IHC 2018 .CAMP
ITALIAN HACKER CAMP

THE DIFFIE-HELLMAN PROTOCOL IS WEAK FOR FERMAT PRIMES

SECRET-KEY CRYPTOGRAPHY

In a secret-key cryptosystem (or symmetric) the keys used in the encryption function and decryption function can be derived from each other.

EXAMPLES:

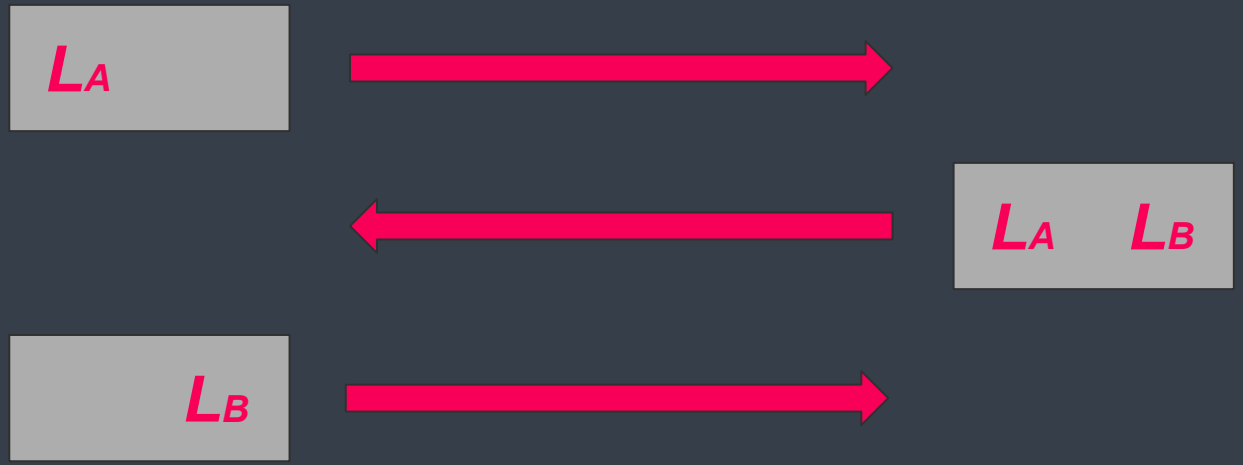
- Data Encryption Standard
- Caesar's cipher

PUBLIC-KEY CRYPTOGRAPHY

In a public-key cryptosystem (or asymmetric) there are two keys:

- a public key, to encrypt data
- a secret key, to decrypt data

THE DOUBLE PADLOCK PROTOCOL



- In **1976** the paper "*New Directions in Cryptography*" (Diffie W., Hellman M.) about public key cryptography was published

- In **1978** the paper "*An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Significance*" (Pohlig S., Hellman M.) was published

CYCLIC GROUP

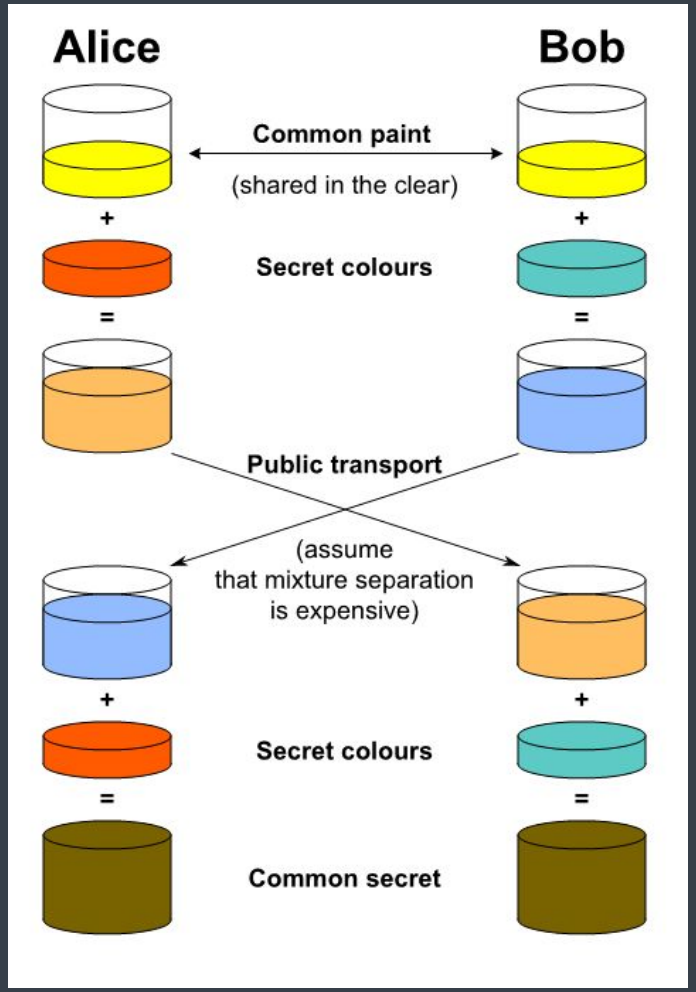
A **group** is a set **G** together with a binary operation which satisfies four requirements: *closure*, *associativity*, *identity element* and *inverse element*.

A **cyclic group** is a group generated by a single element, called *group generator*.

DIFFIE-HELLMAN KEY EXCHANGE

Alice and Bob choose a group **G** of order *n* and a generator *g*.

- Alice chooses a random $a \in \{0, \ldots, n-1\}$ and sends g^a to Bob
- Bob chooses a random $b \in \{0, \ldots, n-1\}$ and sends g^b to Alice
- Alice and Bob can calculate the common value g^{ab}


Alice
Bob
Common paint
(shared in the clear)
+
+
Secret colours
=
=
Public transport
(assume
that mixture separation
is expensive)
+
+
Secret colours
=
=
Common secret

IHC 2018 .CAMP
ITALIAN HACKER CAMP

THE DISCRETE LOGARITHM

The *discrete logarithm* of *x* to the base *g* is the smallest positive integer *a* such that $x = g^a$. Thus $log_g(x) = a$.

THE DIFFIE-HELLMAN PROBLEM

The *Diffie-Hellman problem* in a cyclic group **G** with generator *g* is to find *z* = g^{ab}, given *x* = g^a and *y* = g^b.

If an eavesdropper can solve the discrete logarithm problem, then he or she can solve the Diffie-Hellman problem.

In a cyclic group **G** of order *n* with generator *g*, the discrete logarithm problem of an element *x* to the base *g* can be solved by using less than **n** group operations.

So a requirement for the Diffie-Hellman key exchange is that **n must be big**.

POHLIG-HELLMAN: PREREQUISITES

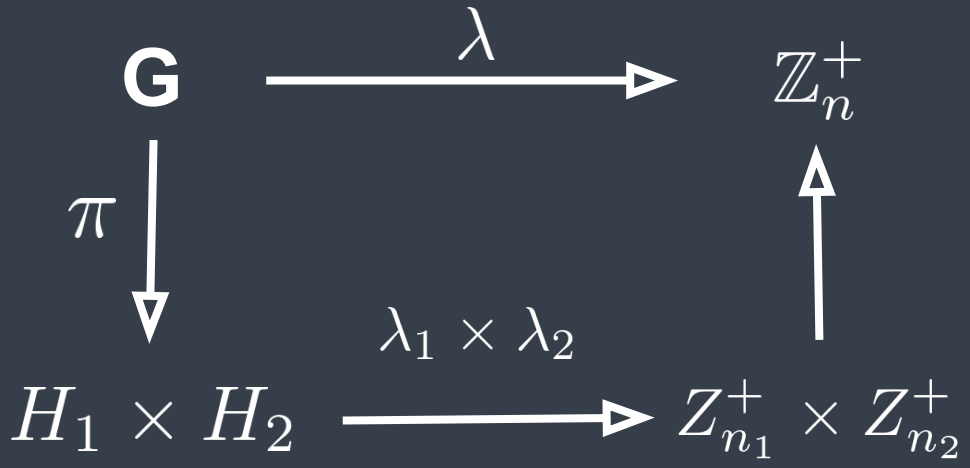
- Any cyclic group **G** of order *n* is isomorphic to $\mathbb{Z}_n^+$. To compute the discrete logarithm to the base *g* is equivalent to compute the isomorphism $\lambda : G \to \mathbb{Z}_n^+$ such that $\lambda(g) = 1_n$

- $n = n_1 n_2$, n_1 and n_2 coprime. Let $H_1 = \{x^{n_2} | x \in G\}$ and $H_2 = \{x^{n_1} | x \in G\}$ be two subgroups of **G** of order n_1 and n_2. Define the group homomorphisms

$$\pi_i : G \to H_i, \pi_1(x) = x^{n_2}, \pi_2(x) = x^{n_1}$$

Then $\pi : G \to H_1 \times H_2, \pi(x) = (\pi_1(x), \pi_2(x))$ is a group isomorphism

- The diagram is commutative



POHLIG-HELLMAN: PART ONE

Let **G** be a cyclic group of order $n = n_1 n_2$, n_1 and n_2 coprime. Let H_1 and H_2 be the subgroups of order n_1 and n_2. The discrete logarithm of a group element *x* can be computed **as fast as** the discrete logarithm of one element in the subgroup H_1 and one element in the subgroup H_2.

This result can be generalized to $n = \prod_{i=1}^{l} p_i^{r_i}$

So another requirement for the Diffie-Hellman key exchange is that **the largest prime tower dividing the order of G must be big**.

POHLIG-HELLMAN: PART TWO

Let **G** be a cyclic group of order $n = p^r$, *p* prime. The discrete logarithm of an element *x* can be computed **as fast as r** discrete logarithms in the subgroup of order *p*.

The last requirement for the Diffie-Hellman key exchange is that **the largest prime dividing the order of G must be big**.

IHC 2018 .CAMP
ITALIAN HACKER CAMP

HOW DOES POHLIG-HELLMAN ALGORITHM WORK?

$$y = g^x \pmod{p}, \quad \varphi(p) = p - 1 = \prod_{i=1}^{l} p_i^{r_i}$$

$$x \pmod{p_1^{r_1}}, \ldots, x \pmod{p_l^{r_l}}$$

CRT

$$x \pmod{\varphi(p)}$$

$$x_i = x \pmod{p_i^{r_i}}$$

- $x_i = \sum_{j=0}^{r_i-1} c_j p_i^j,\ c_j \in \{0, \ldots, p-1\} \forall c_j$
- $y^{\frac{(p-1)}{p_i}} = g^{\frac{c_0(p-1)}{p_i}} \pmod{p}$
- $y_j^{\frac{(p-1)}{p_i^{j+1}}} = g^{\frac{c_j(p-1)}{p_i}} \pmod{p}$

CHINESE REMAINDER THEOREM

Let $p_1, \ldots, p_r$ be pairwise coprime. Then the system of congruences

$$x = c_i \pmod{p_i} \; for \; i \in \{1, \ldots, r\}$$

has a **unique** solution $x \pmod{p}$, where $p = \prod_{i=1}^{r} p_i$

SAFE PRIME

A **safe prime** is a prime of the form **2p+1**, where **p** is a prime.

A cyclic group of order **n = 2p+1**, where **n** and **p** are “big enough” primes, is a suitable group for the Diffie-Hellman protocol.

FERMAT NUMBER

A **Fermat number** is a number of the form $F_n = 2^{2^n} + 1$.

Even if F_n is a prime, it is **not** a safe prime, so the multiplicative group of integers mod F_n is **not** a satisfactory group for Diffie-Hellman key exchange.

17 - $\mathbb{F}_2 = 2^{2^2} + 1$

$$8 = 3^x \pmod{17}\ ,\ x = \sum_{i=0}^{3} c_i 2^i\ ,\ c_i \in \{0, 1\}$$

- $8^{2^3} = 1 = 3^{c_0 2^3} \pmod{17} \rightarrow c_0 = 0$
- $8^{2^2} = 16 = 3^{c_1 2^3} \pmod{17} \rightarrow c_1 = 1$
- $16^2 = 1 = 3^{c_2 2^3} \pmod{17} \rightarrow c_2 = 0$
- $16 = 3^{c_3 2^3} \pmod{17} \rightarrow c_3 = 1$

IHC 2018 .CAMP
ITALIAN HACKER CAMP

BIBLIOGRAPHY