elliptic Curves
Cyclic Groups

Definition
Let \( N \) be a positive integer. Then \( \mathbb{Z}/N\mathbb{Z} = \mathbb{Z}_N \) is a group under addition mod \( N \), and \( \mathbb{Z}_N^* \) is a group under the multiplication mod \( N \).

Definition (Cyclic Group)
Let \( G \) be a finite group of order \( n \), with identity element \( e \). \( G \) is cyclic if there exists an element of order \( n \), called generator of \( G \). A cyclic group is abelian. If \( x \) is a generator, \( G = \{ e, x, \ldots, x^{n-1} \} \).

Definition
The group \( \mathbb{Z}_N^* \) is cyclic when \( N \) is a prime.
In any group $G$, we can define an exponentiation operation:

- If $i = 0$, then $a^i$ is defined to be 1.
- If $i > 0$, then $a^i = a \cdot a \cdot \ldots \cdot a$ ($i - 1$ times).
- If $i < 0$, then $a^i = a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}$ ($i - 1$ times).

For all $a \in G$ and all $i, j \in \mathbb{Z}$:

- $a^{i+j} = a^i \cdot a^j$
- $(a^i)^j = a^{ij}$
- $a^{-1} = (a^i)^{-1} = (a^{-1})^i$
Some relations to know to compute

**Definition**

The order of a group is its size.

**Fact**

- If $G$ is a group and $m = |G|$ its order:
  - $a^m = 1$ for all $a \in G$
  - $a^i = a^{i \mod m}$ for all $a \in G$ and $i \in \mathbb{Z}$

- Example: In $\mathbb{Z}^*_{21} = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$ under the operation of multiplication modulo 21. $m = 12$.

$$5^{86} \mod 21 = 5^{86 \mod 12} \mod 21 = 5^{2 \mod 12} \mod 21 = 25 \mod 21 = 4$$
Subgroups and examples

- If $G$ is a group, $S \subseteq G$ is a subgroup if it is a group under the same operation as that under which $G$ is a group.
- If we already know that $G$ is a group, there is a simple way to test whether $S$ is a subgroup:
  - it is one if and only if $x \cdot y^{-1} \in S$ for all $x, y \in S$.
  - $y^{-1}$ is the inverse of $y$ in $G$.
- Fact: Let $G$ be a group and let $S$ be a subgroup of $G$. Then, the order of $S$ divides the order of $G$.

$\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ for a prime $p$ is cyclic of order $p - 1$:

- E.g. $p = 11$, the subgroups are $S_1 = \{1\}$, $S_2 = \{-1, 1\}$, $S_5 = \{1, 4, 5, 9, 3\}$, and $S_{10} = \{1, 2, 4, 8, 5, 10, 9, 7, 3, 6\}$.
- For each divisors of $p - 1 = 10$, a subgroup of that order exists.
- 2 is a generator, as well as $2^k$ for $\gcd(k, 10) = 1$. 
If \( g \in G \) is any member of the group, the order of \( g \) is defined to be the least positive integer \( n \) st \( g^n = 1 \). We let \( \langle g \rangle = \{g^i | i \in \mathbb{Z}\} = \{g^0, g^1, \ldots, g^{n-1}\} \) denote the set of group elements generated by \( g \). This is a subgroup of order \( n \).

An element \( g \) of the group is called a generator of \( G \) if \( \langle g \rangle = G \) or, equivalently, it its order is \( m = |G| \).

A group is cyclic if it contains a generator.

If \( g \) is a generator of \( G \), then for every \( a \in G \), there is a unique integer \( i \in \mathbb{Z}_m \) s.t. \( g^i = a \). This \( i \) is called the discrete logarithm of \( a \) to base \( g \), and we denote it by \( \text{DLOG}_{G,g}(a) \).

\( \text{DLOG}_{G,g}(a) \) is a function that maps \( G \) to \( \mathbb{Z}_m \), and moreover this function is a bijection.

The function \( \mathbb{Z}_m \) to \( G \) defined by \( i \mapsto g^i \) is called the discrete exponentiation function.
Choosing cyclic group and generators

- The discrete log function is conjectured to be one-way (hard-to-compute) for some cyclic groups $G$. Due to this fact, we often seek cyclic groups.

- Examples of cyclic groups:
  1. $\mathbb{Z}_p^*$ for a prime $p$
  2. a group of prime order

- Finding generators: How to chose a candidate and test it?

- Let $G$ be a cyclic group and let $m = |G|$. Let $p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ be the prime factorization of $m$ and let $m_i = m/p_i$ for $i = 1, \ldots, n$. Then, $g \in G$ is a generator of $G$ iff for all $i = 1, \ldots, n$: $g^{m_i} \neq 1$.

- If $G$ is a cyclic group of order $m$, and $g$ a generator of $G$: $\text{Gen}(G) = \{g^i | i \in \mathbb{Z}_m^*\}$ and $|\text{Gen}(G)| = \varphi(m)$. 

\[\text{Pierre-Alain Fouque}\] 

\[\text{Cryptography – BCS 3 Public-Key Cryptography – Cyclic Group and Elliptic Curves}\]
Example: determine all the generators of $\mathbb{Z}_{11}^*$

- Its size is $m = \varphi(11) = 10$ and the prime factorization of $10 = 2 \cdot 5$. Thus the test for whether a given $a \in \mathbb{Z}_{11}^*$ is a generator is that $a^2 \neq 1 \mod 11$ and $a^5 \neq 1 \mod 11$.
- $\text{Gen}(\mathbb{Z}_{11}^*) = \{2, 6, 7, 8\}$
- Double-checking: $|\mathbb{Z}_{11}^*| = 10$, $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$

\[
\{2^i \in G | i \in \mathbb{Z}_{10}^*\} = \{2^1, 2^3, 2^7, 2^9 \mod 11\} = \{2, 6, 7, 8\}
\]
Algorithm for finding a generator

- Most common choice of a group in crypto is $\mathbb{Z}_p^*$ for a prime $p$
- Idea: Pick a random element and test it. Choose $p$ s.t. the prime factorization of the order of the group $(p - 1)$ is known. E.g., chose a prime $p$ s.t. $p = 2q + 1$ for some prime $q$
- The probability that an iteration of the algorithm is successful:

$$\frac{|\text{Gen}(\mathbb{Z}_p^*)|}{|\mathbb{Z}_p^*| - 2} = \frac{\varphi(p-1)}{p-3} = \frac{\varphi(2q)}{2q-2} = \frac{q-1}{2q-2} = \frac{1}{2}$$

**Algorithm 1** Finding a generator

1: $q = (p - 1)/2$; found ← false
2: while found ≠ true do
3:   $g \leftarrow \mathbb{Z}_p^* \setminus \{1, p - 1\}$
4:   if $(g^2 \mod p \neq 1) \&\& (g^q \mod p \neq 1)$ then
5:     found ← true
6:   end if
7: end while
return $g$
Squares mod $n$

### Quadratic Residue mod $n$

- **Def**: an element $a$ mod $n$ is a quadratic residue mod $n$ if there exists $b$ with $a = b^2$ mod $n$.
- Other elements are called *non-quadratic residue*.
- $1, 4, 9, 5, 3$ are square mod $11$.
- Other values $2, 3, 6, 7, 8, 10$ are not square mod $11$.

<table>
<thead>
<tr>
<th>$a$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a^2$ mod 11</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>9</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>
Elliptic Curves

Elliptic curve is a group for the addition

- an elliptic curve $\mathcal{E}$ is a set of points satisfying the equation $y^2 = x^3 + ax + b$ over $\mathbb{Z}/p\mathbb{Z}$
- These points form a group with an additive notation
- This group is not cyclic, but from one element we can define a cyclic group
- From one point $G$, the $\langle G \rangle$ is the group generated by the point $G$ with the addition (defined in the next slide)
- Specific point at infinity: $\infty$ identity element for this group
- From $G$, we can define $k \times G = G + G + \ldots + G$ ($k - 1$) times
- If the order of the group $\langle G \rangle$ (number of different points) is prime, it is difficult to invert the scalar multiplication operation
Algorithm 2 Double-and-add $d = d_0 + 2d_1 + 2^2d_2 + \ldots + 2^m d_m$

1: $N \leftarrow P$
2: $Q \leftarrow \infty$
3: for $i$ from 0 to $m$ do
4: if $d_i = 1$ then
5: $Q \leftarrow \text{point-add}(Q, N)$
6: end if
7: $N \leftarrow \text{point-double}(n)$
8: end for
return $Q = dP$
El Gamal Encryption – ECIES

Informal description

1. Alice gets Bob’s public key, $g^x$. He knows his own private key $x$.
2. Alice generates a fresh, ephemeral value $y$, and $g^y$ (public).
3. Alice computes $c$ from $m$, the symmetric encryption of $m$ with key $k$ (authenticated encryption scheme): $c = E(k; m)$.
4. Alice sends the public ephemeral $g^y$ and the ciphertext $c$.
5. Bob, knowing $x$ and $g^y$, $k = KDF(g^{xy})$ and recovers $m$ from $c$.

Common Parameters

- Key Derivation Function: HMAC-SHA-1-80 with 80-bit
- Symmetric encryption scheme AES-GCM noted $E$
- Elliptic curve parameters: $\langle G \rangle$ of order $n$, $\infty$ infinity
- Bob’s PK: $K_B = k_B G$, $k_B \in [1, n - 1]$ random private key
- Optional shared information: $S_1$ and $S_2$
El Gamal Encryption – ECIES

Encryption : To encrypt a message \( m \) Alice :

- generates a random \( r \in [1, n - 1] \) and computes \( R = rG \)
- derives a shared secret \( S = P_x, P = (P_x, P_y) = rK_B \neq \infty \)
- uses a KDF to derive symmetric encryption and MAC keys :
  \[ k_E \| k_M = KDF(S \| S_1) \]
- encrypts the message : \( c = E(k_E; m) \)
- computes the tag of \( c \) and \( S_2 \) :
  \( d = MAC(k_M; c \| S_2) \)
- output \( R \| c \| d \)

Decryption : To decrypt the ciphertext \( R \| c \| d \)

1. derives the shared secret : \( S = P_x \) with \( P = (P_x, P_y) = k_B R \) :
   \[ P = k_B R = k_B rG = rK_B G = rK_B, \text{ or output failed if } P = \infty \]
2. \( k_E \| k_M = KDF(S \| S_1) ; \text{ output failed if } d \neq MAC(k_M; c \| S_2) \)
3. uses symmetric encryption scheme to decrypt \( m = E^{-1}(k_E; c) \)
## Signature process: $d_A$ private key

1. $e = \text{SHA} - 2(m)$, convert it to an integer.
2. Let $z$ be the $L_n$ leftmost bits of $e$ where $L_n$ the bit length of $n$.
3. Choose a **cryptographically secure random** $k \in [1, n - 1]$
4. Compute the curve point $(x_1, y_1) = k \times G$
5. Compute $r = x_1 \mod n$. If $r = 0$, go to step 3.
6. Compute $s = k^{-1}(z + rd_A) \mod n$. If $s = 0$, go to step 3.
7. The signature is $(r, s)$. ($(r, -s \mod n)$ is also valid)
# ECDSA

## Verification: $Q_A = d_A G$ public key

1. Check $Q_A \neq \infty$, $Q_A \in \mathcal{E}$, $n \times Q_A = \infty$
2. $r, s \in [1, n - 1]$, if not, return invalid
3. Compute $e = SHA - 2(m)$ and $z$ the $L_n$ leftmost bits of $e$
4. Compute $u_1 = z s^{-1} \mod n$ and $u_2 = r s^{-1} \mod n$
5. $(x_1, y_1) = u_1 \times G + u_2 \times Q_A$. If $(x_1, y_1) = \infty$, Return Invalid.
6. Return Valid if $r = x_1 \mod n$, invalid otherwise

- Do not use twice the same $k$ (PlayStation 3)
- if the first significant bits of $k$ are known, it is possible to recover the secret key!
- Check that $C = u_1 \times G + u_2 \times Q_A = k \times G$
Weierstrass equation: \( y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \)

sage: `EllipticCurve([0,0,1,-1,0])`: Elliptic Curve defined by \( y^2 + y = x^3 - x \) over Rational Field

Elliptic curves over \( \mathbb{Z}/N\mathbb{Z} \) with \( N \) prime are of type "elliptic curve over a finite field" :

sage: `F=Zmod(95); EllipticCurve(F, [2,3])`: \( y^2 = x^3 + 2x + 3 \) over Ring of integers modulo 95

definition of point: sage \( P = E(-1,1) \)

group order: \( P.order() \)