CÓDIGOS Y CRIPTOGRAFÍA. INFORMÁTICA DIEGO RUANO 3/11 2022

LIMITES DE LA CRIPTOGRAFÍA SIMÉTRICA

EN LOS AÑOS 60 SE EMPIEZAN A VER LAS LIMITACIONES DE LA CLAVE PRIVADA-SIMÉTRICA CON EL USO DE INTERNET/TELECOMUNICACIONES.

- INTERCAMBIO DE CLAVES: DOS USUARIOS SE TIENEN QUE PONER DE ACUERDO EN UNA CLAVE. TIENEN QUE MANTENERLA EN SECRETO

- AUTENTIFICACIÓN E INTEGRIDAD: SE NECESITA GARANTIZAR QUE EL EMISOR ES QUIEN DICE SER Y QUE EL MENSAJE TRANSMITIDO NO HA SIDO MODIFICADO

1975: DIFFIE-HELLMAN PRESENTAN "NEW DIRECTIONS IN CRYPTOGRAPHY"

CLAVE PÚBLICA ó ASIMÉTRICA

$L = N \times N$ Y CADA USUARIO u DEL SISTEMA TIENE UN PAR DE CLAVES (e_u, d_u)

- e_u ES PÚBLICA, Y ES LA QUE USA CUALQUIER OTRO USUARIO DEL SISTEMA PARA ENVIAR UN MENSAJE CIFRADO A u.
- d_u ES SÓLO CONOCIDA POR EL USUARIO u Y ES LA QUE USA PARA DESCIFRAR LOS MENSAJES QUE RECIBE

LAS CLAVES USADAS EN LA LÍNEA $\ell = (a, b)$ SON LAS DEL USUARIO b, $K_e = e_b$ Y $K_e' = d_b$.

CONDICIÓN:

AÚN CONOCIDA e_u SEA IMPOSIBLE EN LA PRÁCTICA EL CÁLCULO DE LA CLAVE PRIVADA d_u

ESTO SE INTERPRETA EN TÉRMINOS DE COMPLEJIDAD COMPUTACIONAL DEL CÁLCULO DE d_u A PARTIR DE e_u Y DE LA CANTIDAD DE PARES DE MENSAJES EN CLARO Y CIFRADO QUE TENGA EL CRIPTOANALISTA.

CONDICIONES DIFFIE-HELLMAN:

(DE 1976, ANTES DE CONOCER NINGÚN EJEMPLO)

- CÁLCULO CLAVES PÚBLICA Y PRIVADA DEBE SER COMPUTACIONALMENTE SENCILLO
- PROCESO CIFRADO DEBE SER COMPUTACIONALMENTE SENCILLO
- PROCESO DESCIFRADO, CONOCIENDO LA CLAVE PRIVADA, DEBE SER COMPUTACIONALMENTE SENCILLO
- OBTENER CLAVE PRIVADA A PARTIR DE LA PÚBLICA, DEBE SER UN PROBLEMA "COMPUTACIONALMENTE IMPOSIBLE"
- OBTENER MENSAJE EN CLARO, CONOCIDO EL MENSAJE CIFRADO Y LA CLAVE PÚBLICA, DEBE SER COMPUTACIONALMENTE IMPOSIBLE.

USO DE LA CRIPTOGRAFÍA DE CLAVE PÚBLICA

- NO HAY UN INTERCAMBIO DE CLAVES: CADA USUARIO GENERA SUS CLAVES. LA CLAVE PRIVADA NO SE ENVÍA A NADIE

- NO SUSTITUYEN A LOS SISTEMAS DE CLAVE PRIVADA PORQUE ÉSTOS SON MUCHO MÁS RÁPIDOS

- SE USA UN SISTEMA MIXTO EN EL QUE SE INTERCAMBIAN CLAVES Y AUTENTIFICA CON UN SISTEMA DE CLAVE PÚBLICA.
DESPUÉS SE COMUNICAN USANDO UN SISTEMA DE CLAVE PRIVADA

FUNCIONES DE UNA VÍA

$$f : A \longrightarrow B$$

DADO $x \in A$, ES COMPUTACIONALMENTE SENCILLO CALCULAR $f(x)$

PERO DADO $y \in Im(f) \subset B$, ES COMPUTACIONALMENTE IMPOSIBLE, EN GENERAL, ENCONTRAR $x \in A$ TAL QUE $f(x) = y$.

EJ: $P \subset \mathbb{N}$ CONJUNTO NÚMEROS PRIMOS

$$f : P \times P \longrightarrow \mathbb{N}$$
$$(p, q) \longmapsto p \cdot q$$

ESTE PROBLEMA ES INTRATABLE PARA UN ORDENADOR CLÁSICO (PARA NÚMEROS SUFICIENTEMENTE GRANDES)

EN CAMBIO, ES UN PROBLEMA TRATABLE PARA UN ORDENADOR CUÁNTICO.

FUNCIÓN TRAMPA

UNA FUNCIÓN DE UNA VÍA $f: A \to B$ PARA LA QUE EXISTE UNA INFORMACIÓN COMPLEMENTARIA (SECRETA) t (LA TRAMPA) QUE PERMITE CALCULAR EFICIENTEMENTE $x \in A \,/\, f(x) = y$

APLICACIÓN FUNCIONES TRAMPA EN CRIPTOGRAFÍA

- CIFRADO CLAVE PÚBLICA: APLICACIÓN TRAMPA
- CLAVE PRIVADA: LA "TRAMPA" DE LA FUNCIÓN TRAMPA

RSA 1977 GENERACIÓN DE CLAVES

CADA USUARIO

- ELIGE DOS NÚMEROS PRIMOS p, q
- CALCULA $n = p \cdot q$ Y $\varphi(n) = (p-1)(q-1)$
- ELIGE e TAL QUE $0 < e < \varphi(n)$ Y

$$\operatorname{mcd}(e, \varphi(n)) = 1$$

PARA QUE e TENGA INVERSO MODULO $\varphi(n)$

- CALCULA $d \equiv e^{-1} \bmod \varphi(n)$

CLAVE PÚBLICA : (n, e)

CLAVE PRIVADA : d $(p, q, \varphi(n))$

EJ: $p=3$ $q=5$ $n=15$ $\varphi(n)=(p-1)(q-1)=(3-1)(5-1)=8$

e? $0<e<8 \wedge mcd(e,8)=1$

$e=5$ POR EJEMPLO

$5\cdot 5=25 \equiv 1$

d? $d\equiv e^{-1} \bmod \varphi(n) \equiv 5^{-1} \bmod 8 = 5$

CLAVE PÚBLICA: $(15,5)$

CLAVE PRIVADA: (5)

$e \;/\; mcd(e,8)\neq 1$ $e=4$ ← NO VA A FUNCIONAR

$4\cdot 1=4\neq 1$ $4\cdot 2=8=0\neq 1$ $4\cdot 3=12=4\neq 1$ $4\cdot 4=16=0\neq 1$

NO HAY INVERSO e^{-1} NO EXISTE

$0 < e < \varphi(n)$ TIENE INVERSO MODULO $\varphi(n)$

$$\iff \operatorname{mcd}(e, \varphi(n)) = 1$$

$$\lambda \cdot e + \underbrace{\mu\, \varphi(n)}_{\substack{\shortparallel \\ 0}} = \operatorname{mcd}(e, \varphi(n)) = 1$$

MOD $\varphi(n)$ $\longrightarrow$

$$\lambda e = 1 \mod \varphi(n)$$

$$\lambda = e^{-1} \mod \varphi(n)$$

$$\lambda \cdot e = \underset{\substack{\Uparrow \\ \operatorname{mcd}(e, \varphi(n))}}{1} \mod \varphi(n)$$

RSA. CIFRADO Y DESCIFRADO

MENSAJE $M \in \mathbb{Z}_n$ $(0 \le M < n)$ $(n = p \cdot q)$

CIFRADO: $M \longmapsto M^e \bmod n$

DESCIFRADO: $C \longmapsto C^d \bmod n = M$

FUNCIONA PORQUE $(M^e)^d \equiv M \bmod n$

DEMOSTRACIÓN: A CONTINUACIÓN ...

(VARIOS DÍAS)

EJEMPLO EN SAGE

$p = 11 \qquad q = 23$