2021-06-22

Today 11:32 AM — IIC 3253

Elgamal:

P primo grande, g generador $\{1, .., P-1\}$

$x \leftarrow \{1 .. P-1\}$ llave privada

g^x llave pública

Para enc. un mensaje m con la llave pública

$y \leftarrow \{1 .. P-1\}$

enviar $(g^y, \underbrace{(g^x)^y}_{s} \cdot m)$

Para decriptar (c_1, c_2)

calculamos $s = c_1^x = (g^y)^x = g^{x \cdot y}$

y luego $m = s^{-1} \cdot c_2 = \cancel{(g^{xy})^{-1}} \cancel{(g^{xy})} \cdot m$

Firmar con Elgamal

P, g, x, g^x

Para firmar un mensaje m

$k \leftarrow \{2, .., p-2\}$

$r := g^k \bmod P$

$s := (H(m) - x r) k^{-1} \bmod p-1$

$$a \equiv b \bmod p \not\Rightarrow g^a \equiv g^b \bmod p$$
$$a \equiv b \bmod p-1 \Rightarrow g^a \equiv g^b \bmod p$$

Enviar (r,s) como firma.

Verificar

$$g^{H(m)} \equiv (g^x)^r \cdot r^s \bmod p \stackrel{?}{=} v$$

Un grupo (estructura algebraica) es un conjunto G con una operación binaria $*: G \times G \to G$. La operación tiene que satisfacer:

1) Existencia de un neutro $e \in G$ $a*e = e*a = a$ $\forall a \in G$
2) Existencia de inversos: $\forall a \in G \; \exists a^{-1}: a \cdot a^{-1} = a^{-1} \cdot a = e$
3) $*$ es asociativa $(a*b)*c = a*(b*c)$

$\mathbb{Z}_p^* = (\{1, .., p-1\}, * := \text{mult. mod } p)$

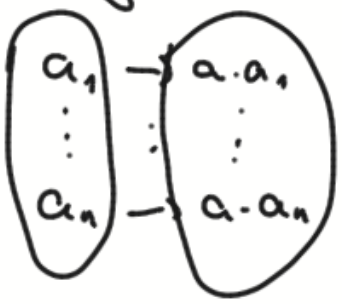
$\mathbb{Z}_N^+ = (\{0, .., N-1\}, * := \text{suma mod } N)$

(Strings binarios de largo N, XOR)

$(G, *)$

Dado un $a \in G$ tomemos la operación $*_a: G \to G$ def por $*_a(b) = a \cdot b$

Preg: es $*_a$ biyectiva?



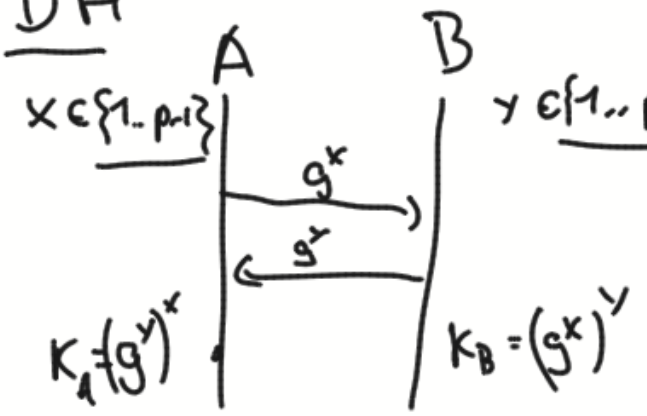
Para que $(*_a)$ no sea biyectiva necesitamos $a_i \neq a_j \in G$ t.q. $a \cdot a_i = a \cdot a_j$

$\Rightarrow a^{-1}(a \cdot a_i) = a^{-1}(a \cdot a_j)$

$\Rightarrow (a^{-1}a) \cdot a_i = (a^{-1}a) \cdot a_j$

Si compartimos un $k \in G$ aleatorio, puedo enviar un mensaje $m \in G$ encriptado como $k \cdot m$, y mientras k sea secreto esto "tiene" perf. secrecy.

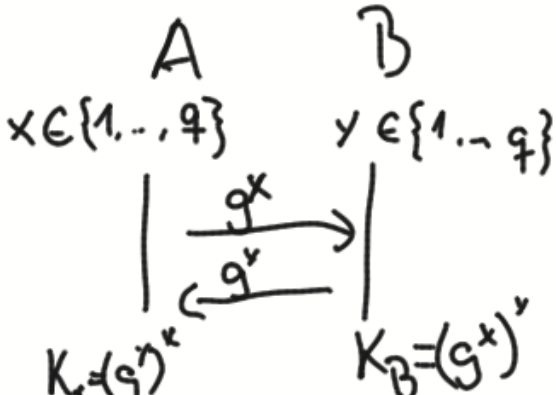
DH



g es generador de $\{1..p-1\}$

Generalizando:

$(G, *)$ un grupo, $g \in G$ es generador de G:
si $|G| = q$, entonces $\{g, g*g, g*g*g, \dots, \underbrace{g*\cdots*g}_{q \text{ veces}}\} = G$



Funciona bien en un grupo en el que el log discreto es difícil.

Schnorr signatures: investigar