

RSA

(Rivest, Shamir y Adleman)

Ing. Max Alejandro Antonio Cerna Flores

Agenda

— — —

Definición

Seguridad

Factorización de Números Enteros Grandes

El problema RSA

Proceso de Generación de claves

Proceso de Cifrado y Descifrado

Definición

El nombre RSA proviene de las iniciales de sus tres creadores, Rivest, Shamir y Adleman, allá por 1977.

Es un sistema criptográfico de clave pública, utiliza factorización de números primos enteros. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

El funcionamiento se basa en el producto, conocido, de dos números primos grandes elegidos al azar y mantenidos en secreto.

Seguridad

Está basado en dos problemas matemáticos: el problema de factorizar números grandes y el problema RSA.

Si el valor N es lo suficientemente grande el algoritmo RSA es seguro. Si N tiene 256 bits o menos, puede ser factorizado en pocas horas con un ordenador personal.

Factorización de Números Enteros Grandes

Consiste en descomponer un número compuesto entero positivo no primo que tiene una única descomposición en números primos o factores primos.

Cuando los números son muy grandes no se conoce ningún algoritmo que resuelva eficientemente este problema.

Los números primos son aquellos que solo son divisibles entre 1 y ellos mismos.

Factorización de Números Enteros Grandes

— — —

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67
71	73	79	83	89	97	101	103	107	109	113	127	131	137	139	149	151	157	163
167	173	179	181	191	193	197	199	211	223	227	229	233	239	241	251	257	263	269
271	277	281	283	293	307	311	313	317	331	337	347	349	353	359	367	373	379	383
389	397	401	409	419	421	431	433	439	443	449	457	461	463	467	479	487	491	499
503	509	521	523	541	547	557	563	569	571	577	587	593	599	601	607	613	617	619
631	641	643	647	653	659	661	673	677	683	691	701	709	719	727	733	739	743	751
757	761	769	773	787	797	809	811	821	823	827	829	839	853	857	859	863	877	881
883	887	907	911	919	929	937	941	947	953	967	971	977	983	991	997			

Factorización de Números Enteros Grandes

— — —

Números Coprimos

Son dos números enteros “a” y “b” que no tienen ningún factor primo en común.

O sea son coprimos, si y sólo si, su máximo común divisor (MCD) es igual a 1.

Factorización de Números Enteros Grandes

Ejemplos

10 y 12 **no** son coprimos ya que el 2 es su divisor en común.

2 y 3 son coprimos porque el máximo común divisor es 1.

67 tiene de divisores 1,67

12 tiene de divisores 1,2,3,4,6,12

67 y 12 solo tienen el 1 en común por tanto son coprimos.

Problema RSA

Se refiere a la dificultad de efectuar una operación de clave privada mediante el sistema criptográfico RSA conociendo tan solo la clave pública.

Para números suficientemente grandes mayores de 1024 bits no se conoce un método eficiente de factorización.

Proceso

Generación de claves:

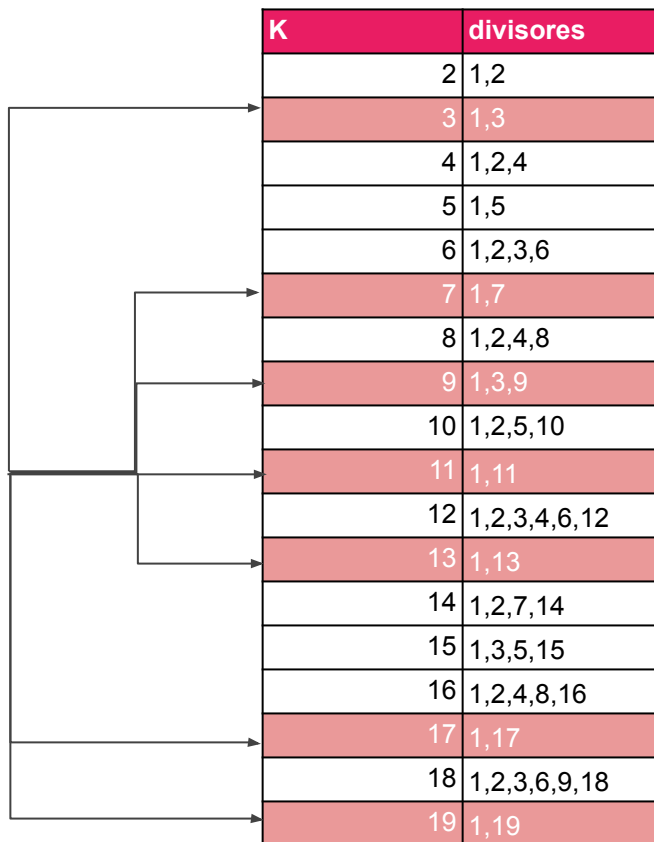
1. Seleccionar dos números primos **p** y **q** (ej: $p=3$, $q=11$)
2. Calcular **n** = $p * q$ (ej: $n = 3 * 11 = 33$)
3. Calcular **z** = $(p-1) * (q-1)$ (ej: $z = (3-1)*(11-1) = 20$)
4. Se elige un número primo **k**, tal que k sea coprimo a z.

$$\text{MCD}(k, z) = 1$$

$$1 < k < z$$

Proceso

Coprimos



K	divisores
2	1,2
3	1,3
4	1,2,4
5	1,5
6	1,2,3,6
7	1,7
8	1,2,4,8
9	1,3,9
10	1,2,5,10
11	1,11
12	1,2,3,4,6,12
13	1,13
14	1,2,7,14
15	1,3,5,15
16	1,2,4,8,16
17	1,17
18	1,2,3,6,9,18
19	1,19

$$z = 20 = \{1,2,4,5,10\}$$

K posibles =>

3, 7, 11, 13, 17 o 19

Proceso

Generación de claves:

5. clave pública (n,k) (ej: {n=33,k=7})
6. calcular clave privada (j)

donde j es un número entero grande que debe cumplir con:

$$(k*j) \bmod z = 1$$

$$k = 7$$

$$z = 20$$

Proceso

— — —

$$k = 7$$

$$z = 20$$

j	k*j	(k*j)mod z
1	7	7
2	14	14
3	21	1
4	28	8
5	35	15
6	42	2
7	49	9
8	56	16
9	63	3
10	70	10
11	77	17
12	84	4
13	91	11
14	98	18
15	105	5
16	112	12
17	119	19

$$(k*j) \bmod z = 1$$

$$j = 3$$

Cifrado

Fórmula de cifrado (emisor):

$$C = M^k \bmod n$$

clave pública (n,k) ($\{n=33, k=7\}$) y M es el mensaje a enviar,
por ejemplo:

$$M = 17$$

$$C = 17^7 \bmod 33$$

$$C = 8$$

Descifrado

Fórmula de descifrado (receptor):

$$M = C^j \bmod n$$

clave privada $\{n=33, j=3\}$ y mensaje cifrado $C=8$:

$$M = 8^3 \bmod 33$$

$$C = 17$$