Breve introducción a la criptografía de llave pública

William de la Cruz de los Santos

Universidad Autónoma del Estado de México
Ingeniería en Computación

WeWork Montes Urales, June 18 to 22, 2018

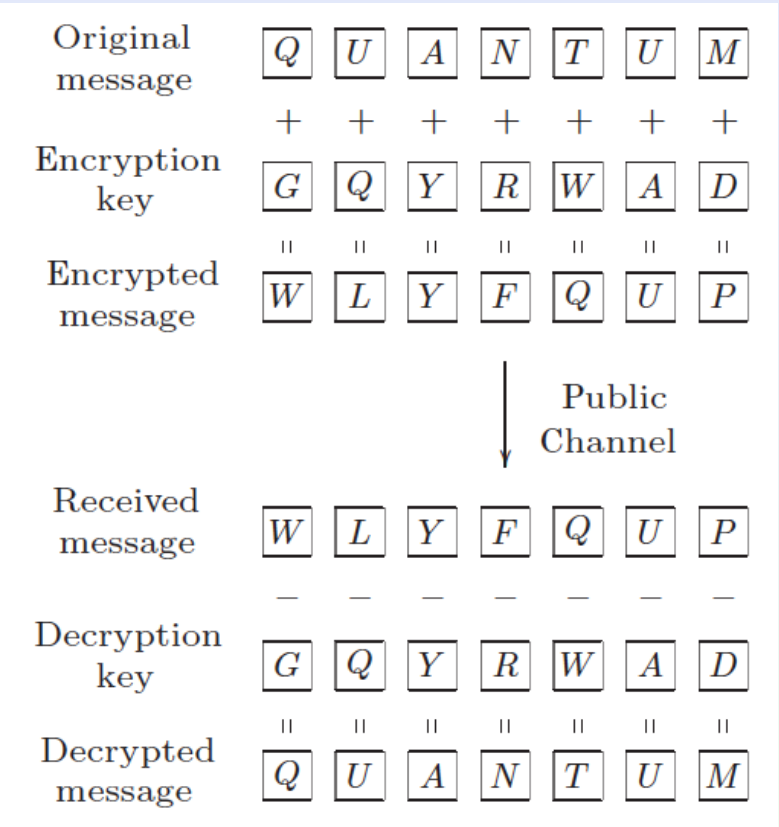
UAEM | Universidad Autónoma del Estado de México

Tecnológico de Monterrey

Table of Contents

CRIPTOGRAFÍA DE LLAVE SIMÉTRICA

En la criptografía de llave simétrica, dos entidades A y B deben acordar una llave que les permita codificar y decodificar al mismo tiempo.



El cifrador simétrico de Vernam (*one time pad*).

Table of Contents

Tipos de llaves criptográficas

- ⇒ Secreta/privada: llave compartida entre dos entidades en la criptografía simétrica.
- ⇒ Privada: llave conocida sólo por la entidad que la generó de acuerdo a algún esquema criptográfico de llave pública.
- ⇒ Pública: llave conocida por un conjunto de entidades que usan algún esquema criptográfico de llave pública.
- ⇒ Sesión: llave generada de forma única para el establecimiento de una comunicación entre dos o más entidades.

PROTOCOLOS DE INTERCAMBIO DE LLAVE

Distribución de llaves

Acuerdo de llaves

Diffie-Hellman

Distribución de llaves

Canales de confianza

Archivos públicos seguros

Entidades de confianza (en/fuera de línea) con certificados digitales

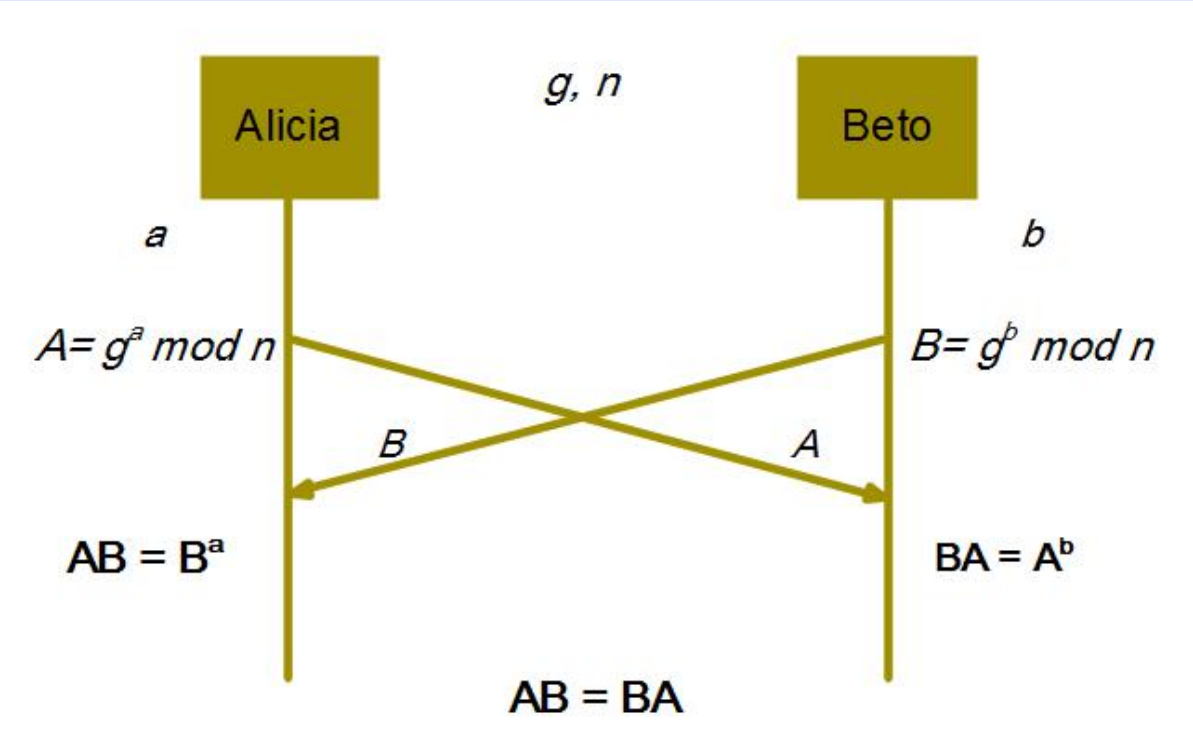
Centro de Distribución de llaves (en/fuera de línea) sin certificados digitales

Acuerdo de llaves

Acordar una llave es un proceso o protocolo por el cual un secreto es compartido para estar disponible entre dos o más entidades.

La llave puede ser simétrica o de sesión

INTERCAMBIO DE LLAVES DIFFIE-HELLMAN



Intercambio de llaves Diffie-Hellman

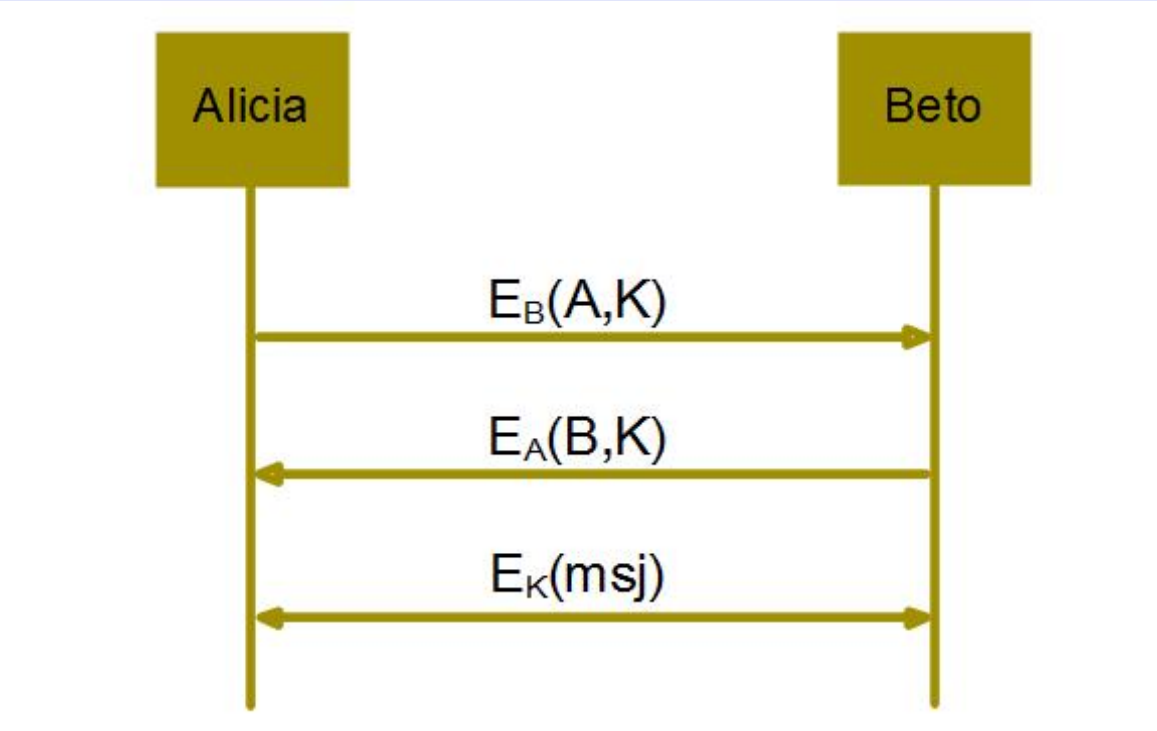
Entidad A

1. Seleccionar $a \in [1, n-1]$
2. Calcular $y_a = g^a \bmod n$
3. Enviar y_a a B
4. Calcular $y_{ab} = (y_b)^a \bmod n$

Entidad B

1. Seleccionar $b \in [1, n-1]$
2. Calcular $y_b = g^b \bmod n$
3. Enviar y_b a A
4. Calcular $y_{ba} = (y_a)^b \bmod n$

PROTOCOLO KERBEROS



Kerberos

$A\ (d_A, e_A, n_A)$

1. Seleccionar
   $|k| \approx 128$
2. Calcular
   $c_K = (A||K)^{e_B}\ mod\ n_B$
3. Enviar c_K a B
4. Calcular
   $K = c_K^{d_A}\ mod\ n_A$

$B,\ (d_B, e_B, n_B)$

1. Calcular
   $K = c_K^{d_B}\ mod\ n_B$
2. Calcular
   $c_K = (B||K)^{e_A}\ mod\ n_A$
3. Enviar c_K a A

Comentarios Finales

- El intercambio de llaves sucumbe ante el ataque del hombre de en medio.
- El uso de autoridades de confianza o centros de distribución de llaves puede proveer mayor seguridad.
- Al final, la comunicación basada en la confianza es necesaria.

Referencia

- S P. Miller, B. C. Neuman, J. I. Schiller and J. H. Saltzer, *Kerberos Authentication and Authorization System*, Published by The Massachusetts Institute of Technology, 1987.
- E. Rescorla, *Diffie-Hellman Key Agreement Method*, Network Working Group, Standards Track, RFC 2631, 1999.

Table of Contents

Introducción

Ante las problemáticas de la criptografía de llave simétrica era necesario contar con un mecanismo que permitiera distribuir las llaves secretas de manera segura.

Tal necesidad dio apertura a la criptografía de llave pública que tiene como principal característica el uso de dos llaves una privada conocida sólo por su dueño y una pública conocida por todos.

Criptografía de llave pública

En 1976, Diffie y Hellman introdujeron el concepto de criptografía de llave pública. Este tipo de esquemas utilizan *funciones de sólo ida* e *información secreta*.

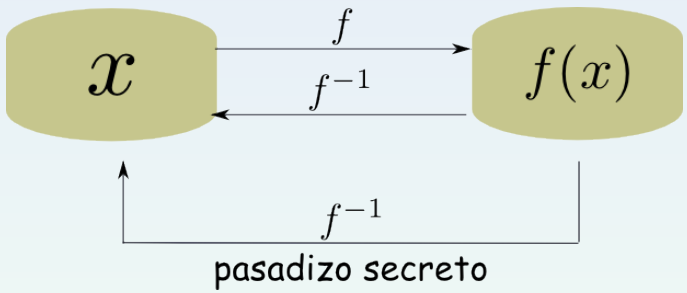
Una función $f : \{0,1\}^* \to \{0,1\}^*$ es de *sólo ida*, si se satisfacen las siguientes condiciones:

i) f es fácil, *es decir, existe un algoritmo $\mathcal{A}$ de tiempo polinomial que calcula eficientemente $f(x)$ para todo x.*

ii) f^{-1} es difícil, *es decir, para cada algoritmo $\mathcal{A}$ de tiempo polinomial, existe la probabilidad desdeñable de que dada la imagen $f(x)$ obtenga x.*

Funciones de sólo ida con pasadizo secreto

Una función de sólo ida f tiene pasadizo secreto si para cualquier argumento x la evaluación $f(x)$ es fácilmente calculada, pero conocida únicamente $f(x)$ es computacionalmente intratable encontrar cualquier $f(y) = f(x)$ sin conocer el *pasadizo secreto*.



Criptografía de llave pública

1. La información secreta es información esencial que permite calcular el inverso de la función de sólo ida.
2. Los cripto-esquemas de llave pública se caracterizan por el hecho de usar un par de llaves, una pública y una privada, ambas asignadas a cada usuario del sistema.
3. La llave privada es conocida sólo por su propietario y la llave pública como su nombre lo indica es de dominio público.
4. La llave pública se calcula usando una función de sólo ida y la llave privada es la información secreta para resolverla.

Criptografía de llave pública

Para construir un cripto-esquema de llave pública se requieren de cuatro primitivas:

1. Los **parámetros de dominio** son generados con la infraestructura matemática de las funciones de sólo ida requerida para cada esquema en particular.
2. **Generación de llaves**: (llave pública, llave privada)
3. **Operación privada**: si se utiliza la llave privada
4. **Operación pública**: si se utiliza la llave pública

Criptografía de Llave pública

- La llave pública es inverso matemático de la llave privada
- La llave privada es conocida únicamente por los legítimos dueños
- La llave pública es almacenada en archivos denominados Certificados Digitales

Esquema de cifrado de llave pública

Los esquemas de cifrado de llave púlbica constan de tres algoritmos principales:

- Generador de llaves: (k_s, k_v)
- Algoritmo de cifrado: $E(k_v, m) = c$
- Algoritmo de descifrado: $D(k_s, c) = m$

Esquema de cifrado RSA (Rivest-Shamir-Adleman)

En 1978, Ronal Rivest, Adi Shamir y Leonard Adleman propusieron el primer esquema de cifrado de llave pública denominado RSA, mismo que fue patentado en Estados Unidos en el año 2000.

Esquema de cifrado RSA (Rivest-Shamir-Adleman)

RSA consiste de los siguientes tres algoritmos:

- Generación de llaves

  Seleccionar dos números primos grandes p y q
  $n = p * q$
  $\phi(n) = (p-1) * (q-1)$
  seleccionar un exponente público e tal que $e < n$ y
  $mcd(e, \phi(n)) = 1$
  $d \equiv e^{-1} \, mod \, \phi(n)$
  Llave pública (e, n), llave privada (d, n)
- Cifrado para el mensaje m

  $c = m^e \, mod \, n$
- Descifrado para el mensaje cifrado c

  $c^d = (m^e)^d = m^{ed} = m \, mod \, n$

Requisitos de RSA

Para su buen funcionamiento, en RSA se debe contemplar lo siguiente:

- Debe ser computacionalmente intratable determinar la llave privada (d, n) a través de la llave pública (e, N)
- Dado un módulo n, deben existir muchos partes (d, e) que impidan un ataque de fuerza bruta
- No es posible cifrar un mensaje con una longitud mayor a la longitud del módulo n de RSA
- Debe ser relativamente fácil calcular el cifrado m^e y el descifrado c^d con números de aproximadamente 1024 bits

Seguridad de RSA

La *factorización de enteros* grandes es el problema intratable computacionalmente que protege las llaves del esquema RSA y se define informalmente como sigue:

- Sea un entero n producto de dos números primos grandes p y q, encontrar la factorización de n es un problema difícil de resolver con la tecnología actual.
- Ejemplo:
  - $142 = 2 \cdot 71$
  - $123456789 = 3^2 \cdot 3803 \cdot 3607$
  - $p = 67$, $q = 41$, $n = 2747$
  - $p = 1234567891$, $q = 1234545803$, $n = 1524130608352611473$

Seguridad de RSA

La *factorización de enteros* grandes es el problema intratable computacionalmente que protege las llaves del esquema RSA y se define como sigue:

Sean p y q números primos, $e \geq 1$ primo relativo de $(p-1)(q-1)$.

Si existe un número d tal que $d * e \equiv 1 \; mod \; (p-1)(q-1)$ *inverso* de e módulo $(p-1)(q-1)$

Entonces, la congruencia $x^e \equiv c \; mod \; pq$ tiene una única solución $x \equiv c^d \; mod \; pq$

Si n es un número grande los algoritmos conocidos para su factorización son imprácticos

Referencias

1. D. R. Stinson, Cryptography: Theory and Practice, Chapman and Hall/CRC, 2006.

2. W. Diffie y M. E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, 1976.

3. R. L. Rivest, A. Shamir y L. M. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, 1978.