$\gcd(a,b) = x \cdot a + y \cdot b \qquad x, y \in \mathbb{Z}$

---

7 The discrete logarithm and Related Cryptosystems

The discrete log forms the basis of numerous cryptographic protocols, the most famous is the El Gamal Cryptosystem.

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

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

is called the order of a modulo n. a is called primitive element modulo n (PE), if $\operatorname{ord}_n(a) = \varphi(n)$.

Idea behind this definition:

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

$$\underbrace{a^1 \bmod n}_{\not\equiv 1}, \underbrace{a^2 \bmod n}_{\not\equiv 1}, \dots, \underbrace{a^{\varphi(n)} \bmod n}_{\equiv 1 \pmod{n}}$$

Suppose that $\exists\ 1 \le i < j \le \varphi(n)$ $a^i \equiv a^j \pmod{n} \in \mathbb{Z}_n^*$

Then $a^{j-i} \equiv 1 \pmod{n}$ ↯

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

$\mathbb{Z}_n^*$ is generated by powers of a. Such groups are called cyclic. a is called a generator.

Problem: Is there always a PE mod n?

Theorem 7.2 a) There exists a PE modulo n iff $n \in \{2, 4, p^k, 2 \cdot p^k \mid p \ge 3 \text{ is prime}, k \in \mathbb{N}\}$.

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

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

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

	powers mod 7
$a = 2$	$2, 4, 8 \equiv 1 \pmod 7$ $\to$ no PE
$a = 3$	$3, 9 \equiv 2, 2\cdot 3 = 6, 6 \cdot 3 \equiv 4, 4 \cdot 3 \equiv 5, 5 \cdot 3 \equiv 1 \pmod 7$ $\to$ P
$a = 5$	$5, 25 \equiv 4, 4 \cdot 5 \equiv 6, 6 \cdot 5 \equiv 2, 2 \cdot 5 \equiv 3, 3 \cdot 5 \equiv 1 \pmod 7$ $\to$ P

It holds that $\varphi(\varphi(7)) = \varphi(6) = |\{1, 5\}| = 2$

$= \varphi(2 \cdot 3) = \varphi(2) \cdot \varphi(3) = 1 \cdot 2 = 2$

Hence, 3 and 5 are the only PE

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

x is called the discrete logarithm of y. Notation: $x = \log_a(y)$

Particularly, if $n = p$ prime:

$\forall y \in \mathbb{Z} \setminus \{0\}\ \exists!\ x \in \{0, \dots, p-2\}$ $y \equiv a^x \pmod p$

$y = a^x \bmod n$ is a one-way function

1. $a^x \bmod n$ (modular exponentiation) can be efficiently computed by the square-and-multiply method.

Example $y = a^{26}$ $\to$ $26 = (11010)_2$ binary representation

$26 = 2 \cdot 13 + \boxed{0}$

$13 = 2 \cdot 6 + \boxed{1}$

$6 = 2 \cdot 3 + \boxed{0}$

$3 = 2 \cdot 1 + \boxed{1}$

$1 = 2 \cdot 0 + \boxed{1}$

$$\underbrace{\Big(\underbrace{\big(\underbrace{(\underbrace{a^2 \cdot a}_{a^3})^2}_{a^6}\big)^2 \cdot a}_{a^{13}}\Big)^2}_{a^{26}}$$

Alg: Let $x = (b_k, \ldots, b_1, b_0)_2 = \sum_{i=0}^{k} b_i \cdot 2^i$ $\quad b_k = 1$

Square-and-Multiply

```
Y ← a mod n          // b_k = 1
for i from k-1 down to 0 do
    Y ← Y^2 mod n
    if (b_i = 1) then
        Y ← Y · a mod n
    end if
end for
```

Number of multiplications: $\lfloor \log_2(x) \rfloor + \sum_{i=0}^{k-1} b_i$
(k squarings) (multiplications)

$\sum_{i=0}^{k-1} b_i$ represents the no. of 1's in the binary representation of x

2. For appropriate a and n, computing $\log_a(y)$ is considered computationally infeasible.

Overview of existing alg:

Menezes et al., p. 104-113

Stinson (02), p228 ff

Cohen et al ('06), chapter 19

7.1 Diffie-Hellman Key Distribution and Key Agreement (76)

Technique providing (unauthenticated) key agreement, allowing two parties to establish a shared (secret) key over an open channel.

- Initial setup: A prime p and a PE mod p $a \in \{2, \dots, p-1\}$ are selected and published.
- Protocol actions:

  A chooses a random secret $x \in \{2, \dots, p-2\}$, sends B: $u = a^x \bmod p$

  B chooses a random secret $y \in \{2, \dots, p-2\}$, sends A: $v = a^y \bmod p$

  B receives u, compute the shared key $K = u^y = (a^x)^y \bmod p$

  A receives v, " " " " $K = v^x = (a^y)^x \bmod p$

- Generation of a, p, a PE mod p:

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

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

Proof: Ex

Application:

1. Choose a large random number prime q until $p = 2q + 1$
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 $\varphi(\varphi(p)) = \varphi(\underbrace{p-1}_{2 \cdot q}) = \varphi(2) \cdot \varphi(q) = q - 1$

we have $q - 1$ PE

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

Remark: Primes p such that $2p+1$ is also prime are called Sophie-Germain primes (SG primes)

It is conjectured that

$$|\{p \mid p \text{ SG prime}, p \leq N\}| \sim \frac{2 \cdot C_2 \cdot N}{(\log N)^2}$$

with $C_2 \simeq 0.66016$

Hence, there are sufficiently many SG primes.

See http://primes.utm.edu/top20/page.php?id=2

$N = 2^{64} \Rightarrow$ Prob of finding SG primes $\approx 0{,}68‰ \approx \frac{1}{1491}$

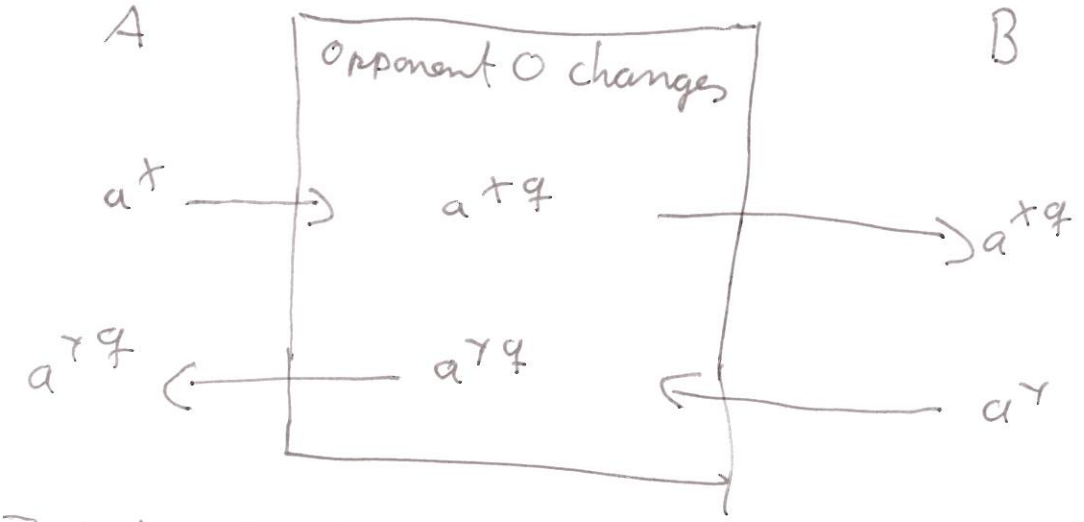
" " " ~~SG~~ " $2{,}25\% \approx \frac{1}{45}$

c.f. $|\{p \mid p \text{ prime}, p \leq N\}| \sim \frac{N}{\log(N)}$

• Intruder-in-the-middle attack on the DH system

Let $p = 2q+1$, p prime, q prime, a PE mod p

$a^q \equiv a^{(p-1)/2}$ has order 2, since $\left(a^{(p-1)/2}\right)^2 \equiv a^{p-1} \equiv 1 \pmod p$



Joint key for A and B: $K = a^{x \cdot y \cdot q} = (a^q)^{xy} \in \{-1, 1\}$

Oscar can try both keys.

<u>Important</u>: authenticity of the exponentials a^x, a^y

$\rightsquigarrow$ use digital signatures