Sistema de Cifrado RSA

- El sistema de cifrado RSA es el sistema de cifrado asimétrico más usado y más sencillo de entender e implementar.
- Una peculiaridad de este algoritmo es que sus dos claves sirven indistintamente tanto para cifrar como para autenticar.
- Debe su nombre a sus tres inventores: Ronald **Rivest**, Adi **Shamir** y Leonard **Adleman**, que publicaron por primera vez el método RSA en 1977.
- Se basa en la dificultad que presenta la factorización de números grandes.

1

Sistema de Cifrado RSA (cont.)

- Las claves **pública** y **privada** se calculan a partir de un número que se obtiene como producto de dos primos grandes.
- Un atacante que quiera recuperar un texto claro a partir del criptograma y de la clave pública, tiene que enfrentarse a dicho problema de factorización.
- El algoritmo consta de tres pasos:
  - Generación de claves
  - Cifrado del mensaje
  - Descifrado del mensaje

2

Sistema de Cifrado RSA
Generación de Claves

- Cada usuario elige dos números primos distintos y grandes *p* y *q* (unas 200 cifras cada uno).
  - Por seguridad deben ser elegidos de forma aleatoria y tener una longitud en bits parecida. Se pueden hallar primos fácilmente mediante test de primalidad.
- Se calcula el producto $n = pq$
  - *n* se usa como el módulo para ambas claves: pública y privada
- Se calcula el grupo (Zn)*, cuyo orden es $\varphi(n) = (p-1)(q-1)$
  - ϕ es la función de Euler
- Se escoge un número entero positivo e menor que $\varphi(n)$, que sea primo relativo con $\varphi(n)$, *e* se usa como el exponente de la clave pública.

Sistema de Cifrado RSA
Generación de Claves

- Se determina el inverso de e en (Zn)*: d, es decir un d (mediante aritmética modular) que satisfaga la congruencia $ed \equiv 1 \pmod{\varphi(n)}$ → $ed \equiv 1 \pmod{(p-1)(q-1)}$, *d* se usa como el exponente de la clave privada
  - *d* es el inverso modular de *e* mod ϕ(*n*)
  - Se calcula mediante el algoritmo de Euclides
  - Se cumple que $ed = 1 + k(p-1)(q-1)$ para cualquier entero *k*.
- La **clave pública** será el par de números (*e*,*n*), que pueden ser conocidos por cualquiera.
- La **clave privada** será el par de números (*d*,*n*), este número *d* debe mantenerse secreto y sólo será conocido por el propietario del par de claves.
- Se deben mantener ocultos también los valores de p, q y φ(n).

Sistema de Cifrado RSA
Generación de Claves

- Para una mayor eficiencia los siguientes valores se calculan de antemano y se almacenan como parte de la clave privada:
  - Los primos para la generación de las claves: p y q.
  - $d \bmod (p-1)$ y $d \bmod (q-1)$
  - $q^{-1} \bmod p$

5

Sistema de Cifrado RSA
Cifrado y Descifrado del Mensaje

- Los mensajes que se cifran y descifran con este algoritmo son números enteros de tamaño menor que n, no letras sueltas como en el caso de los cifrados vistos antes.
- Para obtener el mensaje cifrado C a partir del mensaje original M se realiza la siguiente operación:
  $\boldsymbol{C = M^e \ (mod\ n)}$
- Para recuperar el mensaje original M a partir del cifrado C se realiza la siguiente operación:
  $\boldsymbol{M = C^d \ (mod\ n)}$

6

Fortaleza del algoritmo RSA

¿Qué fortaleza tendrá este algoritmo ante ataques?

- El intruso que desee conocer la clave secreta **d** a partir de los valores públicos **n** y **e** se enfrentará al Problema de la Factorización de Números Grandes (PFNG) puesto que la solución para conocer esa clave privada pasa por deducir el valor del Indicador de Euler $\phi(n) = (p-1)(q-1)$ para así poder encontrar el inverso de la clave pública $d = inv\ [e,\phi(n)]$.
- Existen, no obstante, otros tipos de ataques a este sistema que no pasan por la factorización de n.

Ejemplo de cifrado y descifrado con RSA

Grupo $n = 91 = 7*13$; $\phi(n) = \phi(7*13) = (7-1)(13-1) = 72$ M = 48
Elegimos e = 5 pues mcd (5,72) = 1 ∴ d = inv(5,72) = 29
CIFRADO:
$C = M^e \bmod n = 48^5 \bmod 91 = 5245.803.968 \bmod 91 = 55$
DESCIFRADO:
$M = C^d \bmod n = 55^{29} \bmod 91 = 48$ ... 55^{29} ya es "*número grande*"

55^{29} es un número con 51 dígitos...
$55^{29} = 295473131755644748809642476009391248226165771484375$

Sistema de Cifrado RSA
Ejemplo

- Cifrar STOP con RSA (use números primos pequeños)
  - *p* = 43 y *q* = 59, *n* = 43*59 = 2537
  - *mcd*(*e*,42*58) = *mcd*(13,42*58) = 1
  - Clave pública *Kp* = (13,2537)
  - STOP se pasa a números según la posición y se agrupan en bloques de cuatro dígitos: 1819 1415
  - Se usa la operación para cifrar:

$$C_1 = 1819^{13} \bmod 2537 = 2081$$

$$C_2 = 1415^{13} \bmod 2537 = 2182$$

  - El mensaje cifrado es: 2081 2182

9

Sistema de Cifrado RSA
Ejemplo

- Descifrar 0981 0461 con RSA (use números primos pequeños)
  - *d* = 937 (es el inverso de 13 módulo 42*58=2436)
  - Clave privada *KP* = (937,2537)
  - Se usa la operación para descifrar:

$$M_1 = 0981^{937} \bmod 2537 = 0704$$

$$M_2 = 0461^{937} \bmod 2537 = 1115$$

  - El mensaje descifrado es: 0704 1115
  - Se pasan las posiciones a letras: HELP

10

Referencias

- Ramírez Benavides, Kryscia Daviana. “Estructuras Discretas”
- Ramió Aguirre, Jorge. “Seguridad Informática y Criptografía”