PROYECTO FINAL DE MATEMÁTICAS DISCRETAS
ENCRIPTAMIENTO RSA
JUAN FRANCISCO CISNEROS

HISTORIA SOBRE EL ALGORITMO

RSA es un sistema criptográfico de clave publica que comenzó en 1979, el sistema utiliza factorización de números enteros. Sus siglas RSA provienen de los apellidos de sus desarrolladores Ron Rivest, Adi Shamir y Leonard Adleman. Aunque ellos no fueron quienes descubren el algoritmo pero quienes lo implementan gracias a Clifford Cocks un matemático quien había ya descrito el algoritmo antes.

Los mensajes enviados por el algoritmo se representan mediante números, y estos son multiplicados por dos números primos grandes que en la mayoría de casos son elegidos al azar y siempre mantenidos en secreto para evitar la desencriptación del mensaje por personas que no deben descifrar.

RSA será seguro siempre y cuando no se encuentre una manera fácil de obtener números primos, aun que se dice que con la computación cuántica los días del algoritmo son contados.

¿CÓMO FUNCIONA EL ALGORITMO?

El encriptamiento RSA se basa en factores y en números primos grandes, por ejemplo, los números primos 31 y 37, cuando los multiplicamos entre sí obtenemos 1147, es fácil de resolver, pero si hacemos lo contrario y en vez de obtener los primos tenemos como primera instancia 1147, deberemos ir por todos los números primos desde el 1 al infinito o en este caso desde el 1 al 37 para obtener 31 y 37, esto a una persona se le hace complicado, pero a una computadora no. Es por esto que a una computadora se les da valores tan grandes que hasta para estas son difíciles de resolver computacionalmente.

> Y entonces nos preguntamos ¿Cómo se crea un encriptamiento RSA?, bueno para este proyecto he creado un script en Python el cual encriptará un mensaje utilizando el algoritmo RSA. Pero antes de ejecutarlo deberemos de entender ¿como funciona?

Primero, tomaremos dos números primos grandes P y Q, en el caso de mi ejemplo en Python use números pequeños una vez más para entender el funcionamiento. Luego vamos a encontrar el producto de esos dos números, N=P*Q.

El algoritmo utiliza un número llamado el Euler Totient, o T que se calcula obteniendo el producto de P−1 por Q−1, entonces T= (P−1) * (Q−1).

Ahora elegiremos dos números E y D donde (E*D) Modulo T=1. E debe ser menor que T, y E debe ser coprimo con T y N. Y D no puede ser igual que E

Listo, tenemos todo para el encriptamiento. Deberemos publicar N y E, que son nuestras llaves publicas, estas son usadas por los demás usuarios para encriptar, pero no podrán desencriptar al menos de que tengamos N y D, que es nuestra llave privada.

Quisiera dar un ejemplo para entender como funcionaria entonces el algoritmo si quisiéramos encriptar una letra del abecedario en este caso B:

PASO 1 COMPLETO: OBTENER LAS LLAVES

1. Elegimos dos números primos, P=2 y Q=7
2. Obtenemos el producto de ambos, N=2*7=14
3. Calculamos el numero de Euler, “T”, T= (2−1) * (7−1) = 6
4. Obtenemos la llave de desencriptamiento y encriptamiento D y E respectivamente:

   ```
   (E*D) Modulo T = 1.
   (E*D) Modulo 6 =1.
   ```

5. He utilizado Excel para ayudarme a obtener E y D, adjunto aquí debajo una imagen de lo realizado:

ELEGIR E
DONDE E ES MENOR QUE 6
DONDE E ES COPRIMO CON 6 Y 14

OPCIONES	
1	DESCARTAMOS EL 1
2	ES FACTOR DE 6 Y 14
3	ES FACTOR DE 6
4	ES FACTOR DE 6 Y 14
5	

ELEGIR D
ELEGIR E*D MODULO 6=1
D NO PUEDE SER IGUAL QUE E

MULTIPLOS DE 5	MULTIPLOS * 5	MODULO 6
1	5	5
2	10	4
3	15	3
4	20	2
5	25	1
6	30	0
7	35	5
8	40	4
9	45	3
10	50	2
11	55	1
12	60	0
13	65	5
14	70	4
15	75	3
16	80	2
17	85	1
18	90	0
19	95	5
20	100	4

Mis elecciones son E=5, y D=11

Mis llaves publicas que podrán ser compartidas son: (5,14)

Mis llaves privadas que no podrán ser compartidas son: (11,14)

PASO 2: ENCRIPTAR LA LETRA “B”

6. Con la llave publica (5,14) vamos a enviar la letra “B”, como debemos trabajar con números, decimos que “B” = 2
7. Obtenemos el valor de encriptamiento que es la función , o la letra a encriptar elevado a la primera parte de la llave publica y a eso le sacamos el modulo de la segunda parte de la llave. Aveces debemos redondear.
8. El numero resultante en este caso 4 es el mensaje encriptado, para traducirlo a letras decimos entonces que 4=D, listo.

PASO 3: DESENCRIPTAR LA LETRA “D”

9. Con la llave privada (11,14) vamos a desencriptar la letra “D”, como debemos trabajar con números, decimos que “D” = 4

10. Obtenemos el valor de encriptamiento que es la función , o la letra a desencriptar elevado a la primera parte de la llave privada y a eso le sacamos el modulo de la segunda parte de la llave. A veces debemos redondear

11. El numero resultante en este caso 2 es el mensaje desencriptado, para traducirlo a letras decimos entonces que 2=B, listo. A veces debemos redondear

MI PROGRAMA DE ENCRIPTAMIENTO

Aquí en esta carpeta de entrega final adjunto el código creado con el funcionamiento del algoritmo, con este podremos obtener las llaves publicas y privadas, encriptar frases y desencriptarlas

Referencias

Geeks For Geeks (Ed.). (2021, Enero 5). *RSA algorithm in cryptography*. GeeksforGeeks. Obtenido en Diciembre 8, 2021, from https://www.geeksforgeeks.org/rsa-algorithm-cryptography/.

Ireland, D. (2018, Junio 9). *RSA Algorithm* . RSA algorithm. Obtenido en Diciembre 8, 2021, from https://www.di-mgt.com.au/rsa_alg.html.