HW due: Thursdays

Desirata

$$\begin{tikzcd} \text{Domain} \arrow[r, bend left, "f \text{ easy}"] & \text{Range} \arrow[l, bend left, "f^{-1}_{\text{hard}}"] \arrow[l, bend left=60, "f^{-1} \text{ w/ extra info}"] \end{tikzcd}$$

$e_{k_{pub}}$ public c m

f^{-1} w/ extra info — easy, k_{priv}

History

* Formalism came from Diffie-Hellman (DH '76)
* Merkle undergrad CS major @ Berkeley equivalent to DH (earlier) 60s
* Elgamal turned DH into a PKC in 85
* RSA '78 '73 Rivest, Shamir, Adleman

Intelligence Community (classified)

Discrete Log Problem

Let p be prime. Consider $\mathbb{F}_p$.

$g \in \mathbb{F}_p$ a primitive root so $\forall\, h \in \mathbb{F}_p^*$ are a power of g.

$$\mathbb{F}_p^* = \{1, g, g^2, g^3, \dots, g^{p-2}\}$$

Def^n The discrete log problem (DLP) is the problem of solving

$$g^x \equiv h \mod p$$

for x. The solution is called the discrete log base g of h &

$$x = \log_g(h)$$

Rmk ① Same idea as log in $\mathbb{R}$.

② Warning: we use $\log_2 a$ a lot in time complexity ← $\mathbb{R}$-log

Collision of notation

* $a, 2 \in \mathbb{F}_p^*$ ⇜ discrete
* $a, 2 \in \mathbb{R}$ ← regular.

③ i) Is $\log_b$ well defined?
ii) Where does it take values?

Guess Values in $\mathbb{Z}$

What goes wrong?

$$x = \log_b(h)$$

$$b^x \equiv h \mod p$$

$$\Longrightarrow b^{x+(p-1)} = b^x \cdot b^{p-1} \quad \leftarrow 1 \text{ by Fermat}$$

$$\equiv b^x \equiv h \mod p$$

In fact

$$\underset{\substack{|||\\ x \mod p-1}}{x + k(p-1)} = \log_b h$$

Lemma: $g \in \mathbb{F}_p$ primitive

$$g^a \equiv g^b \mod p$$

Then $a \equiv b \mod p-1$

Pf/ HW

Putting together

$h \in \mathbb{F}_p^*$ $g \in \mathbb{F}^*$ primitive

① $\exists\ x = \log_g h$

② If x, y are both $\log_g h \Rightarrow x \equiv y \mod p-1$

So

$$\log_b : \mathbb{F}_p^* \xrightarrow{\;\;} \mathbb{Z}/(p-1)\mathbb{Z} \qquad (b^x)$$

So

$$\log_b(h) = \begin{pmatrix} \text{the unique } x = 0, \dots, p-2 \text{ s.t.} \\ b^x \equiv h \mod p \end{pmatrix}$$

④ $a, b \in \mathbb{F}_p^*$

$$\log_g(ab) = \underbrace{\log_g a + \log_g b}_{+ \text{ in } \mathbb{Z}/(p-1)}$$

HW

⑤ In $\mathbb{C}$. $e^{2\pi i} = 1$

$$\underset{2\pi i}{\underset{/\!/}{\ln(e^{2\pi i})}} = \underset{0}{\ln 1} \qquad ??$$

Example $(\mathbb{Z}/7\mathbb{Z})^* = \{1, 2, 3, 4, 5, 6\}$

$g=3$	3^0	3^1	3^2	3^3	3^4	3^5
	1	3	2	6	4	5

$\log_3(6) = 3$
$\log_3(5) = 5$

Example (DLP is hard)

$p = 56509$ $g = 2$

$\log_2 38647$

$2^2, 2^3, 2^4, 2^5 \mod p$

$\dots\ 2^{11235} \equiv 38647 \mod p$

ok $\log_2 38647 = 11235$

$\mathbb{R}$ log. Tin

$\sim \log_2 2 + \log_2 3 + \dots + \log_2 11235$

$\mathbb{F}p(2)$

$$= \log_2(11235!)$$

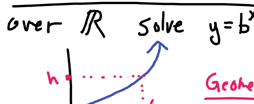
steps ($\mathbb{R}$)

Show Naive computation of $\log_g h$ mod p up to $\sim \mathbb{R}\log_2((p-2)!)$

Grows fast!

Is there a better way?

over $\mathbb{R}$ solve $y = b^x$



Not so clear / $\mathbb{F}_p$

(Graphs in calc)

Assume DLP is hard

Build our first cryptosystem

Diffie-Hellman Key Exchange

Alice & Bob communicate a secret key to eachother over a Public channel

(Eve hears anything they say to eachother)

DHKE

Step 1 Alice & Bob decide on p & $g \in \mathbb{F}_p^*$

(p, g public)

Step 2

Alice chooses secret $a \in \mathbb{Z}$ ← only Alice knows

& computes $A \equiv g^a \mod p$

Bob " " $b \in \mathbb{Z}$ ← only Bob knows

" " $B \equiv g^b \mod p$

Step 3

$$\begin{tikzcd} \text{Alice} \arrow[r, bend left, "A"] & \text{Bob} \arrow[l, bend left, "B"] \end{tikzcd}$$

Eve intercept A & B

Step 4

Alice computes $A' \equiv B^a \mod p$

Bob " $B' \equiv A^b \mod p$

Fact $A' \equiv B' \mod p$

Pf/

$$A' \equiv B^a \equiv (g^b)^a = g^{ab} = (g^a)^b \equiv A^b \equiv B' \mod p$$

If we call $K = A' = B'$

Alice & Bob share secret $K \in \mathbb{F}_p^*$

Can use this for

$$\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{F}_p^*$$

$$e_K(m) = Km \mod p$$

Rmk For p small Eve can guess & check DLP.

But for $p \sim 2^{1000}$ we're safe.

Def^n The Diffie-Hellman Problem (DHP) is the problem of finding $g^{ab} \mod p$ know $g^a \mod p$ & $g^b \mod p$

Slogan The DLP is at least as hard as the DHP.

Precisely

If I solve DLP

$\Longrightarrow$ I solve DHP.

Pf/ Know $g^a \mod p$, $g^b \mod p$

Solution to DLP gives $a = \log_g g^a$.

Compute $(g^b)^a \equiv g^{ab} \mod p$

Question

Does a soln to DHP $\Longrightarrow$ a soln to DLP?

Open Problem

Rmks Not a PKC

Bob doesn't share a secret w/ Alice.

Bob & Alice co create a secret.

Bob doesn't know a

Alice " " b

Further Bob has no control over a so no control over $K = g^{ab}$

← The secret. (not a message).