7. Discrete Logarithm & Related Cryptosystems

Def. 7.1. Let $a \in \mathbb{Z}_n^*$.

$$\mathrm{ord}_n(a) = \min\{k \in \{1, \dots, \varphi(n)\} \mid a^k \equiv 1 \pmod{n}\}$$

is called the order of a modulo n.

a is called a primitive element (PE) if $\mathrm{ord}_n(a) = \varphi(n)$.

Idea:

$|\mathbb{Z}_n^*| = \varphi(n)$. If $a \in \mathbb{Z}_n^*$ is a PE mod n, then

$$\underset{\not\equiv 1}{a^1 \pmod{n}}, \underset{\not\equiv 1}{a^2 \pmod{n}}, \dots, \underset{\equiv 1}{a^{\varphi(n)} \pmod{n}} \in \mathbb{Z}_n^*$$

Suppose that $\exists\, 1 \le i < j \le \varphi(n) : a^i = a^j \pmod{n}$

Then $a^{j-i} \equiv 1 \pmod{n}$, a contradiction.

Hence, $\{a^1 \bmod n, a^2 \bmod n, \dots, a^{\varphi(n)} \bmod n\} = \mathbb{Z}_n^*$

$\mathbb{Z}_n^*$ is generated by powers of a.

Such groups are called cyclic. a is also called generator.

Problem: Is there always a PE mod n ?

Thinking the Future
Zukunft denken

Th. 7.2. a) There exists a PE mod n iff

$n \in \{2, 4, p^k, 2 \cdot p^k \mid p \geq 3 \text{ prime}, k \in \mathbb{N}\}$.

b) If a PE mod n exists, then there are $\varphi(\varphi(n))$ many. ⌋

Particularly, if $n = p$ prime, $\exists\, a \in \mathbb{Z}_p^* : \mathbb{Z}_p^* = \{a^k \mid k = 1, \ldots, p-1\}$.

Example. $n = 7$, $\varphi(n) = 6$. Determine all PE mod 7.

	powers mod 7
$a=2$	$2, 4, 8 \equiv 1 \pmod 7$ → no PE
$a=3$	$3, 9 \equiv 2 \pmod 7, 27 \equiv 6, 81 \equiv 4, 243 \equiv 5, 729 \equiv 1$ → PE
$a=5$	$5, 25 \equiv 4, 125 \equiv 6, 625 \equiv 2, 3125 \equiv 3, 15625 \equiv 1 \pmod 7$ → PE

It holds that $\varphi(\varphi(7)) = \varphi(6) = 2$.

Hence, 3,5 are the only PE mod 7.

Def. 7.4. Let a be a PE mod n, $y \in \mathbb{Z}_n^*$. There exists a unique $x \in \{0, 1, \ldots, \varphi(n) - 1\}$ with $y = a^x \pmod n$.

x is called the discrete logarithm of y.

Notation $x = \log_a y$ ⌋

Particularly, if $n = p$ prime, a PE mod p:

$$\forall y \in \mathbb{Z} \setminus \{0\}\ \exists!\, x \in \{0, \ldots, p-1\} : y \equiv a^x \pmod p.$$

Example (from above)

$n = 7, \ a = 5$

y	1	2	3	4	5	6
$\log_a y$	0	4	5	2	1	3

$y = a^x \bmod n$ (modular exponentiation) is a <u>one-way function</u>.

1. $a^x \bmod n$ can be efficiently computed. by the <u>square-and-multiply</u> method.

$y = a^{26}$ $\qquad 26 = \underline{1}\,\underline{1}\,\underline{0}\,1\,0$

$$(((a^2 \cdot a)^2)^2 \cdot a)^2 = a^{26}$$

Algorithm:

Let $x = (b_k, b_{k-1}, \ldots, b_1, b_0) = \sum_{i=0}^{k} b_i 2^i, \ b_k = 1$

(binary representation)

<u>Square-and-Multiply</u>

```
y := a mod n;
for i := k-1 downto 0 do begin
    y := y^2 mod n
    if b_i = 1 then y := y * a mod n
    end;
```

RWTH AACHEN UNIVERSITY

Number of multiplications: $\lfloor \log_2 x \rfloor + v(x) - 1$,
where $v(x)$ = no. of 1's in the binary representation.

2. For appropriate a and y, computing $\log_a y$ is considered computationally infeasible.
Overview of existing algorithms
Menezes et. al. p. 104–113 (Baby-step giant-step)
Stinson (02), p. 228 ff.

7.1. Diffie Hellman Key Distribution

Joint parameters
p prime, a PE mod p

A	B
secret $x \in \{1, \dots, p-2\}$	secret $y \in \{1, \dots, p-2\}$
compute $u = a^x \bmod p$	compute $v = a^y \bmod p$
v	u

Joint key: $v^x = a^{yx} \bmod p$ $\qquad$ $u^y = a^{xy} \bmod p$

$$K = a^{xy} \bmod p = a^{yx} \bmod p$$

Thinking the Future
Zukunft denken

- Generation of a, p, a PE mod p

Prop. 7.5. $p \geq 3$ prime, $p-1 = \prod_{i=1}^{k} p_i^{t_i}$.

a PE mod $p \iff a^{(p-1)/p_i} \not\equiv 1 \pmod{p}\ \forall i = 1, \dots, k$.

Application:

1. Choose a large random prime q until $p = 2q+1$ is a prime as well. (Miller-Rabin)

2. Choose randomly $a \in \{2, \dots, p-1\}$ until $a^2 \not\equiv 1 \pmod{p}$ and $a^q \not\equiv 1 \pmod{p}$.

For $p = 2q+1$ there are
$$\varphi(\varphi(p)) = \varphi(p-1) = \varphi(2) \cdot \varphi(q) = q-1$$

Hence,
$$P(\text{select a PE mod } p \text{ in step } 2) = \frac{q-1}{p-1} = \frac{q-1}{2q} \approx \frac{1}{2}.$$

Primes q such that $2q+1$ is also prime are called Sophie-Germain primes. (SG primes)

It is conjectured that
$$|\{p \mid p \text{ SG-prime}, p \leq N\}| \sim \frac{2 C_2 N}{(\log N)^2}$$

$C_2 \approx 0.66016\dots$

Hence, there are sufficiently many SG-primes.

Thinking the Future
Zukunft denken

- The opponent O knows $U = a^x \bmod p$, $V = a^y \bmod p$, a, p.
  If O is able to compute discr. logs, the protocol is broken.

- Diffie Hellman problem (DHP)
  Given p, a PE mod p, $a^x \bmod p$, $a^y \bmod p$
  Calculate: $a^{xy} \bmod p$.

  Open question: ~~Comp. dl~~
  Solving the DHP $\succ$ discr. logs ?

- Intruder-in-the-middle attack on the DH-system
  Let $p = 2q+1$, p, q prime, a PE mod p.
  Then $a^q = a^{(p-1)/2}$ has order 2, since

$$(a^{(p-1)/2})^2 \equiv a^{p-1} \equiv 1 \pmod p$$

(by Fermat's theorem)

$$\begin{array}{ccccc}
A & & O & & B \\
a^x \bmod p & \longrightarrow & a^{xq} \bmod p & \longrightarrow & a^{xq} \bmod p \\
a^{yq} \bmod p & \longleftarrow & a^{yq} \bmod p & \longleftarrow & a^y \bmod p
\end{array}$$

Joint key for A and B: $K = a^{xyq} \bmod p$
$= (a^q)^{xy}$

$K = (a^q)^{xy} \bmod p$ has only two possible values, namely a^q, a^{2q}

Oscar can try both as a key.

Important: authenticity of the exponentials $a^x \bmod p$, $a^y \bmod p$ → digital signatures.

7.2 Shamir's no-key protocol

Prop. 7.7. Let p prime, $a, b \in \mathbb{Z}_{p-1}^*$. Then

$$\forall m \in \mathbb{Z}_p : \quad m^{aba^{-1}b^{-1}} \equiv m \pmod p.$$

Proof. $a^{-1}, b^{-1} \in \mathbb{Z}_{p-1}^*$ exist.

$aa^{-1} \equiv 1 \pmod{p-1}$ and $bb^{-1} \equiv 1 \pmod{p-1}$, i.e.

$bb^{-1} = t(p-1)+1$ for some t.

$m \in \mathbb{Z}_p$

$$m^{aba^{-1}b^{-1}} \bmod p = (\underbrace{m^a \bmod p}_{c})^{bb^{-1}a^{-1}} \bmod p$$

$$= (\underbrace{c^{t(p-1)}}_{\equiv 1 \text{ (Fermat)}} \cdot c)^{a^{-1}} \bmod p = m^{aa^{-1}} \bmod p$$

$$\underset{\text{(same argument)}}{=} m \bmod p$$

∎

RWTH AACHEN UNIVERSITY

A sends a message to B:

1. a, p published as above

2. A and B choose secrete numbers $a, b \in \mathbb{Z}_{p-1}^*$

$A \to B$: $c_1 = m^a \bmod p$

$B \to A$: $c_2 = c_1^b \bmod p$

$A \to B$: $c_3 = c_2^{a^{-1}} \bmod p$

B decipher: $m = c_3^{b^{-1}} \bmod p$.