EL ALGORITMO RSA

Angel Hesse Caracena

¿QUE ES?

El algoritmo RSA es un sistema criptográfico de clave pública, es decir, **cifrado asimétrico**, desarrollado por Ronald Linn **R**ivesert, Adi **S**hamir y Leonard **A**delman en 1979. RSA sirve para cifrar y descifrar información, y por ello también provee servicios de autenticidad y de integridad.

Al ser un cifrador asimétrico, trabaja con dos claves, una pública y una privada. Todo el contenido de texto plano, o contenido sin cifrar, que sea hecho con la clave pública, podrá ser descifrado mediante la clave privada, y viceversa, todo el contenido cifrado con la clave privada podrá ser descifrado mediante la clave pública.

FUNCIONAMIENTO

La seguridad de este algoritmo se basa en que los ordenadores actuales no son capaces de factorizar un numero compuesto muy grande que sea producto de dos primos grandes (p*q). Aunque algunos investigadores creen que la computación cuántica podría resolver esto.

Como en todo sistema de clave pública, cada usuario posee dos claves de cifrado: una pública y otra privada. Cuando se quiere enviar un mensaje, el emisor busca la clave pública del receptor, cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, este se ocupa de descifrarlo usando su clave privada.

El algoritmo consta de tres pasos: generación de claves, cifrado y descifrado:

GENERACIÓN DE CLAVES:

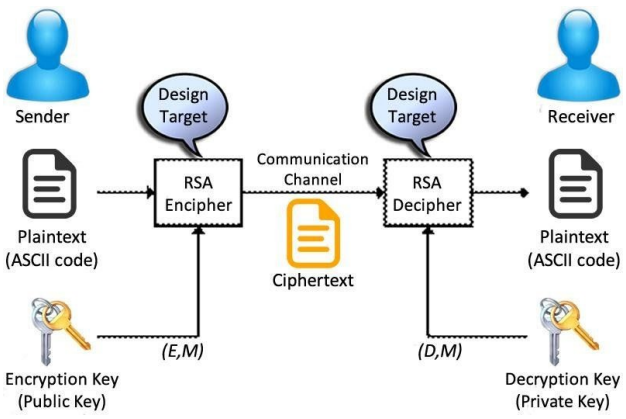
Primero se elijen dos números primos de gran tamaño (actualmente en base a la competencia de nuestros ordenadores >1024 bits), que se llamarán p y q.

Mediante formulas matemáticas adquirimos la clave primaria que tendrá la siguiente forma: (n,k).

Y para calcular la clave privada se elegirá un número j que verifique una ecuación matemática.

CIFRADO Y DESCIFRADO DE MENSAJES:

Mediante otras formulas matemáticas que hacen uso de nuestras claves, el mensaje es cifrado por el emisor y descifrado por el receptor (el emisor utiliza la clave pública (n,k) para cifrar el mensaje y el receptor hace uso tanto de la clave privada (j) como de una parte de la clave pública (n) para descifrarlo).



BIBLIOGRAFÍA

https://www.youtube.com/watch?v=CMe0COxZxb0

https://es.wikipedia.org/wiki/RSA

https://juncotic.com/rsa-como-funciona-este-algoritmo/