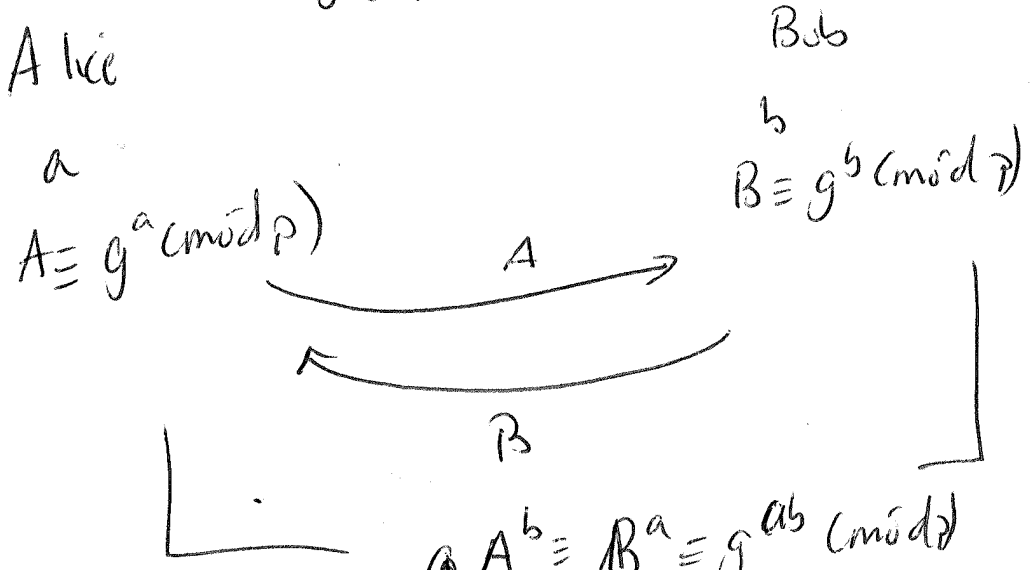
DLP:
dado g, h, p hayar x t.q $g^x \equiv h \pmod p$

DHP:
dado ~~g^a~~ $g, P,$

DH: g y p públicos.



ElGamal (1985) > No es tal prime PKC (históricamente) pero tiene el DLP combinado
> se puede generalizar para cualquier grupo

Procedemos ~~despacio~~ con cuidado. Para un PKC en general:

Alice publica: { clave - un número
algoritmo - una manera para cifrar un mensaje usando la clave (usada por Bob)

Alice mantiene secreta la clave ~~pública~~ privada

Para ElGamal:

Alice elige
- Alice precisa un primo p para que el DLP sea difícil
- Alice precisa un elemento de g módulo p de orden grande y primo

Alice calcula una empresa de seguridad los calcula y los vende a Alice

- Alice elige un número a (secreto) que será su clave privada.
- Alice calcula $A \equiv g^a \pmod{p}$
- Alice publica A como su clave pública.
- Bob escribe su mensaje y lo codifica como un número módulo p.
- Bob elige aleatoriamente otro número k módulo p y lo usa para cifrar un mensaje y solo un mensaje. Lo k se llama una clave efímera
- Bob calcula $c_1 \equiv g^k \pmod{p}$ $\quad c_2 \equiv mA^k \pmod{p}$
- Bob manda (c_1, c_2) a Alice.

"Alice, para descifrar el mensaje calcula:

$$X^{-1} \text{ donde } X \equiv C_1^a \pmod p$$
$$\equiv g^{ka}.$$

O sea, x^{-1} es el inverso de A módulo p. Entonces

$$X^{-1} \cdot C_2 \equiv (C_1^a)^{-1} \cdot C_2$$
$$\equiv (g^{ak})^{-1} m A^k$$
$$= (g^{ak})^{-1} m (g^{ak})$$
$$= m.$$

Para romper el sistema, Eve tiene que resolver una instancia del DLP.

Obs: $m \sim \log_2 p$ bits

$C = (C_1, C_2) \sim 2 \log_2 p$ bits

$\Rightarrow$ El Gamal tiene 2-a-1 expansión de mensaje.

Prop p fijo y base g para ElGamal

Supongamos que Eve tiene acceso a un oráculo que puede descifrar textos cifrados arbitrarios, ~~(cifrados por ElGamal)~~ cifrados por claves públicas arbitrarias de ElGamal. Entonces puede usar el oráculo para resolver el DHP.

Dem Oráculo recibe { p primo, g base, clave pública A, cifrado (c_1, c_2) } y produce $(c_1^g)^{-1} c_2 \pmod p$

Ahora ~~Alice~~ Eve tiene $A = g^a \pmod p$ y $B = g^b \pmod p$

Usando el oráculo que puede hacer Eve?

[oráculo $(p, g, A, (B, 1))$ produce $(g^{ab})^{-1} \pmod p$
y de ahí se calcula g^{ab} como $((g^{ab})^{-1})^{-1}$

Pero tal vez el oráculo sabe que no debería procesar textos cifrados como $(c_1, 1)$.

Entonces Eve puede hacer lo siguiente

Eve elige c_2^* arbitrario y dice al oráculo que el txt cifrado es (B, c_2).

Entonces el oráculo calcula:

$$m \equiv (c_1^a)^{-1} \cdot c_2 \equiv (B^a)^{-1} c_2$$
$$\equiv (g^{ab})^{-1} c_2 \pmod p$$

Y entonces $g^{ab} \equiv m^{-1} c_2 \pmod p$. □

Obs: Usando el oráculo solo se ha resuelto el DHP y no el DLP

Obs: ~~Hemos~~ Este tipo de ataque se llama "Chosen ciphertext attack"

Hemos probado que, suponiendo que el DHP es difícil, el sistema de ElGamal es seguro.

Teoría elemental de grupos

Def. Un grupo consiste de un elemento G y una operación binaria $* : G \times G \to G$ que cumplen

1) (identidad (nulo)) $\exists e \in G$ t.q. $\forall a \in G$
$a * e = e * a = a$.

2) (inverso) $\forall a \in G, \exists! a^{-1} \in G$ t.q.
$a * a^{-1} = a^{-1} * a = e$

3) (asociatividad) $\forall a, b, c \in G$,
$a * (b * c) = (a * b) * c$.

Si además, satisface

4) (conmutatividad) $\forall a,b \in G$, $a*b = b*a$

se dice que es un grupo abeliano.

Obs: Si $\#G < \infty$, G es un grupo finito

Ej: $\Rightarrow (\mathbb{F}_p, +)$

$\Rightarrow (\mathbb{F}_p^\times, *)$

$\Rightarrow (\mathbb{Z}/N\mathbb{Z}, +)$

$\Rightarrow (\mathbb{Z}/N\mathbb{Z}, \times)$

$\Rightarrow (\mathbb{Z}, \times)$

$\Rightarrow (\mathbb{Q}, \times)$

$\Rightarrow (\mathbb{R}^\times, \times)$

$\Rightarrow (\mathbb{R}^+, \times)$

$\Rightarrow G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{R} \;:\; ad - bc \neq 0 \right\}$ con $*$ multiplicación de matrices

$(GL(2,\mathbb{R}), GL(n,\mathbb{R}))$

Notación: $g^x \underset{\text{def}}{=} \underbrace{g * g * g \cdots * g}_{x \text{ veces}}$ (operación binaria)

en $(\mathbb{F}_p)^\times$, $g^3 = g \cdot g \cdot g$ pero en $(\mathbb{Z}/N\mathbb{Z}, +)$, $g^3 = g+g+g$.

Si $x<0$, $g^x = \underbrace{g^{-1} * g^{-1} * \cdots * g^{-1}}_{x \text{ veces}}$; $g^0 = e$.

Def: G grupo, $a \in G$. Si $\exists\, d \in \mathbb{N}$ t.q $a^d = e$, el d más chico que tiene esa propiedad se llama el orden de G. Si no d existe con esa propiedad, se dice que G tiene orden infinito

Prop: G un grupo finito. Entonces todo elemento tiene orden finito. Si, además, $a \in G$ tiene orden d y si $a^k = e$, entonces $d \mid k$.

Dem: Como G es finito, la sucesión

$$a, a^2, a^3, \dots$$

tiene una repetición o sea, Existen $i, j \in \mathbb{N}$ t.q $a^i = a^j$ $(i > j)$

Entonces $a^{i-j} = e$, y a^{i-j} una potencia de a no de e.

El orden de a es la mínima potencia, la llamamos d.

Ahora $k \geq d$ t.q $a^k = e$ Ahora $k = dq + r$ con $0 \leq r < d$

y

$$e = a^k = a^{dq+r} = (a^d)^q * a^r$$

$$= e * a^r$$

$$= a^r.$$

Pero d es la potencia más chica que verifica esta igualdad.

Entonces $r = 0$ y $d \mid k$. $\square$

Thm (Lagrange) G grupo finito, $a \in G$. Entonces orden de $a \mid \#G$.

Más precisamente: sea $n = \#G$
$d = \text{ord}(a)$

Entonces $a^n = e$ y $d \mid n$.

Dem (para G ~~conmutativo~~ abeliano)

$G = \{g_1, \dots, g_n\}$ porque $\#G < \infty$.

Definimos ~~para $a \in G$~~

$$S_a = \{ag_1, \dots, ag_n\}$$

Se ve que son distintos: si $ag_i = ag_j \Rightarrow g_i = g_j$. Entonces $\#S_a = n$ y entonces $G = S_a$ (como conjuntos). Ahora

$$ag_1 * ag_2 * \dots * ag_n = g_1 * \dots * g_n$$

donde se ve $a^n = e$. Y $d \mid n$ ~~por~~ □
la prop. anterior.

¿Cómo se caracteriza la dificultad de resolver DLP?

Una medida natural es la cantidad de operaciones que uno precisa.

Por ejemplo, si g^x es una operación, fuerza bruta para resolver el DLP para g^x módulo p sería interminable: si g tiene orden n, ~~hay una solución~~ se hallaría una solución en a lo más n operaciones pero si $n > 2^{80}$?

- Si n y x tienen k-bits (o sea si $n \sim 2^k$)

Calcular $g^x \pmod p$ ~~para~~ requiere:

$\sim k$ multiplicaciones para cada x y $\sim 2^k$ cálculos

O sea $\sim k\, 2^k$ (donde el $\sim$ dice un pequeño múltiplo de)

Si tenemos algo $\sim 2^k$ o $\sim k 2^k$ o $\sim k^2 2^k$ lo importante es el 2^k los factores pequeños no importan.

Def. ~~f y g funciones~~ $f, g : A \to \mathbb{R}^+$ funciones

Se dice que f es big Θ de g y se denota

$$f(x) = \Theta(g(x))$$

si existen constantes positivas c y C tal que

$$f(x) \leq c\, g(x) \quad \forall x \geq C.$$

Se escribe $f(x) = \Theta(1)$ si $f(x)$ es acotado para todo $x \geq C$.