Mª Joaquina Berral Yerón, Inmaculada Serrano Gómez

El cifrado RSA

Este método se basa en la dificultad de hallar los factores primos de un número n que sea producto de dos primos muy grandes. En principio es lo mismo tener los dos números primos que tener su producto: dados dos números es fácil multiplicarlos, y dado un número es teóricamente posible factorizarlo en producto de números primos[1]. Pero cuando hablamos de un número de tamaño 1024 bits (309 cifras en sistema decimal), intentar factorizarlo es computacionalmente impracticable.

Los ordenadores encuentran con rapidez números primos grandes y también pueden multiplicarlos en una milésima de segundo para obtener un resultado de doscientas cifras. Por ejemplo, esto se hace cada vez que se visita una página segura, el navegador genera sobre la marcha una nueva clave de usar y tirar. Pero, ¿cuánto cuesta descomponer en factores primos un número con doscientas cifras? Es prácticamente imposible, esto es lo que garantiza la seguridad del sistema.

El RSA es un algoritmo asimétrico que cifra en bloque y que utiliza una clave distribuida públicamente y otra privada guardada en secreto por su propietario. Si dos personas A y B se quieren comunicar con este método es el receptor B quien tiene *toda* la clave; el emisor A conoce la parte pública de la clave, que sirve para cifrar mensaje. El receptor guarda cuidadosamente la parte privada de la clave, que sirve para descifrar.

Vamos a ir haciendo todos juntos los pasos que se deben seguir para enviar un mensaje. Para entender bien el proceso usaremos números pequeños y cifraremos carácter a carácter. Ve calculando cada uno de los valores de los pasos y completa las tablas.

1. Generación de las claves (por parte del receptor del mensaje)

Paso 1. El receptor B selecciona dos números primos suficientemente grandes, p y q.
Por ejemplo, p =17 y q =2.

Paso 2. Halla $N = p \times q = 17 \times 2 = 34$.

Paso 3. Calcula la función indicador de Euler: $\Phi(N) = (p-1)\cdot(q-1) = 16 \times 1 = 16$

Esta función nos da la cantidad de números primos relativos con N y menores que N. Esto quiere decir que hay 16 números enteros x, tales que mcd(34, x)=1.

Paso 4. Selecciona un número e menor que $\Phi(N)$ y tal que mcd(e, $\Phi(N)$) = 1. Tomamos e =3 ya que mcd(3,16) = 1.

[1] Una forma posible de descomponer un número n en sus factores es probar a dividirlo por todos los números enteros positivos comprendidos entre 2 y la raíz de n. Por supuesto, a lo largo del tiempo los matemáticos han inventado otros métodos de factorización más eficientes, pero ninguno ha conseguido un algoritmo con un orden de complejidad que permita factorizar en un tiempo razonable números de tamaños como los empleados en RSA actualmente, aun con la potencia de los mejores ordenadores de hoy en día.

Elaborado por:
Profundiza
Federación Española de Sociedades de Profesores de Matemáticas
MINISTERIO DE EDUCACIÓN
SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL

Paso 5. Calcula el inverso de e en un reloj con $\Phi(N)$ horas. Es decir el número d que verifique que: $e \times d \equiv 1 (\text{mod } \Phi(N))$

Si $e = 3$ puedes comprobar que $d = 11$, si el reloj tiene 16 horas: $3 \times 11 = 33 = 1 (\text{mod} 16)$

Precisamente el pequeño teorema de Fermat y el resultado de Euler garantizan que este número existe y es único. Los cálculos anteriores se pueden hacer con relativa facilidad. Para obtener d se puede usar el Algoritmo extendido de Euclides (consulta el apartado para saber más)

Paso 6. La clave pública está constituida por $(N, e) = (34, 3)$ y la secreta por $(N, d) = (34, 11)$

Ahora que B tiene la clave, anuncia la parte pública a todo el mundo que nos quiera mandar mensajes (la misma clave pública sirve para cualquier persona que se quiera comunicar con él). La clave secreta la conserva celosamente el receptor. Ese par de claves es tal que aún conociendo una de ellas es casi imposible calcular la otra.

2. Cifrado del mensaje (por parte del emisor)

Para cifrar, el emisor A realiza los pasos siguientes:

Paso 7. Localiza la clave pública del destinatario para conocer los valores de **N** y e.

En nuestrao caso: $(N, e) = (34, 3)$

Paso 8. Utiliza la función: $C \equiv M^e \ (\text{mod } N)$ siendo M del mensaje original y C del cifrado.

Texto claro	V	I	E	R	N	E	S
Texto expresado en numerous (M)	26	8					
Mensaje cifrado $C \equiv M^e \ (\text{mod } N)$	32	2					

Paso 9. Envía al destinatario el criptograma C.

3. Descifrado del criptograma por parte del receptor

Paso 10. Si el destinatario B quiere recuperar el mensaje que ha recibido usa su clave privada d para calcular: $M \equiv C^d \ (\text{mod } N)$

Texto recibido	32	2	30	18	21	30	25
Texto descifrado: $D = C^d \ (\text{mod } N)$	26	8					
Texto claro	V	I					

Con este ejemplo has aprendido a cifrar usando un sistema de clave pública pero no olvides que en realidad es bastante más complicado ya que en nuestra simulación se han usado valores de p, q y e muy pequeños y se ha cifrado carácter a carácter. En la realidad se usan números primos enormes y se cifra en bloque pero esto requiere el uso de cálculos tan enormes que se necesitan ordenadores de gran potencia para calcularlos.

Elaborado por:
Federación Española de Sociedades de Profesores de Matemáticas
MINISTERIO DE EDUCACIÓN
SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL