Remark:

Fast Power Slow

1 step $A \to \lfloor A/2 \rfloor$ floor

① A = math.floor(A/2)

Not an integer

A float ← only 64 bits

Can't remember huge #s (64 binary sig figs)

Lose info for HUGE #s $> 2^{64}$

BAD

② A = A//2

integer division

(returns q from $A = 2q + r$)

Avoid rounding errors.

GOOD!

Correction (last thursday)

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

Find $\log_g h = $ (the x s.t. $g^x = h$)

Could

$g, g^2, g^3, \dots, g^x = h$ ← done!

$\log_2(1) + \log_2(2) + \dots + \log_2(x)$

Know g^n → Fast Power (g^{n+1}) $\log_2(n+1)$

Want g^{n+1} → $g^n \times g$ ← 1 step

~~$\log_2(x!)$~~ ← x steps.

$x \approx p \approx 2^{80}$

too long.

Recall DHP

Fixed p, $g \in \mathbb{F}_p^*$ ← public

Alice	Eve	Bob
secret a		secret b
g^a →		← g^b mod p
g^{ba}		g^{ab} ← k

Shared secret

Not a PKC

Bob can't control a

so can't control secret.

g^{ab} not a message.

Recall A PKC

Alice Publishes

$(\mathcal{M}, \mathcal{C}, \mathcal{K}, e, d, k_{pub})$

Alice keeps k_{priv} secret.

Bob computes $e(k_{pub}, m)$ ← public "c"

Alice can compute $d(k_{priv}, c) = m$

Elgamal (1985)

Alice

1) prime p. $g \in \mathbb{F}_p^*$ Public

k_{priv} 2) Secret $a \in \mathbb{Z}$ Private

k_{pub} 3) Computes $A \equiv g^a \bmod p$ Public

Bob:

1) $m \in \mathcal{M} = \{1, 2, \dots, p-1\} \subset \mathbb{F}_p^*$

2) Choose random $k \in \mathbb{Z}/(p-1)\mathbb{Z}$ $k = \{1, \dots, p-2\}$

i) Keep k secret

ii) Only use for one message

3) Bob computes ciphertext

$c_1 = g^k \bmod p$

$c_2 = m A^k \bmod p$

Sends to Alice. $m \cdot k$

Alice's Decryption

1) $x = (c_1^a)^{-1} \bmod p$ k^{-1}

i) c_1^a Fast Power

ii) Invert → Ext E.A. → Fast Power + Fermat

2) Computes $y \equiv c_2 \cdot x \bmod p$

Claim $y \equiv m \bmod p$

Pf/ $y \equiv x \cdot c_2 \bmod p$

$\equiv (c_1^a)^{-1} \cdot c_2 \bmod p$

$\equiv (g^{ak})^{-1} m A^k \bmod p$

$\equiv (g^{ak})^{-1} m (g^{ak}) \bmod p$

$\equiv m \bmod p$

Example $p = 467$, $g = 2$

Alice	Eve	Bob
$a = 153$		
$A = g^a = 2^{153} \equiv 224$		$m = 331$
		Random $k = 197$
		$c_1 = 2^{197} \equiv 87$
		$c_2 = 331 \cdot A^k = 331 \cdot 224^{197} \equiv 57$
$(c_1^a)^{-1} = c_1^{p-1-a} = 87^{313} \equiv 14$		
$c_2 \cdot 14 = 57 \cdot 14 = 331$.		

Remark

$\mathcal{M} = \mathbb{F}_p^* \ni m$ But

$\mathcal{C} = \mathbb{F}_p^* \times \mathbb{F}_p^* \ni (c_1, c_2)$

Storage space

$\mathcal{C}$ is twice as large

"2:1 message expansion"

Question Is Elgamal as hard as DH?

"Oracle Proof"

CS_A, CS_B ← 2 crypto systems

I have access to a CS_A oracle

Can I use this oracle to break CS_B

→ Decode any CS_A cipher immediately.

Prop

Fix p & $g \in \mathbb{F}_p^*$. Supp you have access to an Elgamal Oracle who can decrypt an (c_1, c_2) into a message. Then you can solve DHP.

Pf/ Know $A \equiv g^a \bmod p$, $B \equiv g^b \bmod p$

Want g^{ab}

Give Elgamal oracle $A, (c_1, c_2)$ get $m = (c_1^a)^{-1} c_2$

Give $c_1 = g^b$, $c_2 = 1$

$(c_1^a)^{-1} c_2 = (g^{ba})^{-1}$. invert to get g^{ab} ✓

Get $(g^{ba})^{-1} \cdot c_2$ multiply by c_2^{-1} & invert to get g^{ab}

Solving Elgamal solve DHP so Elgamal "harder"

HW DHP oracle solves Elgamal!

"Same level of hardness"

A crash course in Groups

Properties of mult in $\mathbb{F}_p^*$

Identity 1) $\exists\, 1 \in \mathbb{F}_p^*$ & $1 \cdot a = a$ any $a \in \mathbb{F}_p^*$

Inverse 2) any $a \in \mathbb{F}_p^*$ there is (unique) $a^{-1} \in \mathbb{F}_p^*$ & $a \cdot a^{-1} = 1 = a^{-1} \cdot a$

Associa 3) $a(bc) = (ab)c$

Commute 4) $ab = ba$

$\mathbb{Z}/n\mathbb{Z}$ with addition

Identity 1) $\exists\, 0 \in \mathbb{Z}/n\mathbb{Z}$ s.t. $a + 0 = a$ any $a \in \mathbb{Z}/n\mathbb{Z}$

Inverse 2) $a \in \mathbb{Z}/n\mathbb{Z}$ $\exists$ unique $-a$ s.t. $a + -a = 0 = -a + a$

Assoc 3) $a + (b + c) = (a + b) + c$

comm 4) $a + b = b + a$

Example

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

$g^a \cdot g^b = g^{a+b}$ FLT mod $p-1$

$\mathbb{Z}/(p-1)\mathbb{Z} = \{0, 1, 2, \dots, p-2\}$

$a + b \equiv a + b \bmod p-1$.

$g^2 g^3 = g^5$ $2 + 3 = 5$

"Up to relabeling these are the same"

$\log_g : \mathbb{F}_p^* \xrightarrow{\sim} \mathbb{Z}/(p-1)\mathbb{Z}$

witnesses sameness.

Groups = the type of thing that these are the "same" of.

Def G a set. $*$ is a rule for combining pairs of elts in G. $a, b \in G \Rightarrow a * b \in G$. (binary operation)

G is a group if the followings laws hold.

Identity 1) $\exists\, e \in G$ s.t. $e * a = a * e = a$ any $a \in G$

Inverse 2) Any $a \in G$ there is a (unique) $a^{-1} \in G$ s.t. $a * a^{-1} = e = a^{-1} * a$

Assoc 3) $a * (b * c) = (a * b) * c$

If also 4) $a * b = b * a$

$\Rightarrow G$ is commutative group or Abelian group.

Examples

$*$ = mult.

1) $G = \mathbb{F}_p^*$. $e = 1$. inverse of a is a^{-1}

If G is finite it is called a finite Group. The $\#G = |G| =$ order of G.

1) $|\mathbb{F}_p^*| = p - 1$

2) $\mathbb{Z}/n\mathbb{Z}$. $* = +$. $e = 0$ inverse of $a = -a$

$|G| = |\mathbb{Z}/n\mathbb{Z}| = n$.

3) $G = \mathbb{Z}$. $* = +$. $e = 0$ inverse a $-a$.

$\mathbb{Z}$ is infinite

4) $G = \mathbb{Z}$ $*$ = mult. $e = 1$

NOT A GROUP. No 2^{-1}

5) $G = \mathbb{R}$. $*$ = mult $e = 1$

NOT A GROUP $1 \cdot a = a$

But no 0^{-1}

$0 \cdot a = 0 \neq 1$.

6) $G = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$

$*$ = mult.

$a^{-1} = a^{-1}$ $e = 1$ ✓

Infinite group.