Criptografía de clave pública. El sistema RSA

Estímulo del Talento Matemático

Real Academia de Ciencias

20 de mayo de 2006

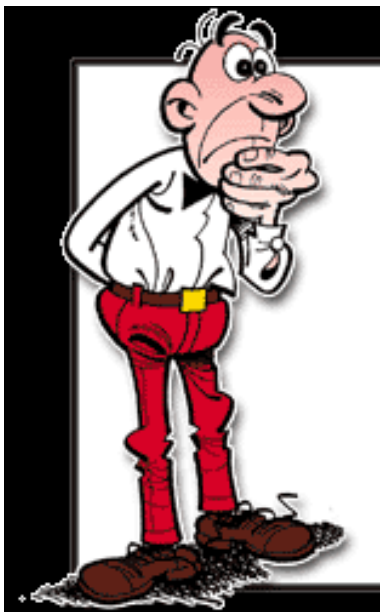
Intercambio de claves

En 1976, Diffie y Hellman presentaron un sistema de **intercambio de claves**. Con este sistema, dos personas que no comparten ninguna información pueden ¡en una discusión pública! acordar una clave secreta. . . **paradójico**, ¿no?

Vamos a ver cómo Mortadelo y Filemón, los dos superagentes de la T.I.A, pueden acordar una clave, que utilizarán para mandarse mensajes secretos.

¡Recordemos que la temible organización A.B.U.E.L.A. está al acecho!

Mortadelo y Filemón consultan al Profesor Bacterio, que les muestra qué deben hacer.



Ya vimos el juego de los dos candados. Ahora queremos diseñar un procedimiento **matemático** análogo.

Primer intento

Mortadelo y Filemón hacen público un número s. Más aún, no tienen reparos en afirmar que van a utilizar la función

$$\boxed{s^x}$$

Es decir, que para transmitir el número x, lo "enmascararán" transformándolo en s^x.

1. Mortadelo elige un número m (su "candado", que sólo él conoce) y se lo transmite a Filemón como s^m.

2. Filemón elige un número f (secreto). Y le envía a Mortadelo el número s^f.

3. Mortadelo ha recibido el número s^f. Lo eleva a su número secreto m y obtiene

$$(s^f)^m = s^{f\,m}$$

4. Por su parte, Filemón, que ha recibido s^m, hace la misma operación, pero con su número secreto f:

$$(s^m)^f = s^{m\,f}$$

¡Han conseguido ponerse de acuerdo en un número común! (y no han tenido que compartir sus números secretos)

Una vez hecho esto, Mortadelo y Filemón pueden enviarse mensajes codificando y descodificando con algún método que use esa clave.

Problemas del procedimiento:

- Primero, si los números involucrados (s, m y f) son grandes, entonces los cálculos de las potencias son enormes.
- Pero, más importante. Pongámonos en la piel de los espías de la A.B.U.E.L.A. Conocen el número s, pues es público, y también la "receta" de codificación (elevar s al número que corresponda).
  - Si interceptan el mensaje enviado por Mortadelo, s^m, pueden obtener el número m.
  - Y si captan el enviado por Filemón, s^f, recuperarán f.
  - Una vez conocidos estos dos números, pueden obtener la clave $s^{m\,f}$.

> Digamos, por ejemplo, que $s = 3$. Espiando, descubrimos que Mortadelo ha enviado 81, que sabemos que es 3^m, para un cierto m. ¿Cuál?
> ¿Y si hubiéramos interceptado 16677181699666569?
> En las calculadoras tenemos la función **logaritmo** (decimal, neperiano, en base 2, en base 3, etc.) que nos permite obtener la respuesta.

No parece que el procedimiento sea muy bueno. . .

Pero, ¿y si hacemos todos los cálculos anteriores en la aritmética del reloj?

Segundo intento

Para empezar, se ponen de acuerdo en un número primo p (¿por qué primo?, luego lo veremos) y un entero s menor que p. Los números p y s pueden hacerse públicos.

1. Mortadelo escoge un entero $a < p$ y calcula

$$\alpha = s^a \pmod{p}.$$

El resultado, α, es un número entre 0 y $p - 1$.

Filemón escoge un entero $b < p$ y calcula

$$\beta = s^b \pmod{p}.$$

Cada uno envía el resultado de sus cálculos (α y β) al otro.

2. Ahora, Mortadelo calcula

$$\beta^a \equiv s^{ba} \pmod{p}$$

y Filemón calcula

$$\alpha^b \equiv s^{ab} \pmod{p}.$$

3. Los dos han obtenido el mismo valor $k = s^{ab}$ (de nuevo, un número entre 0 y $p - 1$) que constituye la **clave secreta** con la que van a comunicarse.

¿Y la A.B.U.E.L.A, qué hace?

Como veremos, casi nada. Pero, para entender las ventajas de este procedimiento, debemos estudiar las $potencias$ en la aritmética del reloj.

Cálculo de potencias

Queremos calcular cantidades del tipo 2^{95}, 14^{346}, $(-13)^{23}$ módulo un cierto n.

> ¿Cómo de "grande" es 2^{95}? Para hacernos una idea, ¿cuánto tardaría un ordenador en mostrar en la pantalla todos los números del 1 al 2^{95}?

Por ejemplo, calculemos 2^{95} módulo 9.

$$\begin{array}{rcccccccccc} & 2 & 2^2 & 2^3 & 2^4 & 2^5 & 2^6 & 2^7 & 2^8 & \cdots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ \text{módulo } 9 \longrightarrow & & & & & & & & & \end{array}$$

¿Ocurre algo que simplifique el cálculo? Veamos otros ejemplos:

$$\begin{array}{rcccccccc} & 2 & 2^2 & 2^3 & 2^4 & 2^5 & 2^6 & 2^7 & \cdots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ \text{módulo } 7 \longrightarrow & & & & & & & & \end{array}$$

$$\begin{array}{rcccccccc} & 5 & 5^2 & 5^3 & 5^4 & 5^5 & 5^6 & 5^7 & \cdots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ \text{módulo } 7 \longrightarrow & & & & & & & & \end{array}$$

¿Ocurrirá siempre, sea cual sea la cuenta que hagamos?

Periodicidad y patrones

Sumas y productos

Estamos en módulo 7. Y calculamos

$2+0\equiv$	$3+0\equiv$	$5+0\equiv$	$2\times 0\equiv$	$3\times 0\equiv$	$5\times 0\equiv$
$2+1\equiv$	$3+1\equiv$	$5+1\equiv$	$2\times 1\equiv$	$3\times 1\equiv$	$5\times 1\equiv$
$2+2\equiv$	$3+2\equiv$	$5+2\equiv$	$2\times 2\equiv$	$3\times 2\equiv$	$5\times 2\equiv$
$2+3\equiv$	$3+3\equiv$	$5+3\equiv$	$2\times 3\equiv$	$3\times 3\equiv$	$5\times 3\equiv$
$2+4\equiv$	$3+4\equiv$	$5+4\equiv$	$2\times 4\equiv$	$3\times 4\equiv$	$5\times 4\equiv$
$2+5\equiv$	$3+5\equiv$	$5+5\equiv$	$2\times 5\equiv$	$3\times 5\equiv$	$5\times 5\equiv$
$2+6\equiv$	$3+6\equiv$	$5+6\equiv$	$2\times 6\equiv$	$3\times 6\equiv$	$5\times 6\equiv$
$2+7\equiv$	$3+7\equiv$	$5+7\equiv$	$2\times 7\equiv$	$3\times 7\equiv$	$5\times 7\equiv$
$2+8\equiv$	$3+8\equiv$	$5+8\equiv$	$2\times 8\equiv$	$3\times 8\equiv$	$5\times 8\equiv$

Ahora en módulo 12:

$2+0\equiv$	$3+0\equiv$	$5+0\equiv$	$2\times 0\equiv$	$3\times 0\equiv$	$5\times 0\equiv$
$2+1\equiv$	$3+1\equiv$	$5+1\equiv$	$2\times 1\equiv$	$3\times 1\equiv$	$5\times 1\equiv$
$2+2\equiv$	$3+2\equiv$	$5+2\equiv$	$2\times 2\equiv$	$3\times 2\equiv$	$5\times 2\equiv$
$2+3\equiv$	$3+3\equiv$	$5+3\equiv$	$2\times 3\equiv$	$3\times 3\equiv$	$5\times 3\equiv$
$2+4\equiv$	$3+4\equiv$	$5+4\equiv$	$2\times 4\equiv$	$3\times 4\equiv$	$5\times 4\equiv$
$2+5\equiv$	$3+5\equiv$	$5+5\equiv$	$2\times 5\equiv$	$3\times 5\equiv$	$5\times 5\equiv$
$2+6\equiv$	$3+6\equiv$	$5+6\equiv$	$2\times 6\equiv$	$3\times 6\equiv$	$5\times 6\equiv$
$2+7\equiv$	$3+7\equiv$	$5+7\equiv$	$2\times 7\equiv$	$3\times 7\equiv$	$5\times 7\equiv$
$2+8\equiv$	$3+8\equiv$	$5+8\equiv$	$2\times 8\equiv$	$3\times 8\equiv$	$5\times 8\equiv$
$2+9\equiv$	$3+9\equiv$	$5+9\equiv$	$2\times 9\equiv$	$3\times 9\equiv$	$5\times 9\equiv$
$2+10\equiv$	$3+10\equiv$	$5+10\equiv$	$2\times 10\equiv$	$3\times 10\equiv$	$5\times 10\equiv$
$2+11\equiv$	$3+11\equiv$	$5+11\equiv$	$2\times 11\equiv$	$3\times 11\equiv$	$5\times 11\equiv$
$2+12\equiv$	$3+12\equiv$	$5+12\equiv$	$2\times 12\equiv$	$3\times 12\equiv$	$5\times 12\equiv$
$2+13\equiv$	$3+13\equiv$	$5+13\equiv$	$2\times 13\equiv$	$3\times 13\equiv$	$5\times 13\equiv$

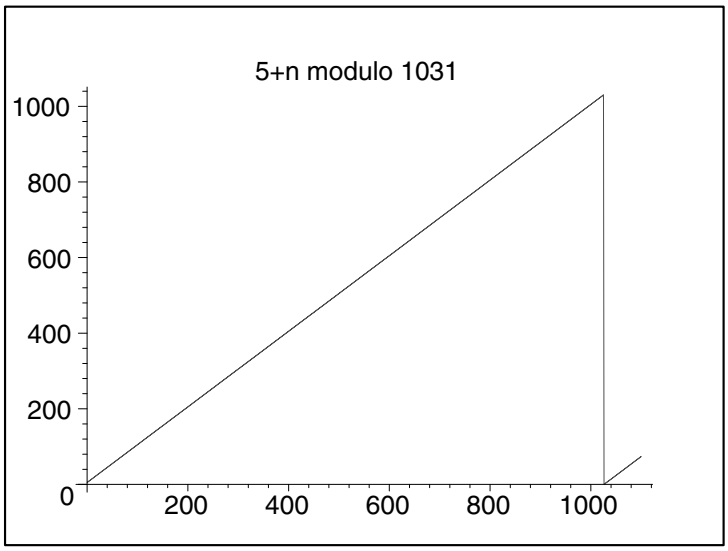
Vamos con las **potencias**. En módulo 7, de nuevo, calculamos

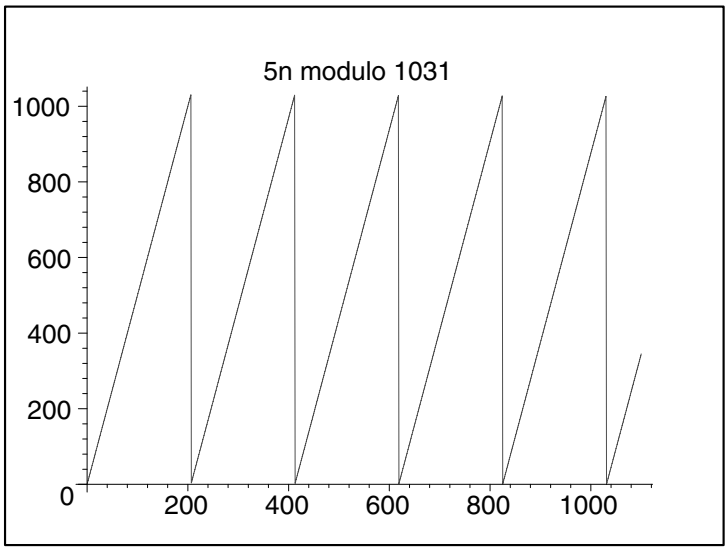
$$\begin{array}{l|l|l|l} 2^0 \equiv & 3^0 \equiv & 5^0 \equiv & 6^0 \equiv \\ 2^1 \equiv & 3^1 \equiv & 5^1 \equiv & 6^1 \equiv \\ 2^2 \equiv & 3^2 \equiv & 5^2 \equiv & 6^2 \equiv \\ 2^3 \equiv & 3^3 \equiv & 5^3 \equiv & 6^3 \equiv \\ 2^4 \equiv & 3^4 \equiv & 5^4 \equiv & 6^4 \equiv \\ 2^5 \equiv & 3^5 \equiv & 5^5 \equiv & 6^5 \equiv \\ 2^6 \equiv & 3^6 \equiv & 5^6 \equiv & 6^6 \equiv \\ 2^7 \equiv & 3^7 \equiv & 5^7 \equiv & 6^7 \equiv \\ 2^8 \equiv & 3^8 \equiv & 5^8 \equiv & 6^8 \equiv \end{array}$$

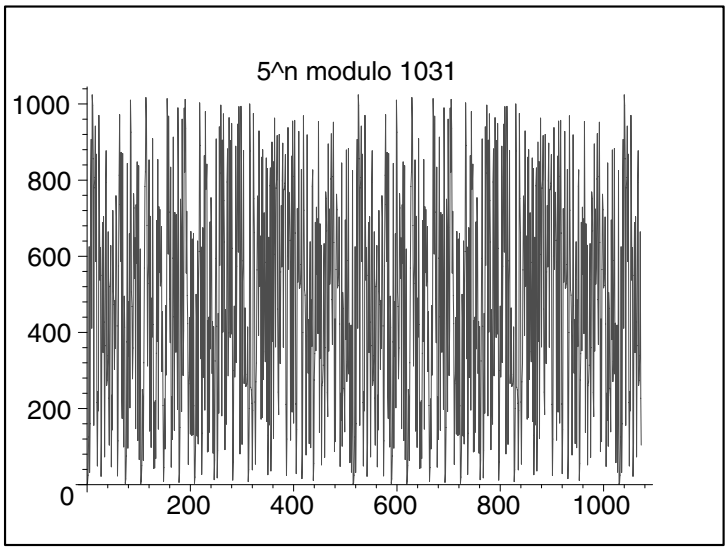
En módulo 12:

$$\begin{array}{l|l|l|l} 2^0 \equiv & 3^0 \equiv & 5^0 \equiv & 7^0 \equiv \\ 2^1 \equiv & 3^1 \equiv & 5^1 \equiv & 7^1 \equiv \\ 2^2 \equiv & 3^2 \equiv & 5^2 \equiv & 7^2 \equiv \\ 2^3 \equiv & 3^3 \equiv & 5^3 \equiv & 7^3 \equiv \\ 2^4 \equiv & 3^4 \equiv & 5^4 \equiv & 7^4 \equiv \\ 2^5 \equiv & 3^5 \equiv & 5^5 \equiv & 7^5 \equiv \\ 2^6 \equiv & 3^6 \equiv & 5^6 \equiv & 7^6 \equiv \\ 2^7 \equiv & 3^7 \equiv & 5^7 \equiv & 7^7 \equiv \\ 2^8 \equiv & 3^8 \equiv & 5^8 \equiv & 7^8 \equiv \\ 2^9 \equiv & 3^9 \equiv & 5^9 \equiv & 7^9 \equiv \\ 2^{10} \equiv & 3^{10} \equiv & 5^{10} \equiv & 7^{10} \equiv \\ 2^{11} \equiv & 3^{11} \equiv & 5^{11} \equiv & 7^{11} \equiv \\ 2^{12} \equiv & 3^{12} \equiv & 5^{12} \equiv & 7^{12} \equiv \\ 2^{13} \equiv & 3^{13} \equiv & 5^{13} \equiv & 7^{13} \equiv \end{array}$$

El aspecto de las gráficas:







Los malvados de la A.B.U.E.L.A. quieren obtener la clave secreta que han acordado Mortadelo y Filemón, y para eso espían las comunicaciones.

Saben, primero, los valores de s y p (pues son públicos), y conocen también el mecanismo que se está utilizando.

Pero, por supuesto, no saben qué elecciones de a y b han hecho Mortadelo y Filemón. Pero, interceptando la comunicación, obtienen los valores de α y β.

Si a partir de ellos logran obtener a y b, habrán roto la seguridad del sistema (con ellos, pueden calcular k). ¡El mundo en peligro!

Pero claro, para esto necesitarían calcular el "logaritmo" (en la aritmética del reloj de p posiciones). Fijémonos en el siguiente cálculo, donde s y p son públicos:

$$\alpha \equiv s^a \pmod{p}.$$

Si conocemos a, calcular α es muy sencillo. Pero si lo que tenemos es α, ¿cómo obtenemos a?

El problema es extremadamente difícil. Compara los dos siguientes cálculos:

- encontrar a tal que $5^{23} = a$ módulo 1031;
- encontrar a tal que $5^a = 970$ módulo 1031;

Ya hemos solucionado el problema del intercambio de claves, pero todavía queda el asunto del número de claves necesarias.

El sistema RSA

Después de que, en 1976, Diffie y Hellman asombraran al mundo con su sistema de intercambio de claves y propusieran el concepto de cifrado asimétrico, en 1977 aparece el llamado sistema RSA, uno de los primeros criptosistemas de clave pública (y todavía muy usado hoy en día). Su nombre se debe a sus autores Rivest, Shamir y Adleman[1].

Queremos diseñar un sistema para que una serie de usuarios se comuniquen entre sí. Nuestros objetivos son:

- que no sea necesario el intercambio de claves;
- que haya, esencialmente, una clave por usuario (en lugar de una clave por cada *pareja* de usuarios).
- Y, claro, que sea *seguro*. Es decir, que sea "prácticamente imposible" que un "espía" pueda *romper el sistema*, leyendo mensajes ajenos o haciéndose pasar por algún usuario.

[1] Aunque recientemente se ha sabido que el servicio secreto británico había diseñado un sistema semejante unos años antes.

Los sistemas de criptografía de clave pública (entre los que el sistema RSA es, quizás, el más famoso) se utilizan en un montón de situaciones reales:

- controles de acceso (por ejemplo, el sistema de contraseñas para acceder a un ordenador);
- identificación de personas (por ejemplo, cuando usamos las tarjetas de los cajeros o cuando nos comunicamos elctrónicamente con el banco);
- autentificación (las firmas digitales que garantizan que alguien es quien dice ser electrónicamente), etc.

Que el proceso de cifrado sea "prácticamente imposible" de deshacer quiere decir que el tiempo que llevaría sería demasiado largo como para que resultara útil en la práctica.

Lo que hay detrás de todos estos procedimientos son unas funciones matemáticas que suelen llamarse *funciones trampa o ratonera*.

Ya vimos un ejemplo, en el protocolo de Diffie-Hellman: elevar un número a otro en la aritmética del reloj de p posiciones (la tarea "fácil"), frente al cálculo del "logaritmo" en la aritmética de un reloj de p posiciones (la tarea inversa, y "difícil").

La clave del sistema RSA es que es **fácil multiplicar** números, mientras que es **muy difícil** el proceso inverso, **encontrar los factores primos** de un número.

¿Por qué es difícil factorizar?

Eso de que es muy difícil factorizar un número en primos. . . ¡pero si lo aprendimos hace mucho en el colegio!

Mira: por ejemplo, tomo el número 486 y como veo que es par divido por 2 y me queda 243. Éste no es par, pero enseguida veo que es múltiplo de 3; divido y me queda 81, que me suena mucho porque es $9^2 = 3^4$. Y si no me suena da igual, yo sigo dividiendo por 3 y llego a lo mismo, o sea que $486 = 2 \times 3^5$. Y ya está.

¿Y si el número es 713? No es mucho más grande que el anterior, pero no es par, ni es divisible por 3, ni por 5, ni por 7 (me basta ir probando con los números primos) . . . ni por 11, ni por 13, ni por 17 . . . esto se está poniendo feo . . . ni por 19. ¡Ah!, menos mal, se puede dividir por 23 y sale 31, que también es primo. En resumen, $713 = 23 \times 31$. Bueno, ha costado algo más, pero lo hemos conseguido.

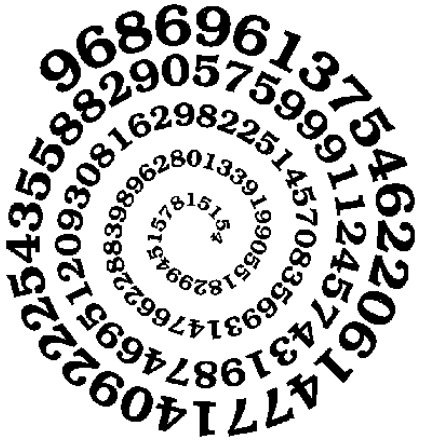
¿Todavía crees que factorizar es fácil? Pues inténtalo con el número $n = 23360947609$. ¡Glub!. . . El "primer" número primo que divide a este n es $p = 152041$. ¿Cuánto habrías tardado en encontrarlo?

Bueno, pero es cuestión de tiempo, y con los ordenadores actuales el tiempo no es un problema. . .

En realidad, sí lo es y para hacernos una idea, con este método de probar a dividir entre los primos, desde 2 en adelante (observando que basta con probar hasta llegar a $\sqrt{n}$ aproximadamente), factorizar un número del orden de 10^{12} podría llevarnos 1 segundo, pero

si es del orden de 10^{20} ya sería un año y si ponemos 10^{60}, apaga y vámonos, ¡tardaríamos 10^{30} años!

Ya estarás imaginando que debe haber métodos más rápidos para factorizar y es verdad, los hay.



En los años 60, se podían factorizar números de unas 40 cifras sin despeinarse demasiado. A finales de los 80, el récord estaba en unas 100 cifras. A lo largo de los 90, se han factorizado números cada vez más grandes: en 1994 cayó el llamado RSA129 (de 129 cifras decimales) y dos años después, el RSA130 (gracias, entre otras cosas, al trabajo de unos 600 voluntarios que pusieron su granito de arena con sus ordenadores personales).

Desde entonces han caído otros RSA. Por ejemplo, en 2003 se consiguió factorizar uno de 174 cifras decimales, conocido como RSA-576. Por cierto, ¡si consigues factorizar el RSA-2048 (que tiene 617 cifras decimales), te caerán 200000 dólares!

25195908475657893494027183240048398571429282126204
03202777713783604366202070759555626401852588078440
69182906412495150821892985591491761845028084891200
72844992687392807287776735971418347270261896375014
97182469116507761337985909570009733045974880842840
17974291006424586918171951187461215151726546322822
16869987549182422433637259085141865462043576798423
38718477444792073993423658482382428119816381501067
48104516603773060562016196762561338441436038339044
14952634432190114657544454178424020924616515723350
77870774981712577246796292638635637328991215483143
81678998850404453640235273819513786365643912120103
97122822120720357

Lo que necesitamos saber de Maple

Después de iniciar Maple, veremos un símbolo ">.en la pantalla. A continuación de ese símbolo, le iremos dando instrucciones a Maple que terminaremos siempre con un ";"

Las instrucciones que daremos a Maple serán:

- elevar un número a una potencia módulo otro número,

  ```
  > 12111^131 mod 661643;
                                  109073
  ```

- encontrar el máximo común divisor de dos números,

  ```
  > gcd(131,659880);
                                    1
  ```

- factorizar en primos un número entero:

  ```
  > ifactor(661643);
                                (541)(1223)
  ```

- también serán útiles las funciones `isprime`, `ithprime`, etc. La instrucción `>with(numtheory)` nos permite utilizar ciertas funciones especiales de Maple.
- calcular el inverso de un número en un cierto módulo:

  ```
  > 131^(-1) mod 659880;
                                  639731
  ```

  Recordemos que esto significa que

$$639731 \times 131 \equiv 1 \qquad \text{mod } 659880.$$

El gran Euler y las potencias de los primos

Figura 1: Euler

Volvemos a fijarnos en las potencias a^x módulo n. Ya vimos que en la sucesión de números (módulo un cierto n)

$$1, a, a^2, a^3, a^4, a^5 \ldots$$

hay periodicidad: un patrón que se repite indefinidamente.

Si el módulo es un primo p, Pierre de Fermat (1601-1665) ya demostró que se cumple que

$$\boxed{a^{p-1} \equiv 1 \qquad \text{módulo } p}$$

(siempre que a no sea un múltiplo de p, claro).

Si el módulo no es primo, el resultado análogo se debe a Euler (1707-1783). Es un poco más complicado. Dice así:

$$\boxed{a^{\phi(n)} \equiv 1 \qquad \text{módulo } n}$$

siempre que a y n no tengan factores en común.

Pero, ¿quién es $\phi(n)$?

Es una función peculiar: $\phi(n)$ cuenta el número de enteros entre 1 y n que no tienen factores en común con n.

Calcula, por ejemplo, los valores de

$$\phi(4) = \quad \phi(5) = \quad \phi(7) = \quad \phi(12) = \quad \phi(23) =$$

¿Sabrías decir cuánto vale $\phi(p)$, si p es un número primo?

$$\phi(p) =$$

Un poco más difícil: ¿cuánto vale $\phi(pq)$, donde p y q son números primos?

Calcula $\phi(10) = \phi(2 \times 5) =$

Calcula $\phi(21) = \phi(3 \times 7) =$

Deduce una fórmula general:

$$\phi(pq) =$$

Así que, si tenemos un número $N = pq$ y *conocemos* los primos p y q, calcular $\phi(N)$ es una tarea muy sencilla.

Sin embargo, y ésta es la observación clave, calcular $\phi(N)$ (sin conocer los factores primos p y q) es *muy difícil* si N es un número muy grande.

Es una tarea equivalente a factorizar el propio número N (algo que, ya sabemos, es muy complicado).

Lo que nos interesa para el sistema RSA es la siguiente observación.

Sabemos que

$$m^{\phi(n)} \equiv 1 \qquad \text{módulo } n$$

si m no tiene factores en común con n.

Supongamos que nos dan el valor de n y que hemos calculado $\phi(n)$. Si ahora elegimos un número a que valga 1 en la aritmética del reloj de $\phi(n)$ posiciones, esto es,

$$a \equiv 1 \qquad \text{módulo } \phi(n)$$

o, lo que es lo mismo,

$$a = 1 + \alpha\, \phi(n)\,,$$

donde α es cierto entero, entonces

$$\boxed{m^a \equiv m \qquad \text{módulo } n}$$

siempre que m no tenga factores en común con n. ¿Sabrías decir por qué?

En el sistema que vamos a describir, m es un número, el mensaje que queremos transmitir. Lo vamos a elevar a un cierto número, a, calcularemos el resultado en la aritmética n, y obtendremos de nuevo m (¡recuperaremos el mensaje original!)

Pero ese número a va a tener una parte $p\acute{u}blica$ (que pondrá el que envía el mensaje) y una parte $privada$ (que sólo conoce el receptor del mensaje).

¿Cómo funciona RSA?

El proceso consta de dos partes. En un paso previo, un usuario del sistema prepara las claves que los demás necesitarán para comunicarse con él, además de las claves que él utilizará para descifrar los mensajes (esto debe hacerlo cada usuario del sistema, claro). La segunda parte es la transmisión de mensajes propiamente dicha.

A. Preparación del sistema

El usuario Mortadelo sigue el siguiente proceso:

1) Primero, elige dos números primos p y q grandes (con muchas cifras decimales, 70, 80, 100). Estos dos números son **PRIVADOS**.

2) Los multiplica y tiene el número $N = pq$, que es **PÚBLICO**.

> Sabiendo que interesa que N sea difícil de factorizar, ¿cómo elegirías p y q?

3) Como Mortadelo conoce p y q, le resulta de lo más sencillo calcular $\phi(N)$:

$$\phi(N) = (p-1)(q-1)\,.$$

> ¿Y a un posible espía, que sólo conoce el número N?

4) Mortadelo elige un número e que no tenga factores en común con $\phi(N)$. El número e también se hace **PÚBLICO**.

5) Y ahora, Mortadelo busca el número d que cumple que

$$ed \equiv 1 \qquad \text{módulo } \phi(N)\,,$$

esto es, el inverso de e en la aritmética módulo $\phi(N)$. Este número d es **PRIVADO**.

> Recuerda que en la aritmética del reloj, no todos los números tienen inverso. ¿Por qué sabes que este número d existe con seguridad? Otra pregunta: conociendo N y e (que son datos públicos), ¿podrías obtener d? Una tercera pregunta: ¿¿es fácil calcular un inverso como éste??

Mortadelo ha terminado la preparación. Publica (por ejemplo, en el periódico) los números

$$\boxed{N \text{ y } e}$$

Es la clave pública, que los demás usuarios utilizarán para comunicarse con él.

Y se guarda los números

$$\boxed{p,\ q \text{ y } d}$$

Es la clave privada, que él utilizará para descifrar los mensajes que le envíen (en realidad sólo va a utilizar el número d).

Los demás usuarios del sistema deben hacer elecciones análogas (pero distintas, claro) a las de Mortadelo. Cada uno de ellos construye así un juego de claves públicas y otro de claves privadas.

En resumen:

- para comunicarse con Mortadelo, $todos$ los demás usuarios emplearán la misma clave. (¿Cuántos juegos de claves hay, entonces, en el sistema?)
- No hace falta reunirse con él para saber cuál es, pues ésta aparece en el periódico (no es necesario $intercambiar\ claves$).
- Sólo queda comprobar que el sistema es $seguro$.

B. Cifrado y descifrado de mensajes

Queremos mandarle a Mortadelo un mensaje. Digamos que el mensaje, por simplificar, es un número m.

Buscamos, en la guía, en el periódico, o donde esté publicado, los números necesarios para comunicarse con Mortadelo: N y e. Ahora calculamos el número

$$m^e \qquad \text{módulo } N$$

y se lo enviamos a Mortadelo.

Mortadelo recibe un número m^e (módulo N). Es distinto de m. Toma su número secreto d y calcula, en la aritmética N,

$$(m^e)^d = m^{ed}\,.$$

Como hemos visto antes (dado que e y d son inversos módulo $\phi(N)$), el resultado es m, el mensaje original.

El intento de descifrado del espía. Dispone de N y e, como todo el mundo, y además conoce cómo funciona el procedimiento.

El hábil espía ha interceptado también el mensaje enviado a Mortadelo: el número m^e. Para recuperar m, necesita elevarlo a d (módulo N). Pero no conoce d.

1. Si conociera p y q, podría seguir el procedimiento que realizó Mortadelo y obtener su clave privada d. ¿Puede, a partir de N, obtener p y q?

2. Aunque como sólo quiere conocer d (y sabe que es el inverso de e módulo $\phi(N)$), le basta calcular $\phi(N)$. Una vez hecho, calcular inversos es tarea fácil. ¿Puede, a partir de N, calcular $\phi(N)$?

Ejercicio final. Con Maple. Cada uno va a construir su juego de claves públicas y privadas, y mostrará las primeras.

Utiliza las claves públicas de tus compañeros para comunicarte con ellos.

¡Y espía e intenta descifrar los mensajes que se están enviando por ahí!