RSA: Criptografía con Números Primos

Proyecto Realizado por José Garrido Santamaría

Junta de Castilla y León

Índice y Objetivos

- ¿ Qué es el RSA?
- Base Teórica
- Aritmética Modular
- Criptografía de Clave Privada
- Criptografía de Clave Pública
- RSA
- Generación de Claves
- Cifrado RSA
- Usos del RSA
- Maple
- Futuro de la Criptografía
- Conclusiones y Agradecimientos

¿Qué es el RSA?

El RSA es el criptosistema de clave Pública más usado en la actualidad.

Fue inventado en 1979 por los matemáticos Ronald Rivest, Adi Shamir y Leonard Adleman.

Base Teórica

Para entender el RSA antes es necesario estudiar su base matemática:

En este proyecto hemos estudiado:

- La aritmética Modular
- Los números primos
- El algoritmo de Euclides
- El teorema Chino de los Restos
- La función φ, el teorema de Euler y el Pequeño teorema de Fermat.
- El cifrado y descifrado del RSA
- La seguridad del RSA
- Test de Rabin para encontrar números primos

Aritmética Modular

$$25 \equiv 1 \bmod 3$$

$$25 \div 3 = 3 \times 8+1$$

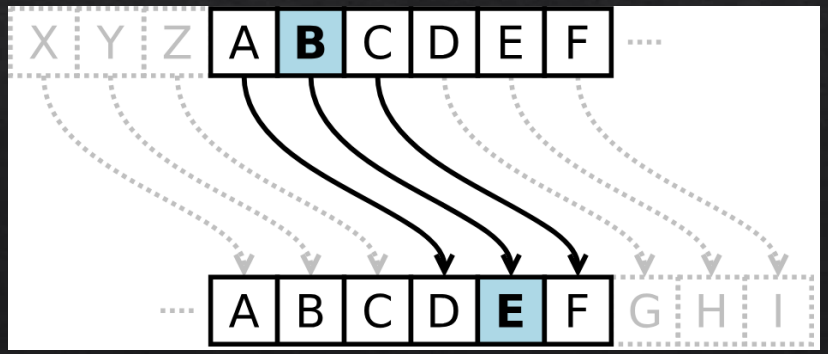
30 mod 24 = 6

12 + 6 = 18

Criptografía de Clave Privada

A envía un mensaje cifrado a B

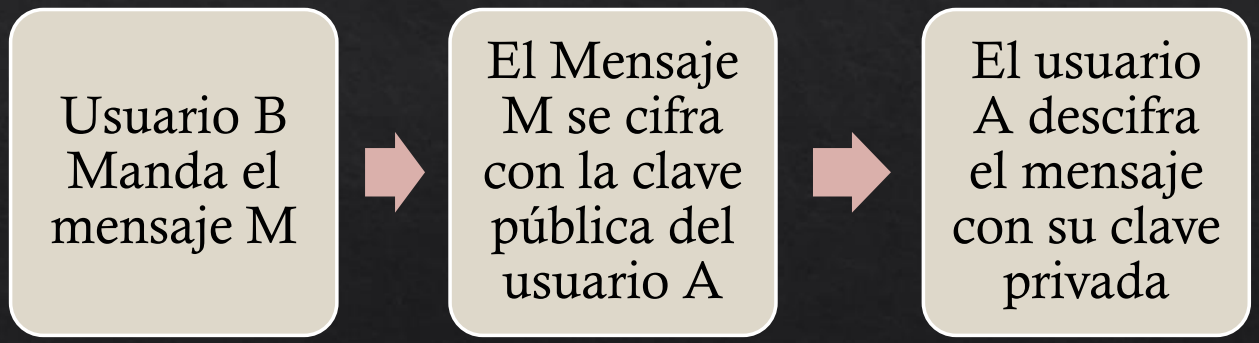
B descifra el mensaje usando la clave de descifrado



Criptografía de Clave Pública

En 1967 los ingenieros Whitfiel Diffie y Martin Hellman desarrollaron esta idea.

En este tipo de criptografía existen dos claves, una que es pública y otra privada.



No hace falta que A y B establezcan una clave previamente entre ellos.

RSA

La seguridad del RSA está basada en la dificultad de factorizar números muy grandes que son el producto de dos primos.

El protocolo del RSA consta de tres partes:

- La generación de las claves.
- El cifrado del mensaje.
- El descifrado del mensaje.

Generación de claves

Un usuario A (Alicia) elige dos claves, una pública y la otra privada.

A elije dos números primos p y q y los multiplica, obteniendo así n , n =(pq).

A partir de n, A calcula φ(n), e y d, siendo e el exponente de cifrado y d el exponente de descifrado. La clave pública será (n,e) y la privada (n,d)

Para que este cifrado sea seguro, es muy importante que A mantenga en secreto p, q, d y φ(n).

Cifrado RSA

Un usuario B (Bob) quiere enviar un mensaje a A (Alicia).

B consigue la clave pública de A → B representa su mensaje en un código numérico. → B cifra el mensaje con la clave pública de A

Descifrado RSA

Para descifrar el mensaje A solo necesita utilizar su clave privada.

Ejemplo RSA

Clave Pública de A de cifrado (n, e)

Clave Privada de A de descifrado (n,d)

B

A

Mensaje

"Hola"

Mensaje codificado (m)

"60003978"

Mensaje cifrado (C)

(150620011079823592158653482732475305921674219074663709505354723191601975682343471219684716700652001539212991396237591357027035674033142933364960616957269183891298174861191317)

Mensaje codificado (m)

"60003978"

Mensaje original

"Hola"

Cifrado

$C = m^e mod\ n$

Descifrado

$C^d \equiv m\ mod\ n$

n=

478269054622265064932567431792523013603361900549998170793372973076890964981924265924079149312941597981553607137912788051199286400459705574583270771585515768191019110265 2743103

e=

265804811327424323272984094910800930424618421334756975532604327831959727823029420257806825105057419853875705315118639834310640433563074188682112796612452586787883674214 2829625

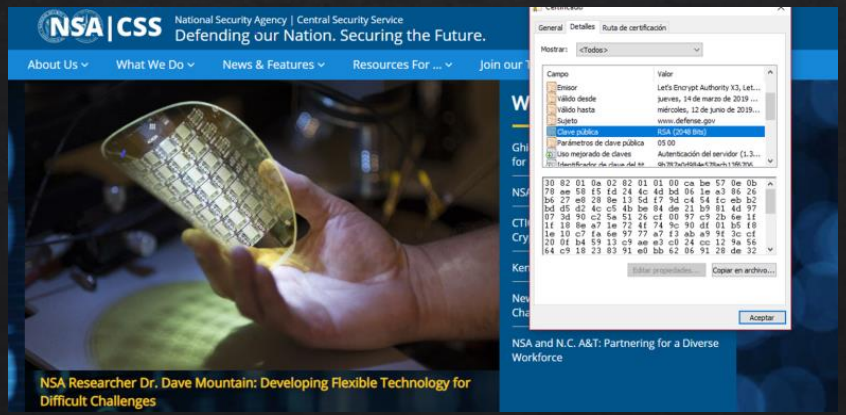
d=

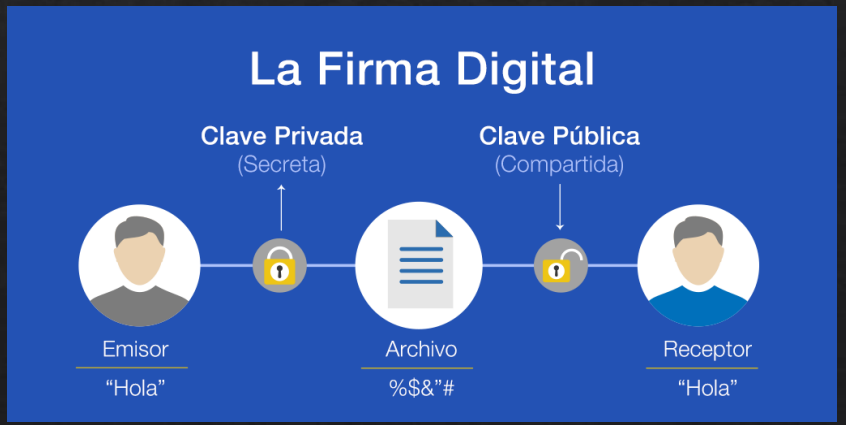
361882205034243795836104320451418808176736004975383287184034780966398391282057130277773762594693035810152770484537637311029168401883951096144161955825846328337724094128664887 3

Usos del RSA

RSA®

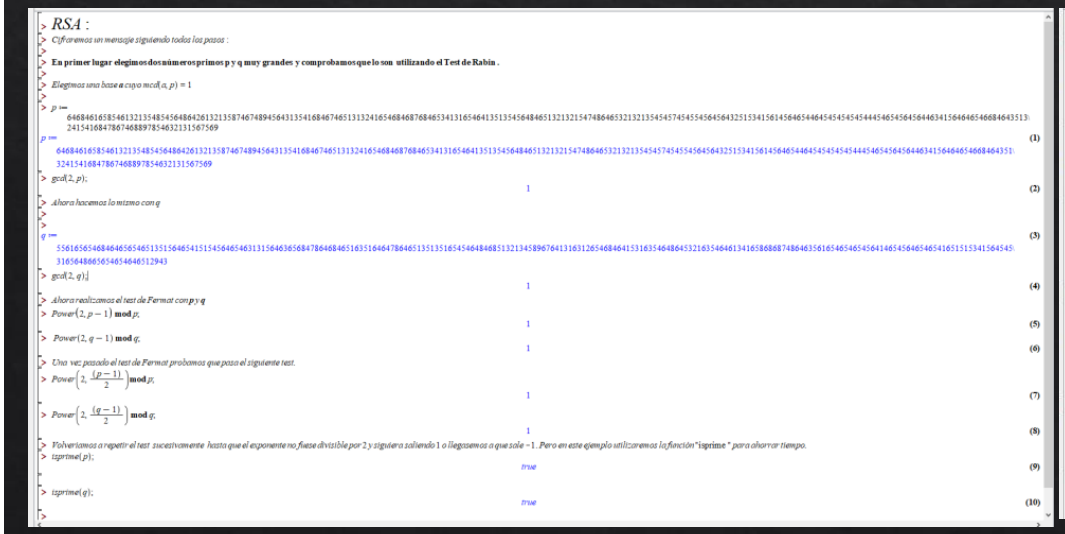
AES



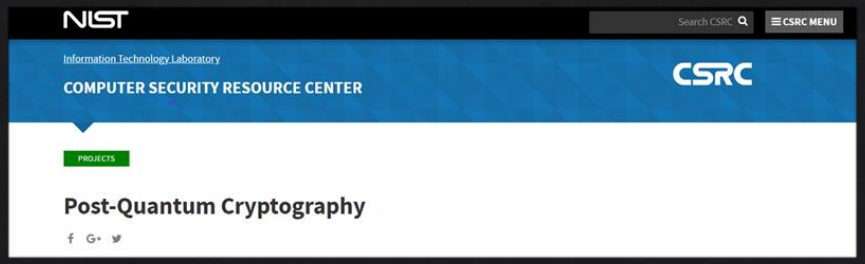


Maple

Maple es un programa de cálculo simbólico que nos permite realizar el proceso completo de cifrado.



Futuro de la Criptografía



Conclusiones

- Actualmente dependemos totalmente de la Criptografía y las matemáticas.
- El RSA sigue siendo uno de los sistemas de cifrado más seguros en la actualidad.
- Los programas de cálculo como Maple son de gran utilidad en este tipo de proyectos.
- El proyecto me ha parecido realmente interesante y se deberían realizar un mayor número de trabajos de este tipo.

Agradecimientos

- Agradecer al IES Andrés Laguna, a la Universidad de Valladolid y la Junta de Castilla y León el permitirme la oportunidad de realizar este proyecto.

- Especialmente, agradezco el apoyo y ayuda durante estos meses, a mis dos tutores: Rodrigo Santos Álvarez (IES Andrés Laguna) y Diego Ruano Benito (Uva)

FIN