Lecture 6 Discrete Log Problem & Diffie-Hellman key exchange

§2.1 – 2.3

Discrete log problem

Let p be a prime. Let $g \in \mathbb{F}_p$ be a generator / a primitive root.

So $\mathbb{F}_p^\times = \{ g^0, g^1, \dots, g^{p-2} \}$

$\exp_g(n) = g^n$, $\log_g(g^n) = n \in \mathbb{Z}/(p-1)$

The discrete log problem is the problem of finding $\log_g(h)$ for $g, h \in \mathbb{F}_p^\times$.

Ex In $\mathbb{F}_{11}$, find $\log_2(7)$.

$2^0 = 1$ $2^3 = 8$ $2^6 = 20 = 9$

$2^1 = 2$ $2^4 = 16 = 5$ $2^7 = 18 = 7$

$2^2 = 4$ $2^5 = 10$

$\Rightarrow \log_2(4) = 7.$

Rmk The log problem makes sense in any group G. if $g \in G$ is some element & $\mathrm{ord}(g) = d$ then

$$\log_g : \{ g^0, g^1, \dots, g^{d-1} \} \longrightarrow \mathbb{Z}/d$$

(G is the union of these elements)

is the log of G. Note though that in general not every elt of the gp can be written as a power of g.

ex (1) $G = ((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$ our previous example.

(2) $G = (\mathbb{Z}/m\mathbb{Z}, +)$.

"g^n" $= \underbrace{g + \cdots + g}_{n \text{ times}} = ng.$

The logarithm here is easy.

(3) Later in this class: G coming from an elliptic curve.

This has a harder log problem than $\mathbb{F}_p^\times$.

Diffie Hellman Key exchange

Goal: To decide on a secret key k over a public channel. Can then use k for symmetric encryption.

Everyone publically agrees on a prime p & a generator g of $\mathbb{F}_p^\times$.

Alice

Pick $a \in \mathbb{Z}/(p-1)\mathbb{Z}$

Compute $A = g^a \in \mathbb{F}_p^\times$ —send to Bob→

Bob

Pick $b \in \mathbb{Z}/(p-1)\mathbb{Z}$

←send to Alice— Compute $B = g^b \in \mathbb{F}_p^\times$

Compute $B^a = (g^b)^a = g^{ab}$

Compute $A^b = (g^a)^b = g^{ab}$.

Now Alice & Bob have a shared secret

g^{ab}.

Ex $g = 2$ in $\mathbb{F}_{11}$.

Alice

Pick $a = 2$

$\rightsquigarrow A = g^a = 2^2 = 4$ ⟶

Bob

Pick $b = 3$

⟵ $B = g^b = 2^3 = 8$

$B^a = 8^2 = 9 \pmod{11}$

$A^b = 4^3 \equiv 9 \pmod{11}$

Rmk Key exchange is not a public key cryptosystem.

But we can use DLP for public key cryptography too.

Eve's perspective

Know $A = g^a$ & $B = g^b$

Want g^{ab}

If Eve can solve DLP then she knows a, b

$\rightsquigarrow$ computes g^{ab}.

What Eve really needs :3:

Problem (Diffie Hellman problem)

Given g^a & g^b find g^{ab}.

DLP $\geq$ DHP

↳ Discrete log problem is at least as hard as Diffie-Hellman problem.

A third variant

Problem (Decision Diffie-Hellman Problem DDP)

Given g^a, g^b, & C decide if $g^{ab} = C$.

$$DLP \geq DHP \geq DDP.$$

Elgamal Public Key Cryptography

Fix p, $g \in \mathbb{F}_p^\times$ a generator.

Alice

Pick private key

$a \in \mathbb{Z}/(p-1)\mathbb{Z}$

Compute public key

$A = g^a \in \mathbb{F}_p^\times$ ⟶

Bob

Plaintext $m \in \mathbb{F}_p^\times$

Pick random

$k \in \mathbb{Z}/(p-1)\mathbb{Z}$

Compute

$c_1 = g^k$

$c_2 = mA^k$ ⟵

⟵ c_1

Compute $c_2 \cdot c_1^{-a} = c_2 \cdot g^{-ak}$

$= c_2 A^{-k}$

$= m.$