UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

Método de ElGamal

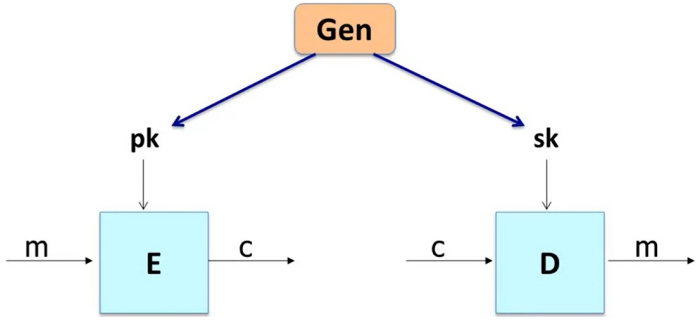
Alan Reyes-Figueroa

Criptografía y Cifrado de Información (Aula 19) 26.octubre.2021

Criptografía de Clave Pública

Recordemos que un sistema de clave pública es una tripla (G, E, D), donde

- G: es un algoritmo aleatorizado. Emite un par de claves (**pk**, **sk**).
- $E(\mathbf{pk}, \mathbf{m})$ es un algoritmo aleatorizado que toma $\mathbf{m} \in \mathcal{M}$ y produce $\mathbf{c} \in \mathcal{C}$
- $D(\mathbf{sk}, \mathbf{c})$ es un algoritmo determinista que toma $\mathbf{c} \in \mathcal{C}$ y produce $\mathbf{m} \in \mathcal{M}$.

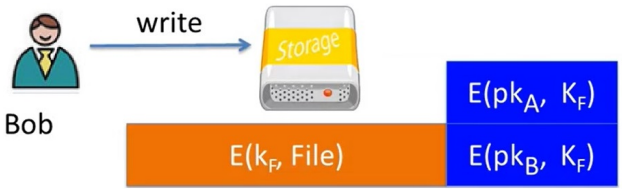


Esquema general de un sistema de clave pública.

Criptografía de Clave Pública

Aplicaciones:

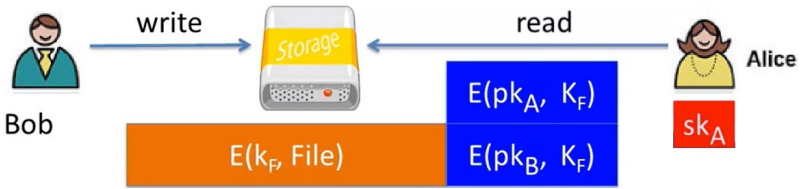
- Intercambio de claves (web, HTTPS, ...)
- Encripción en ambientes no interactivos:
  - Envío de Email,
  - Encripción de archivos.



Criptografía de Clave Pública

Aplicaciones:

- Intercambio de claves (web, HTTPS, ...)
- Encripción en ambientes no interactivos:
  - Envío de Email,
  - Encripción de archivos.



Criptografía de Clave Pública

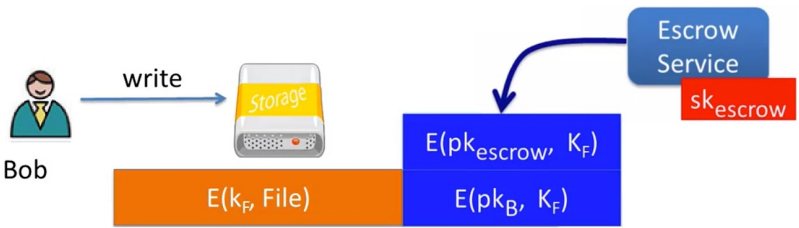
Aplicaciones:

- Intercambio de claves (web, HTTPS, ...)
- Encripción en ambientes no interactivos:
  - Envío de Email,
  - Encripción de archivos,
  - Depósito de llaves (*key escrow*), para decriptar sin la clave de Bob.

Criptografía de Clave Pública

Aplicaciones:

- Intercambio de claves (web, HTTPS, ...)
- Encripción en ambientes no interactivos:
  - Envío de Email,
  - Encripción de archivos,
  - Depósito de llaves (*key escrow*), para decriptar sin la clave de Bob.



Método de ElGamal

Es un sistema de clave pública, construido con base en el protocolo de intercambio de Diffie-Hellman.

Puede ser utilizado tanto para generar firmas digitales como para cifrar o descifrar.

Fue creado por Taher ElGamal en 1984 (estudiante de Martin Hellman).

La seguridad del algoritmo se basa en la suposición que la función utilizada es de un solo sentido debido a la dificultad de calcular un logaritmo discreto.

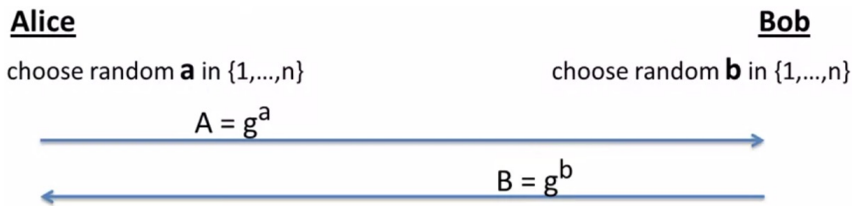
Aplicaciones:

- Protocols GPG (GnuPG, *GNU Private Guard*).
- Sistemas recientes de PGP (*Pretty Good Privacy*).
- Firmas digitales.

Método de ElGamal

Recordemos el esquema de intercambio de Diffie-Hellman:

- Elegimos un grupo cíclico G de orden n, por ejemplo $G = (\mathbb{Z}/p\mathbb{Z})^* = U(p)$.
- Elegimos un generador g en G, esto es $G = \{1, g, \mathbf{g}^2, \mathbf{g}^3, \ldots, \mathbf{g}^{n-2}, \mathbf{g}^{n-1}\}$.
- Alice y Bob eligen claves aleatorias $\mathbf{a}, \mathbf{b} \in \{1, 2, \ldots, n-1\}$.



Método de ElGamal

El cifrado ElGamal funciona de manera similar a Diffie-Hellman:

- Elegimos un grupo cíclico G de orden n, por ejemplo $G = (\mathbb{Z}/p\mathbb{Z})^* = U(p)$.
- Elegimos un generador $\mathbf{g}$ en G, esto es $G = \{1, g, g^2, g^3, \ldots, g^{n-2}, g^{n-1}\}$.
- Alice y Bob eligen claves aleatorias $\mathbf{a}, \mathbf{b} \in \{1, 2, \ldots, n-1\}$.

se trata a $A = \mathbf{g^a}$ como una clave pública.

Método de ElGamal

Bob calcula $\mathbf{g^{ab}} = A^{\mathbf{b}}$, y deriva una clave simétrica $\mathbf{k}$ a partir de ello,

Bob envía $\mathbf{c} = (B, E(\mathbf{k}, \mathbf{m}))$, donde $B = \mathbf{g^b}$ y $E(\mathbf{k}, \mathbf{m})$ es el mensaje encriptado con un cifrado simétrico.

Luego, Alice calcula $\mathbf{g^{ab}} = B^{\mathbf{a}}$, deriva $\mathbf{k}$ y decripta el mensaje $\mathbf{m} = D(\mathbf{k}, E(\mathbf{k}, \mathbf{m}))$.

Método de ElGamal

Más concretamente, el sistema de encripción del ElGamal consiste de tres componentes:

- G es un grupo finito cíclico de orden n (*e.g.* $G = U(p)$),
- (E_s, D_s) un cifrado simétrico, sobre el espacio $(\mathcal{K}, \mathcal{M}, \mathcal{C})$,
  (*e.g.* AES, DES, ...)
- $H : G \times G \to \mathcal{K}$, una función hash.
  (*e.g.* SHA-256, se deben concatenar las dos entradas).

Construimos un esquema de cifrado de clave pública (G, E, D), como sigue:

- G el generador de claves:
  - Elegimos un generador aleatorio $\mathbf{g} \in$, y un valor aleatorio $\mathbf{a} \in \mathbb{Z}/n\mathbb{Z}$.
  - Definimos las claves secreta y pública, como

$$\mathbf{sk} = \mathbf{a}, \qquad \mathbf{pk} = (\mathbf{g}, \mathbf{h}), \text{ con } \mathbf{h} = \mathbf{g}^{\mathbf{a}}.$$

Método de ElGamal

- *G* el generador de claves:
  - Elegimos un generador aleatorio $\mathbf{g} \in$, y un valor aleatorio $\mathbf{a} \in \mathbb{Z}/n\mathbb{Z}$.
  - Definimos las claves secreta y pública, como

$$\mathbf{sk} = \mathbf{a}, \qquad \mathbf{pk} = (\mathbf{g}, \mathbf{h}), \text{ con } \mathbf{h} = \mathbf{g}^{\mathbf{a}}.$$

- Las funciones de encripción *E* y decripción *D*:

E(pk=(g,h), m) :

$b \xleftarrow{R} Z_n$, $u \longleftarrow g^b$, $v \longleftarrow h^b$

$k \longleftarrow H(u,v)$, $c \longleftarrow E_s(k, m)$

output (u, c)

D(sk=a, (u,c)) :

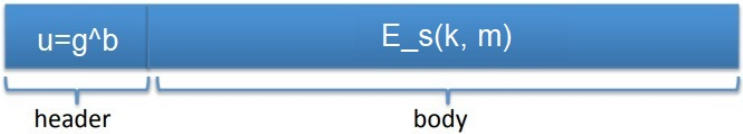
$v \longleftarrow u^a$

$k \longleftarrow H(u,v)$, $m \longleftarrow D_s(k, c)$

output m

Método de ElGamal

En figuras:



Desempeño:

E(pk=(g,h), m) :

$b \leftarrow Z_n$, $u \leftarrow g^b$, $v \leftarrow h^b$

D(sk=a, (u,c)) :

$v \leftarrow u^a$

- Encripción: 2 esponentes (base fija)
  - Podemos precalcular $(\mathbf{h}^{(2^i)}, \mathbf{g}^{(2^i)})$, $i = 1, 2, \ldots, \log_2 n$.
  - Esto gana cerca de 3x velocidad (o más).
- Decripción: 1 exponente (base variable).