

Remark:

Fast Power Slow  
1 step  $A \rightarrow [A/2]$

①  $A = \text{math.floor}(A/2)$   
A float  $\leftarrow$  only 64 bits  
can remember huge #'s  
(64 binary sig figs)

Lose info for huge #'s  $> 2^{64}$   
BAD

②  $A = A//2$   
integer division  
(returns  $y$  s.t.  $A = zg+r$ )  
Avoid rounding errors.  
GOOD!

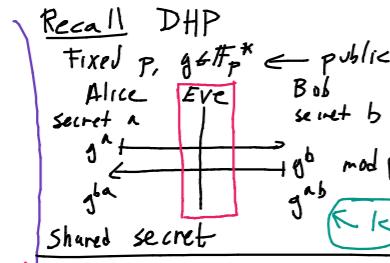
Correction (last thursday)

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

Find  $\log_g h = (\text{the } x \text{ s.t. } g^x = h)$   
Could  
 $g, g^2, g^3, \dots, g^x = h \leftarrow \text{done!}$

$\log_2(1) + \log_2(2) + \dots + \log_2(n)$   
know  $g^n \rightarrow \text{Fast Power}(log)$   
Want  $g^{n+1} \rightarrow \text{Fast Power}(log(n+1))$   
 $\log(x!) \leftarrow x \text{ steps.}$

$x \approx p \approx 2^{80}$   
too long.



Not a PKC  
Bob can't control  $a$   
so can't control secret.  
 $g^{ab}$  not a message.

Recall A PKC

Alice Publishes

$(m, C, K, e, d, k_{\text{pub}})$

Alice keeps  $k_{\text{priv}}$  secret.  
Bob computes  $e(k_{\text{priv}}, m)$   $\leftarrow$  public  
Alice can compute  
 $d(k_{\text{priv}}, c) = m$

Elgamal (1985)

Alice

1) prime  $P$ .  $g \in \mathbb{F}_p^*$  Public  
2) Secret  $a \in \mathbb{Z}$  Private  
3) Computes  $A \equiv g^a \text{ mod } P$  Public

Bob: 1)  $m \in \mathbb{Z}$   
 $= \{1, 2, \dots, P-1\} \subset \mathbb{F}_p^*$   
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

$$\begin{aligned} C_1 &\equiv g^K \text{ mod } P \\ C_2 &\equiv m A^K \text{ mod } P \\ \text{Sends to Alice. } m \cdot k \end{aligned}$$

Alices Decryption

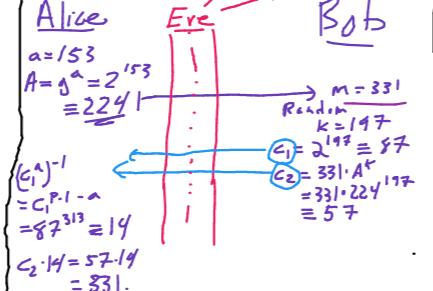
- 1)  $X = (C_1^a)^{-1} \mod P$
- i)  $C_1^a$  Fast Power
- ii) Invert  $\rightarrow$  Ext E.A  $\rightarrow$  Fast Power + Format
- 2) Computes  $y \equiv C_2 \cdot X \mod P$

Claim

$$y \equiv m \mod P$$

$$\begin{aligned} \text{Pf: } y &\equiv X \cdot C_2 \mod P \\ &\equiv (C_1^a)^{-1} \cdot C_2 \mod P \\ &\equiv (g^{ab})^{-1} m A^k \mod P \\ &\equiv (g^{ab})^{-1} m (g^{ak}) \mod P \\ &\equiv m \mod P \quad \text{QED} \end{aligned}$$

Example  $P=67$ ,  $g=2$



Remark

$$\begin{aligned} m &\in \mathbb{F}_p^* = m \text{ but} \\ C &= \mathbb{F}_p^* \times \mathbb{F}_p^* \ni (c_1, c_2) \end{aligned}$$

Storage space

$$\begin{aligned} C &\text{ is twice as large} \\ &\text{"2-1 message expansion"} \end{aligned}$$

Question Is Elgamal as hard as DHP?  
"Oracle Proof"

CSA, CSB  $\leftarrow$  2 crypto systems

I have access to a CSA oracle  
Can I use this oracle to break CSB?

Decode any CSA 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  $A \equiv g^a \mod P$   
 $B \equiv g^b \mod P$   
Want  $g^{ab}$

Give Elgamal oracle  
 $A, (C_1, C_2) \rightarrow m = (C_1^a)^{-1} C_2$

Given  $c_1 = g^b$   $c_2 = ?$   
 $(c_1^a)^{-1} \cdot c_2 = (g^{ba})^{-1}$   
invert to get  $g^{ab}$  ✓

Get  $(g^{ba})^1 \cdot C_2$   
multipl by  $c_1^b$  & 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  $a^{-1}$

$a^{-1} \in \mathbb{F}_p^*$  &  $a \cdot a^{-1} = 1 = a^{-1} \cdot a$

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

Commutativity 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.  $a + -a = 0 = -a + a$

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

Commutativity 4)  $a+b=b+a$

Example

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

$$\begin{aligned} g^a \cdot g^b &= g^{a+b} \mod p-1 \\ \text{FLT mod } p-1 \end{aligned}$$

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

$$a+b \equiv ab \mod p-1$$

$$g^3 \cdot g^5 = g^8 \equiv 5$$

$z+3=5$   
Up to relabeling these are the same

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

witnesses smartness.

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

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

$G$  is a group if the following laws hold.

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

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

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

Identity 4)  $a * b = b * a$

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

Examples  $* = \text{mult}$ .  
 $e = 1$ . inverse of  $a$  is  $a^{-1}$

1)  $G = \mathbb{F}_p^*$ .  $e = 1$ . inverse of  $a$  is  $a^{-1}$ .  
 $\mathbb{Z}/n\mathbb{Z}$  is finite it is called a finite group. The # of elements is  $|G|$  = order of  $G$ .

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

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

$\mathbb{Z}$  is infinite  
NOT A GROUP. No  $z^{-1}$

4)  $G = R$ .  $* = \text{mult}$   $e = 1$

NOT A GROUP.  $1 \cdot a = a$  But no  $a^{-1}$ .  $0 \cdot a = 0 \neq 1$ .  
 $a \cdot a^{-1} = 1$

5)  $G = \mathbb{R}^*$   $= \mathbb{R} \setminus \{0\}$   
 $* = \text{mult}$

$a \cdot a^{-1} = 1$

Infinite group.