CÓDIGOS Y CRIPTOGRAFÍA. INFORMÁTICA DIEGO RUANO 15/11 2022

CRIPTOSISTEMA DE CLAVE PÚBLICA: ELGAMAL

SEGURIDAD BASADA EN EL PROBLEMA DEL LOGARITMO DISCRETO

DADOS p PRIMO GRANDE Y g UN GENERADOR DEL GRUPO MULTIPLICATIVO $(\mathbb{Z}_p)^*$, O AL MENOS, UN GENERADOR DE UN SUBGRUPO SUFICIENTEMENTE GRANDE $\{g^0, g^1, g^2, \ldots, g^u\}$. Y DADO $1 < y < u$

ES COMPUTACIONALMENTE DIFÍCIL ENCONTRAR x

TAL QUE
$$g^x \equiv y \mod p$$
$$x = \log_g y \mod p$$

GENERACIÓN DE LAS CLAVES

ES UN SISTEMA DE CLAVE PÚBLICA POR LO QUE SE TIENE UNA CLAVE PRIVADA Y OTRA PÚBLICA.

- EL USUARIO ELIGE UN NÚMERO PRIMO p Y PREFERENTEMENTE UNA RAÍZ PRIMITIVA MODULO p, g, O AL MENOS UN ELEMENTO DE ORDEN GRANDE.

ELIGE TAMBIÉN DE FORMA ALEATORIA $a \in \{2, \ldots, p-2\}$

(EN ALGUNOS SITIOS $a \in \{0, 1, \ldots, p-2\}$)

CALCULA

$$A = g^a \bmod p$$

CLAVE PÚBLICA: (p, g, A)

CLAVE PRIVADA: a

- PARA ENVIAR UN MENSAJE AL USUARIO ANTERIOR, EL MENSAJE M, CON $0 \leq M < p$.

SE USA SU CLAVE PÚBLICA (p, g, A)

Y ADEMÁS ELIGE ALEATORIAMENTE $b \in \{2, \dots, p-2\}$

CALCULA

$$B = g^b \bmod p$$

$$C = A^b M \bmod P$$

EL MENSAJE CIFRADO ES EL PAR (B, C)

- DESCIFRADO

EL USUARIO CON CLAVE PÚBLICA (p, g, A) Y PRIVADA a, RECIBE (B, C)

CALCULA $K = B^a \bmod p$

Y RECUPERA EL MENSAJE COMO: $M = C K^{-1} \bmod p$

PUESTO QUE

$$K \equiv B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \mod p \; (*) \quad Y$$

$$C K^{-1} \equiv A^b M \left(\underset{(*)}{A^b}\right)^{-1} \equiv M \, A^b \cdot A^{-b} \equiv M \mod p$$

$(a^b)^c = a^{b \cdot c}$

$a^{a+c} = a^b \cdot a^c$

NO ES NECESARIO CALCULAR K^{-1} mod:

$$\boxed{M = B^{p-1-a} C \mod p}$$

PORQUE SI g TIENE ORDEN $p-1$:

$$B^{p-1-a} C \equiv (g^b)^{p-1-a} A^b M \equiv g^{b(p-1-a)} (g^a)^b M \equiv$$

$$g^{b(p-1-a)} \cdot g^{ab} M \equiv g^{b(p-1-a)+ab} M \equiv g^{b(p-1)} M \equiv (\underbrace{g^{p-1}}_{=1})^b M \equiv$$

$$\equiv M \mod p$$

EJ: $P = 23$, $g = 7$

ALICE $\leftarrow$ BOB

ALICE ESCOGE: $a = 13$ $(2 \leq a \leq P-2)$

ALICE CALCULA:

$$A = g^a \bmod p = 7^{13} \bmod 23 = 20$$

CLAVE PÚBLICA $(P=23, g=7, A=20)$

CLAVE PRIVADA $(a=13)$

BOB ESCOGE: $b = 9$ Y SU MENSAJE ES $M = 5$

BOB CALCULA:

$$B = g^b \bmod p = 7^9 \bmod 23 = 15$$

$$C = A^b M \bmod p = 20^9 \cdot 5 \bmod 23 = 2$$

BOB ENVÍA EL MENSAJE CIFRADO $(B, C) = (15, 2)$
A ALICE

ALICE RECUPERA M CALCULANDO

$$B^{p-1-a} C \bmod p = 15^{23-1-13} \cdot 2 \bmod 23 = 5$$

ALTERNATIVA ALICE RECUPERA M:

$$C(\underbrace{B^a}_{K})^{-1} = 2 \cdot (15^{13})^{-1} \bmod 23 = 5$$

EFICIENCIA DE ELGAMAL

- LA GENERACIÓN DE CLAVES, CIFRADO Y DESCIFRADO REQUIERE EXPONENCIACIÓN MODULAR. LO CUAL PUEDE HACERSE GRACIAS AL ALGORITMO DE LOS CUADRADOS REPETIDOS
- PARA EL CIFRADO SE NECESITA HACER DOS POTENCIAS

$$\beta = g^b \bmod p \quad y \quad A^b \bmod p$$

Y UNA MULTIPLICACIÓN $\quad C = (A^b) \cdot M \bmod p$

INSIGNIFICANTE

- PARA EL CIFRADO DE RSA SÓLO SE NECESITA HACER UNA POTENCIA

PERO:

LAS DOS POTENCIAS DEL CIFRADO DE ELGAMAL

PUEDEN PRECALCULARSE DADO QUE NO DEPENDEN
DEL MENSAJE A ENVIAR, POR LO QUE PARA
CIFRAR, SÓLO SE NECESITARÍA HACER UNA
MULTIPLICACIÓN MODULAR. LO CUAL ES MUY
RÁPIDO. Y EN PARTICULAR MUCHO MÁS RÁPIDO
QUE RSA (QUE REQUIERE UNA POTENCIA MODU-
LAR PARA CADA MENSAJE A ENVIAR)

DESVENTAJA:

LAS DOS POTENCIAS PRECALCULADAS DEBEN
SER ALMACENADAS EN UN LUGAR SEGURO, COMO
UNA "SMARTCARD"

SEGURIDAD DE ELGAMAL

- COMO EN EL INTERCAMBIO DE CLAVES DE DIFFIE-HELLMAN, LA SEGURIDAD ESTÁ BASADA EN EL PROBLEMA DEL LOGARITMO DISCRETO.

EVE PODRIA INTENTAR CALCULAR LA CLAVE SECRETA a A PARTIR DE LA CLAVE PÚBLICA

$$a = \log_g A \mod p$$

- DE HECHO ROMPER EL CRIPTOSISTEMA DE ELGAMAL ES EQUIVALENTE A ROMPER EL INTERCAMBIO DE CLAVES DE DIFFIE-HELLMAN
- NOTA: EL EXPONENTE k DEBE SER DIFERENTE CADA VEZ PARA EVITAR ATAQUES DE TIPO ESTADISTICO

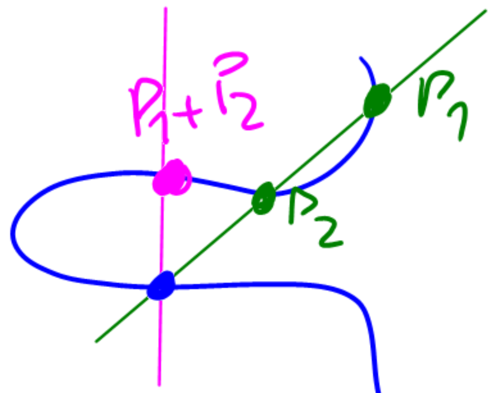
- EN GENERAL LOS SISTEMAS BASADOS EN LOGARITMO DISCRETO SON SEGUROS, AUNQUE HAY QUE TENER CUIDADO PORQUE HAY ATAQUES PARA CONDICIONES PARTICULARES

- SE SUELE TOMAR P DE AL MENOS LONGITUD BINARIA 1000. Y COMO EN RSA, EVITAR PRIMOS DE DETERMINADAS PROPIEDADES (COMO TENER TODOS LOS FACTORES DE P-1 PEQUEÑOS)

- GRUPO ARBITRARIO FINITO CICLICO

- $(\mathbb{Z}_p)^* = \{1, \ldots, p-1\}$

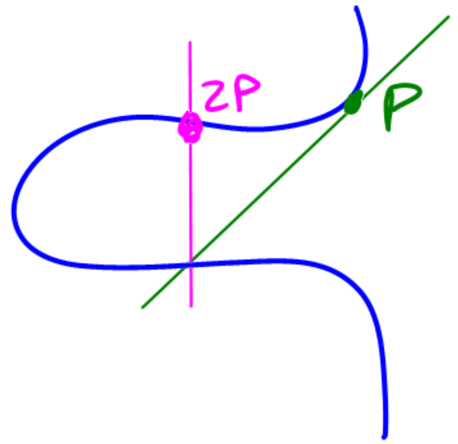
- CURVAS ELIPTICAS



$\{P, 2P, 3P, \ldots\ldots, \}$

GRUPO CÍCLICO

GENERADOR P



PUNTO $P \Longleftrightarrow g$ NÚMERO

$\mathbb{Z}_p^*$

OTROS CRIPTOSISTEMAS DE CLAVE PÚBLICA:

- MOCHILAS (KNAPSACK): MERKLE-HELLMAN 1978. ROTO EN 1984
- RABIN (1979): PARECIDO RSA SEGURO CONTRA ATAQUE DE TEXTO PLANO CONOCIDO
  INCONVENIENTE: DADO UN OUTPUT HAY 4 POSIBLES INPUTS
- MASSEY-OMURA: 3 ENVÍOS