Criptografía RSA

Jorge Andrino

15 de Noviembre del 2024

Contenido

Objetivos de una criptografía

Principalmente debe habilitar técnicas de cifrado y descifrado, pero tambien debe tener los siguientes principios en mente:

- Privacidad
- Autenticación
- Integridad
- No repudio

Predecesor

En 1975, se introduce el método Diffie-Hellman para la criptografía. Uno de los primeros medios para encriptar información de dos grupos mediante una clave. Creando una base para métodos de este tipo.

Componentes del predecesor

Tomemos a Alice y Bob como los individuos que quieren transmitir información. Entonces los componentes de Diffie-Hellman serían:

- A es la llave pública de Alice y B es la llave pública de Bob.
- a es la llave privada de Alice y b es la llave privada de Bob.
- g es el generador base, el cual es público.
- p es un primo el cual es público.

Componentes cifrado y descifrado de Diffie-Hellman

Para los mensajes con Diffie-Hellman, el proceso se puede ver mediante estas expresiones:

- Alice manda el mensaje cifrado de la forma $A = g^a$ (mod p).
- Bob manda el mensaje cifrado de la forma $B = g^b$ (mod p).
- Hay una clave secreta $k = g^{ab}$(mod p)
- Ambos pueden descifrar el mensaje utilizando: A^b(mod p) $\equiv (g^a)^b \equiv g^{ab} \equiv (g^b)^a \equiv B^a$ (mod p).

Problema de Diffie-Hellman

¿Que limitantes tiene este método de criptografía?

Problema de Diffie-Hellman

¿Que limitantes tiene este método de criptografía? Aunque se encripte un mensaje entre dos grupos, este método está expuesto al "Middle Man".

Entrada de R, S, A

Con esas piezas en juego, entran tres jugadores a la escena de la criptografía:

- Ron Rivest.
- Adi Shamir.
- Leonard Adleman.

Los tres son matemáticos que luego sacaron un doctorado en las ciencias de la computación.

Motivación de R, S, A

Este trio quería solucionar un problema introducido por el método de Diffie-Hellman. Al igual que crear una función que permitiera al receptor descifrar un mensaje mediante información que solo este posee.

Entrada de RSA

El método RSA fue creado en el MIT en 1977, publicaron su artículo en la revista Scientific American. El nombre son las iniciales de cada matemático que se unió para este método.

Componentes RSA

Para realizar este método, se necesitaban las siguientes partes:

- M es el mensaje
- C es el texto cifrado
- e es la clave pública del destino
- d es la clave privada del destino
- n es el modulo público del destino

Cifrado y descifrado de RSA

Para el método RSA, se utilizan las siguientes expresiones:

- Para cifrar el mensaje, $C = M^e$ (mod n).
- Para descifrar el mensaje, $M = C^d$ (mod n).

Para poder cifrar, se necesitan $2*log(e)$ multiplicaciones y divisiones.

Claves del RSA

Para poder generar una clave, se necesita de dos primos. Sean estos p, q, entonces si multiplicamos estos dos entre sí obtenemos n número. Después utilizamos la función de Euler,
$\phi(n) = \phi(pq) = (p-1)(q-1) = pq - p - q + 1 = n - p - q + 1$
Entonces para realizar la clave privada se tiene que d es el inverso modular de e(mod ϕ(n)), y para la clave pública e se tiene que e es el inverso modular de d(mod ϕ(n)).

¿Este es el algoritmo RSA?

Lo anterior es solo la base para poder utilizar el método RSA de **libro de texto**.

Ejemplo RSA de libro de texto

Tomemos dos primos, $p = 3$ y $q = 11$,
$\Rightarrow n = p * q = 3 * 11 = 33$
$\Rightarrow \phi(n) = (p - 1) * (q - 1) = 2 * 10 = 20.$
Elijamos una e, sea esta 7,
$\Rightarrow$ para encontrar d, este el el inverso modular de e(mod ϕ(n)) $\Rightarrow$ $d = 3$.
Lo cual nos daría como clave pública $(7, 33)$ y como clave privada $(3, 33)$.

Ejemplo de cifrado y descifrado con RSA de libro de texto

Digamos que el mensaje original es 2,
$\Rightarrow$ para nuestro cifrado sería $C = M^e$ (mod n) $= 2^7$ (mod 33) $=$ 29. Nuestro mensaje cifrado sería 29.
$\Rightarrow$ para descifrarlo, sería $M = C^d$ (mod n) $= 29^3$ (mod 33) $= 2$.
Regresando el mensaje original.

Problema del método RSA de libro de texto

El método RSA de libro de texto no es el utilizado en el algoritmo. Dado que este posee varios aspectos vulnerables. Uno es su falta de seguridad semántica y otro aspecto es que todavía no tiene aleatoriedad.

Refuerzos

La manera de abordar estos problemas es mediante los Public-Key Cryptography Standards (o bien PKCS). Con cada uno de estos se miraba una posibilidad de atacarlos y una manera de contrarestar este ataque.
Unos de los refuerzos que se han hecho es en cuanto a mejorar el pre-procesamiento, se han utilizado:

- Padding
- OAEP
- OAEP +
- SAEP +

Ventajas del RSA

- Reduce el efecto del problema "Middle Man" con las defensas agregadas.
- Tiene mejor seguridad dado que no se puede factorizar n, computarizar ϕ(n), o determinar d de una manera sencilla.
- Utiliza solamente una clave pública y una clave privada.

Dificultades del RSA

- Dado que es asimétrico, es un proceso más lento por lo que restringe sus áreas de aplicación.
- Los tamaños de las claves de esta es significativamente más grande que los otros métodos de criptografía.

Referencias

- Abarca Pita, J. F. (2018). Fundamentos matemáticos del algoritmo RSA (Tesis de maestría). Universidad Autónoma de Guerrero. https://ri.uagro.mx/bitstream/handle/uagro/776/OK15158773_maestria.pdf?sequence=1&isAllowed=y
- Calderbank, M. (2007). The RSA Cryptosystem: History, Algorithm, Primes. Universidad de Chicago. https://www.math.uchicago.edu/~may/VIGRE/VIGRE2007/REUPapers/FINALAPP/Calderbank.pdf
- Rivest, R. L., Shamir, A., & Adleman, L. (1977). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. https://cdn.nakamotoinstitute.org/docs/rsa-paper.pdf