# §3: The Discrete Log Problem & Public Key Encryption

## §3.1 Key exchange

### Merkle's Puzzles

1) Bob generates N keys
2) Bob encrypts a message
   "This is the $i$th key
   the key is $K_i$"
   w/ alg possible but
   hard to brute force.
3) Bob sends Alice all N keys
   Alice chooses 1 at random to decrypt.
4) Alice finds out $i$ and sends
   it to Bob.
5) Bob and Alice can use
   $K_i$ to communicate

Problem: want
easy enough that it
doesn't impose on
Alice

hard enough to dissuade
Eve

Can't get it asymmetric
enough.

## §3.2 Diffie-Hellman key exchange.

Invented by Ellis, Cocks, Williamson 1975

First published by D-H in 1976

Algorithm:

1) Choose large prime $p$ (256-bits)
   non-zero $g \in \mathbb{Z}/p\mathbb{Z}$
   invertible

2) Alice chooses secret $a \in \mathbb{Z}$
   Bob chooses secret $b \in \mathbb{Z}$.

3) Alice computes $A \equiv g^a \mod p$
   Bob $B \equiv g^b \mod p$

   publicly exchange these values.

4) Bob compute $B' \equiv A^b \mod p$
   Alice computes $A' \equiv B^a \mod p$.

   But, $B' \equiv A^b \equiv (g^a)^b \equiv (g^b)^a \equiv B^a \equiv A' \mod p$

5) Alice and Bob can use this 'shared secret' $A' = B'$ as their key.

1. Choose a large prime $p$, and a non-zero integer $g \in \mathbb{Z}/p\mathbb{Z}^{\times}$.
2. Alice chooses a secret integer $a$, and Bob chooses a secret integer $b$. Neither party reveals this integer to anyone.
3. Alice computes $A \equiv g^a \mod p$ and Bob computes $B \equiv g^b \mod p$, and they (publicly) exchange these values with each other.
4. Now Alice computes $A' \equiv B^a \mod p$ and Bob computes $B' \equiv A^b \mod p$.
5. $A' \equiv B' \mod p$, so Alice and Bob use this shared information as their key.

ex: $p = 29$

$g = 2$

$a = 7$

$b = 17$

$A = g^a = 2^7$

$= 128 \equiv 12 \mod 29$

$B = g^b = 2^{17}$

$\equiv 21 \mod 29$

$B^a = 21^7 \equiv 12 \mod 29$

$A^b = 12^{17} \equiv 12 \mod 29$

Shared secret $= 12$.

$p = 941$

$g = 627$

$a = 342$

$b = 781$

$A = 627^{342}$

$\equiv 390 \mod 941$

$B = 627^{781}$

$\equiv 691 \mod 941$

$A' = B^a = 691^{347}$

$\equiv 470 \mod 941$

$B' = A^b = 390^{781}$

$\equiv 470 \mod 941$

1. Choose a large prime $p$, and a non-zero integer $g \in \mathbb{Z}/p\mathbb{Z}^\times$.
2. Alice chooses a secret integer $a$, and Bob chooses a secret integer $b$. Neither party reveals this integer to anyone.
3. Alice computes $A \equiv g^a \mod p$ and Bob computes $B \equiv g^b \mod p$, and they (publicly) exchange these values with each other.
4. Now Alice computes $A' \equiv B^a \mod p$ and Bob computes $B' \equiv A^b \mod p$.
5. $A' \equiv B' \mod p$, so Alice and Bob use this shared information as their key.

Security of D-H

Q1) What do A, B have to do?

have to do large exponentiations

A1) $2^7$

$2^1 = 2$

4

8

16

32

64

$128 \equiv 99$

70

41

12

$O(p) = O(2^{\log p})$

A2)

$2^1 = 2$

4

8

16

$32 \equiv 3$

6

12

Keeps #s smaller

but still $O(p) = O(2^k)$

$(k = \log p)$

A3) $2^1 = 2$

$2^2 = 4$

$2^4 = 16$

$2^7 = 2^4 \cdot 2^2 \cdot 2^1 = 16 \cdot 4 \cdot 2 = 128 \equiv 12 \mod 29$.

total multiplications: 4

$2 \log_2(a) = O(\log_2(p)) = O(k)$.

Fast exponentiation

Algorithm:

Want: $g^a$.

1) $g^{2^k}$ for $2^k \le a$

i.e. $g, g^2, g^4, g^8, \dots$

2) write $a$ in binary

$a = c_0 + c_1 \cdot 2 + c_2 \cdot 2^2 + \dots + c_k 2^k$

$c_i \in \{0, 1\}$

3) $g^a = g^{c_0 + c_1 2 + c_2 2^2 + \dots + c_k 2^k}$

$= g^{c_0} (g^2)^{c_1} (g^{2^2})^{c_2} \dots (g^{2^k})^{c_k}$

$O(\log a) = O(k)$.

Want $627^{342} = 627^{256} \cdot 627^{64} \cdot 627^{16} \cdot 627^4 \cdot 627^2$

5 mults

• compute

$627$

$627^2$

$627^4$

$627^8$

$627^{16}$

$627^{32}$

$627^{64}$

$627^{128}$

$627^{256}$

8 squarings

Total: 13 steps

$342 = 256 + 64 + 16 + 4 + 2$

$p = 2^{\log_2 p}$

$p = O(2^{\log_2 p}) = O(2^k)$

Eve:

sees $A = g^a \bmod p$

$B = g^b \bmod p$

$g, p$

wants: $A^b \equiv B^a \bmod p$.

"obvious" attack: try to find $b$.

Discrete logarithm problem:

Given modulus $p$,

integers $g, A \in \mathbb{Z}/p\mathbb{Z}$,

find $x$ s.t. $g^x \equiv A \bmod p$.

<u>Think</u> that D-H is as secure as DL

How to solve DL?

compute $g, g^2, g^3, \ldots$

until get $A$.

expect to need $\approx \frac{p}{2}$

$O(p) = O(2^k)$

Shanks's Babystep-Giantstep algorithm

have $p, g, A$; want to find $x$ s.t. $g^x \equiv A \bmod p$.

1) $n = 1 + \lfloor \sqrt{p} \rfloor$

2) (Baby steps) compute

$$g^0, g^1, g^2, \ldots, g^n \bmod p$$ ($\sqrt{p}$ steps)

find inverse for $g^n \bmod p$ (easy-ish)

3) (Giant steps) compute

$$A, Ag^{-n}, Ag^{-2n}, \ldots, Ag^{-n^2} \bmod p$$ ($\sqrt{p}$ steps)

4) There is a # on both lists.

have $g^i \equiv A g^{-jn}$

5) $g^{i+jn} \equiv A \bmod p$.

$$O(\sqrt{p} \cdot \log p) = O(2^{k/2} \cdot k)$$

Pf this works:

If $g^x \equiv A \bmod p$

write $x = nq + r$ for $0 \le r < n$, $q \ge 0$

$$q = \frac{x-r}{n} < \frac{p}{n} < n$$

Then

$$g^{nq+r} \equiv A$$

$$g^r \equiv A g^{-nq}$$

shows up in BS

shows up in GS.

Solve $10^x \equiv 7 \bmod 23$

1) $n = 5$

2) $10^0 = 1$

$10^1 = 10$

$10^2 = 100 \equiv 8$

$10^3 \equiv 80 \equiv 11$

$10^4 \equiv 110 \equiv 18$

$10^5 \equiv 180 \equiv 19$

$19 \cdot (-6) \equiv 1 \bmod 23$

3) $7(-6)^0 = 7$

$7(-6)^1 = -42 \equiv 4$

$7(-6)^2 \equiv -24 \equiv 22$

$7(-6)^3 \equiv 6 \bmod 23$

$7(-6)^4 \equiv -36 \equiv 10$

$10^1 \equiv 7(-6)^4$

$\equiv 7(10^{-5})^4 \bmod 23$

$\equiv 7 \cdot 10^{-20} \bmod 23$

$10^{21} \equiv 7 \bmod 23.$

So $x = 21.$

1. let $n = 1 + \lfloor \sqrt{p} \rfloor$. Thus $n > \sqrt{p}$.
2. (Baby steps) Calculate $g^0, g^1, g^2, \ldots, g^n \mod p$. Find an inverse for $g^n \mod p$.
3. (Giant steps) Calculate $A, A \cdot g^{-n}, A \cdot g^{-2n}, \ldots, A \cdot g^{-n^2} \mod p$.
4. Find a match between these two lists, so that we have $g^i \equiv hg^{-jn}$.
5. Then $x = i + jn$ is a solution to $g^x \equiv h \mod p$.