2021-06-15

Today 11:23 AM

IIC 3253

El gamel:

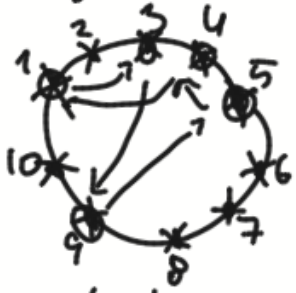
P un primo grande (>300 dígitos)

$\{1, .., P-1\}$, multiplicación módulo P.

$g \in \{1, .., P-1\}$ generador $\{1, .., P-1\}$

$\{g, g^2, g^3, .., g^{P-1}\} = \{1, .., P-1\}$

$P = 11, g = 2$



Alice genera su llave privada x que es un número aleatorio en $\{1, .., P-1\}$.

La llave pública de Alice se define como g^x.

Bob quiere enviar un mensaje $m \in \{1, .., P-1\}$ a Alice.

1) Generar $y \xleftarrow{Unif} \{1, .., P-1\}$. Def $c_1 := g^y$
2) Def. $s := (g^x)^y$
3) Def $c_2 := s \cdot m$
4) Enviar (c_1, c_2) a Alice.

Bob genera $y \leftarrow \{1, .., P-1\}$ y envía $(g^y, g^{xy} \cdot m)$

Para decriptar (c_1, c_2), Alice:

1) Def $S := c_1^x$

2) Calcular $S^{-1} \pmod p$

3) Calcular $s^{-1} \cdot c_2 = S^{-1} \cdot S \cdot m = m$.

Seguridad?

Un atacante no debería poder obtener x en base a g^x. (Problema del logaritmo discreto)

$g^x, (g^y, g^{xy} \cdot m)$

Un atacante no debería poder obtener $g^{x \cdot y}$ en base a g^x y g^y (Problema computacional de Diffie-Hellman)

Dados g^x y g^y para x e y aleatorios, un atacante no puede distinguir g^{xy} de un número aleatorio (Problema de desición de Diffie-Hellman).

Adv. Ver.

Genera P_k, S_k, envía P_k a Adv.

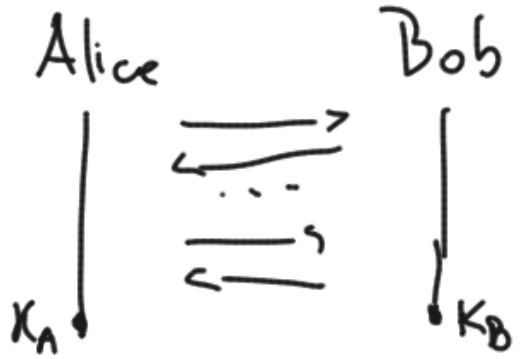
Genera m_0, m_1 y los envía a Ver.

Genera $b \leftarrow \{0,1\}$ y encripta m_b, y envía $c := Enc(P_k, m_b)$ a Adv.

Decide si $b=0$ ó $b=1$

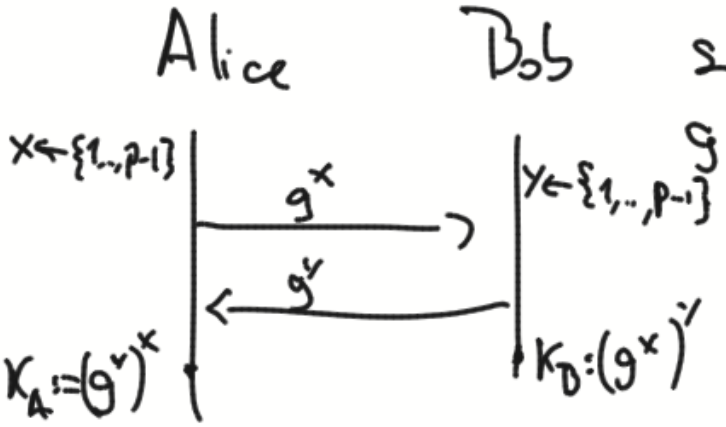
Con el juego esto podría funcionar bien :)

Diffie - Hellman Key. exchange



Prop: $K_A = K_B =: K$

Este protocolo es seguro si a partir de los mensajes enviados, no se puede obtener K.



Sup p primo grande y g un generador de $\{1,..,p-1\}$

Esto funciona bien si suponemos que el problema de decisión de Diffie-Hellman es complejo.