Criptografía

Estímulo del Talento Matemático

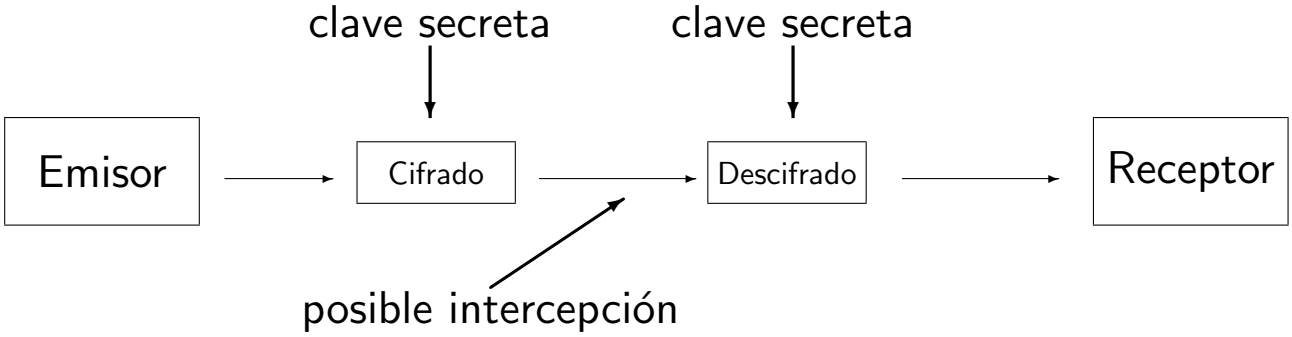
Real Academia de Ciencias

6 de mayo de 2006

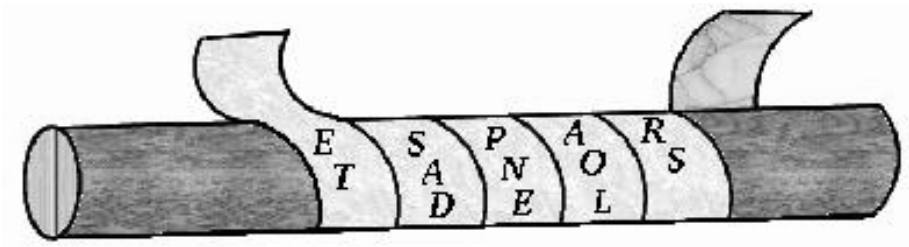
Criptografía clásica

Las comunicaciones confidenciales son necesarias. . . pero todos deseamos **descubrir secretos**.

Desde la Antigüedad se han creado **sistemas de cifrado** (criptosistemas) y, por supuesto, métodos para descifrar un mensaje interceptado (criptoanálisis).



Primer aparato criptográfico de la historia: el **escítalo**.



Aquí **la clave** es el grosor del escítalo.

Ejemplo ¿Te atreves a descifrar el siguiente mensaje

NSNCO◡◡I◡TFLEAA

cifrado con un escítalo? (ojo: entre las dos primeras palabras hay dos espacios en blanco)

La aritmética del reloj

Fijamos un cierto número natural: por ejemplo, 12. Y "contamos" como si estuviéramos con un reloj de manecillas. Las posibles "horas" son, por ejemplo, los números del 0 al 11.

	0	6	11	12	15	123	-11
Escribe aquí la "hora" $\longrightarrow$							

Lo que estamos haciendo es dividir (división entera) el número en cuestión entre 12, y quedarnos con el resto.

Podemos cambiar el reloj; por ejemplo, para el reloj de **dos** posiciones (que solo marca ceros y unos):

	0	6	11	12	15	123	-11
Escribe aquí la "hora" $\longrightarrow$							

O para el de **cinco**:

	0	6	11	12	15	123	-11
Escribe aquí la "hora" $\longrightarrow$							

En general, elegiremos un número n y diremos que estamos trabajando **módulo** n.

Operaciones módulo n

Sumar (y restar):

$3+3$	$\equiv$	(mod 7)	$9+13$	$\equiv$	(mod 10)
$-6+7$	$\equiv$	(mod 4)	$11+13$	$\equiv$	(mod 53)
$14+3$	$\equiv$	(mod 7)	$9+9$	$\equiv$	(mod 2)

Multiplicar:

3×3	$\equiv$	(mod 7)	9×13	$\equiv$	(mod 10)
-6×7	$\equiv$	(mod 4)	11×13	$\equiv$	(mod 53)
14×3	$\equiv$	(mod 7)	9×9	$\equiv$	(mod 2)

Pero, ¿y dividir?

Ya sabemos que, dentro de los *enteros*, no siempre se puede dividir.

En cambio, sí que se puede hacer en los *racionales*. Por ejemplo, podemos considerar la división entre 5 y 3. El resultado, $5/3$ es un número racional.

Pero, en realidad, ¿qué quiere decir que

$$x = \frac{5}{3}\ ?$$

Que x es el número racional que verifica que $3x = 5$, pues

$$3 \times \frac{5}{3} = 5.$$

Ahora vamos a trabajar módulo 7. Es decir, en el "reloj" de 7 posiciones. Observa que los únicos "números" que vamos a manejar son $1, 2, 3, 4, 5, 6, 7$.

"Dividir 5 por 3", por ejemplo, consiste en hallar el x tal que

$$3x \equiv 5 \pmod 7.$$

Este número es $x = 4$, pues $3 \times 4 = 12 \equiv 5$ módulo 7.

Un caso especial, el más importante: cuando buscamos, por ejemplo, el número x para el que $3x \equiv 1$ módulo 7. La solución es $x = 5$, porque $3 \times 5 = 15 \equiv 1$ módulo 7. Decimos entonces que 5 es el **inverso** de 3 en la aritmética módulo 7.

Completa la lista de los inversos de los números módulo 7:

$$\begin{aligned} 1x &\equiv 1 \Longrightarrow x = \\ 2x &\equiv 1 \Longrightarrow x = \\ 3x &\equiv 1 \Longrightarrow x = \\ 4x &\equiv 1 \Longrightarrow x = \\ 5x &\equiv 1 \Longrightarrow x = \\ 6x &\equiv 1 \Longrightarrow x = \\ 7x &\equiv 1 \Longrightarrow x = \end{aligned}$$

¿Y si fuera módulo 6?

$$\begin{array}{cccccc} 1x \equiv 1 & 2x \equiv 1 & 3x \equiv 1 & 4x \equiv 1 & 5x \equiv 1 & 6x \equiv 1 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ x = & x = & x = & x = & x = & x = \end{array}$$

A la vista de estos ejemplos, ¿te atreverías a decir cuándo un número m tiene inverso módulo n?

Codificación por trasposición

Consiste en tomar las letras del texto y cambiarlas de orden siguiendo un mecanismo fijo.

Tomamos un número a que va a ser nuestra **clave secreta**. Dado un texto de N letras, numeramos las letras como $0, 1, 2, \ldots, N-1$, y codificamos llevando la letra en el lugar x al lugar y dado por

$$y = f(x) = a\ x \qquad (\text{mod } N).$$

Necesitamos que N y a sean **primos entre sí**, como veremos en un momento. Si esto no ocurriese, añadimos un espacio al final del texto para conseguirlo.

Ejemplos:

1. Codifica el texto VENI◡VIDI◡VICI◡, con la clave $a = 2$.

2. El texto del escítalo es una codificación por transposición. ¿Cuál es la clave?

Cuando el texto le llega al receptor lo ha de descifrar usando la clave secreta a (que por supuesto conoce).

Para ello toma un inverso de a módulo N, es decir un número b tal que $a\,b \equiv 1 \pmod{N}$. El texto se reordena poniendo la letra del lugar y en el lugar

$$b\,y = b\,a\,x = 1x = x \qquad (\text{mod } N),$$

con lo que se recupera el original.

Más ejemplos:

3. Descifra el texto cifrado

BIEABSSI◡TRLA◡I◡ENENES◡ACTSRR

con la clave $a = 3$.

4. Eres un espía que ha interceptado el texto

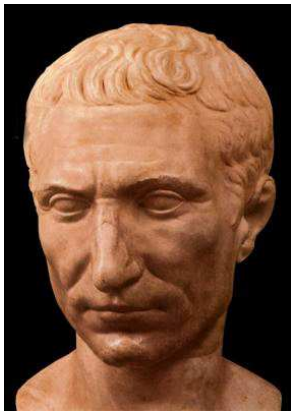
CAOSOFNRIOCRPNI◡ACDI◡ O◡CPNIIOTS

¿Sabrías descifrar el mensaje? ¿Cuál es la clave?

Como mucho, ¿cuántas claves posibles hay que probar?

5. Una mejora puede consistir en tomar como clave dos números a y N primos entre sí (ambos secretos), y dividir el texto en paquetes de N en los que se aplica el algoritmo anterior de forma independiente.

Criptosistema de César



Sustituimos cada letra del mensaje por la que se encuentra tres posiciones más allá en el alfabeto.

Éste es un sistema de sustitución monoalfabética.

En términos más matemáticos, adjudicamos

$$A = 0, B = 1, \ldots, Y = 25, Z = 26\,.$$

Y cifrar una letra x del mensaje es hacer

$$f(x) = x + 3 \qquad (\text{mod } 27).$$

La **clave secreta** es el número 3.

x	ABCDEFGHIJKLMNÑOPQRSTUVWXYZ
$f(x)$	DEFGHIJKLMNÑOPQRSTUVWXYZABC

¿Se podría cifrar con otra clave k? ¿Qué valores puede tomar k? ¿Dirías que es un método seguro para cifrar?

Ejemplos:

1. Cifra la frase AVE$\smile$CESAR, usando $k = 5$.

2. Descifra

ÑÑHJXH◡YL◡YHPFL

(sabiendo que se ha utilizado el 3 como clave) ¿Y si no supiéramos que la clave es 3?

3. Eres un espía e intentas descifrar los siguientes mensajes:

KDV◡GHVFXELHUWR◡HÑ◡VHFUHWR

GSQ◡HMID◡GERSQIW◡TSV◡FEQHE

◡ZMIQXS◡IQ◡TSTE◡E◡XSHE

Si tienes dificultades, intenta identificar las palabras de 1 o 2 letras primero.

Observa que cada letra ha de poder ser descifrada de manera única. Una vez identificada una letra, ¿es difícil descifrar el resto del mensaje?

Análisis de frecuencias

Lo importante para la seguridad de un sistema criptográfico no es mantener oculto el método de cifrado, sino la clave. Para ello,

- es necesario que el emisor y el receptor se pongan de acuerdo en una misma clave que sirve para cifrar y descifrar;
- y debe haber un número suficientemente grande de claves para que a cualquier espía que intercepte el mensaje le sea imposible probar con todas las posibles claves hasta dar con la correcta.

La codificación por sustitución sustituye cada letra del alfabeto por otra (o por un símbolo inventado). Fue usada hasta finales de la Edad Media, cuando los árabes (y luego los hombres del Renacimiento) encontraron su punto débil.

Ejemplos:

1. Usando la siguiente clave de sustitución

x	ABCDEFGHIJKLMNÑOPQRSTUVWXYZ
$f(x)$	MICLAVEÑOPQRSTUWXYZBDFGHJKN

cifra un mensaje y pásaselo a tu compañero para que lo descifre.

2. ¿Cuántas claves distintas hay? ¿Dirías que es seguro este método de cifrado?

3. Si eres un espía y recibes el siguiente mensaje

SBY ECDÑ SJZBYDI FBH OJYEJ MCDYKB DY FBFJ J KBEJ MDWJ YB SBHKJ DW XJH ICYB MLDWJ LY MDWDHB ODHRJYKCY OJADW FCHJKJ GLD WWJXJY FBH IL OHJMLHJ DW KDXCEB DY KBEB XJH SBYBSCEB EDW LYB JW BKHB SBYPCY

¿cómo lo descifrarías?

No todas las letras del castellano son igual de frecuentes. La siguiente tabla muestra las frecuencias de las distintas letras.

A	$11,96\,\%$	H	$0,89\,\%$	Ñ	$0,29\,\%$	U	$4,80\,\%$
B	$0,92\,\%$	I	$4,15\,\%$	O	$8,69\,\%$	V	$0,39\,\%$
C	$2,92\,\%$	J	$0,30\,\%$	P	$2,77\,\%$	W	$0,01\,\%$
D	$6,87\,\%$	K	$0,01\,\%$	Q	$1,53\,\%$	X	$0,06\,\%$
E	$16,78\,\%$	L	$8,37\,\%$	R	$4,94\,\%$	Y	$1,54\,\%$
F	$0,52\,\%$	M	$2,12\,\%$	S	$7,88\,\%$	Z	$0,15\,\%$
G	$0,73\,\%$	N	$7,01\,\%$	T	$3,31\,\%$		

En el texto dado podemos hacer un análisis de frecuencias, contando las proporciones de las distintas letras que aparecen. Esto nos puede ayudar a averiguar la clave y así descifrar el texto.

x	ABCDEFGHIJKLMNÑOPQRSTUVWXYZ
$f(x)$	

Criptografía de clave pública

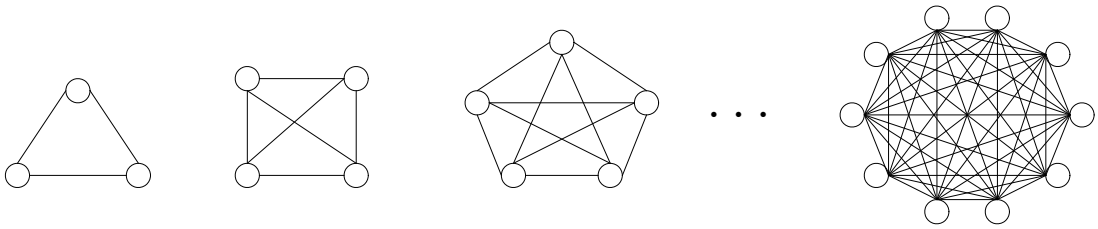
Hoy en día estamos en la era de las comunicaciones: correo electrónico, Internet, llamadas vía satélite, TV por cable, banca electrónica, etc. Por esto, la criptografía es necesaria de forma cotidiana.

Por otro lado, la potencia de cálculo de los ordenadores nos permite usar sistemas de cifrado con un número de claves altísimo, de forma que sea imposible comprobar todas las claves para descifrar un mensaje interceptado.

El punto débil (donde un espía tiene posibilidad de romper el código) es la intercepción la clave en el momento en el que emisor y receptor se ponen de acuerdo en la misma.

La **criptografía clásica** plantea dos **problemas** fundamentales:

- **Intercambio** seguro de claves.
- El **número de claves** necesarias en un sistema de n usuarios es. . .



Por ejemplo, si $n = 100000$, ¿cuántas claves se necesitarían?

En los años 70 surge un tipo nuevo y revolucionario de criptografía, en el que cada usuario dispone de

- una clave PÚBLICA (para cifrar);
- y otra clave PRIVADA (para descifrar).

Esta nueva criptografía se llama de **clave pública**.

Ahora:

- No hace falta intercambio.
- n usuarios necesitan n claves privadas.
  Compara, por ejemplo, con la criptografía clásica si $n = 100000$.

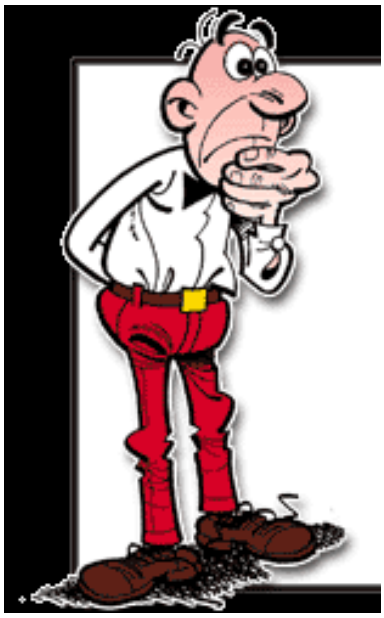
Intercambio de claves

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?

Mortadelo y Filemón, los dos superagentes de la T.I.A quieren acordar una clave, que utilizarán para mandarse mensajes secretos.

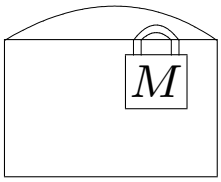
¡Pero la temible organización A.B.U.E.L.A. está al acecho!

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



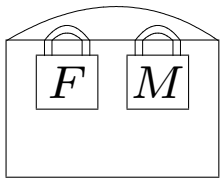
Mortadelo tiene un candado, del que sólo él guarda la llave. Le envía un mensaje (por ejemplo, la clave que se quiere compartir) a Filemón en un cofre cerrado con su candado (para que nadie, salvo él, pueda abrirlo):

Mortadelo cierra el cofre



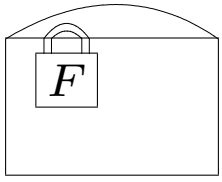
Filemón recibe el cofre cerrado. No puede abrirlo. Pero sí ponerle su propio candado (del que sólo él tiene llave) y reenviárselo a Mortadelo.

Filemón añade su candado



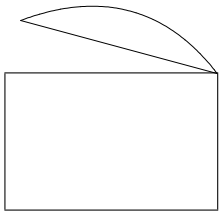
Mortadelo lo recibe, retira su candado y se lo vuelve a enviar a Filemón.

Mortadelo retira su candado



Filemón, finalmente, recibe el cofre, retira su candado y puede leer el mensaje.

Filemón puede abrir el cofre



Lo anterior nos convence de que **se puede hacer**. Pero falta definir adecuadamente los "candados".

Un **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:

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

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

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

Periodicidad y patrones

Suma. Estamos en módulo 7. Y calculamos

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

Ahora en módulo 12:

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

Producto. En módulo 7, de nuevo, calculamos

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

Ahora en módulo 12:

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

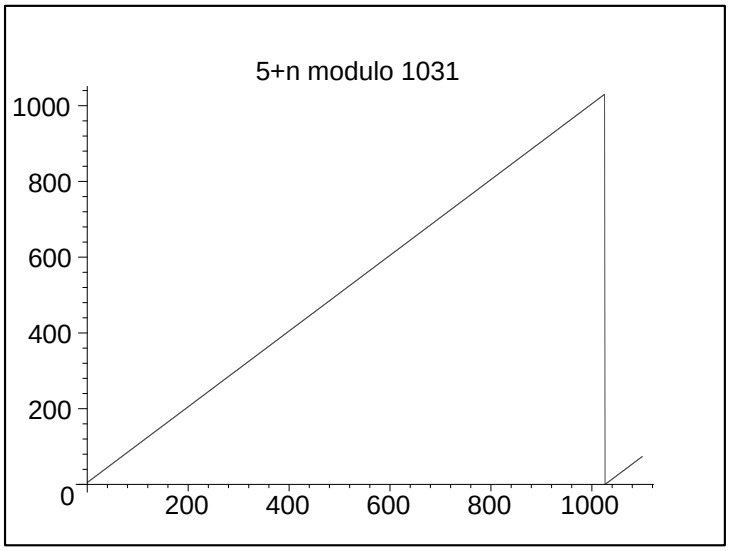
Vamos con las **potencias**. En módulo 7, de nuevo, calculamos

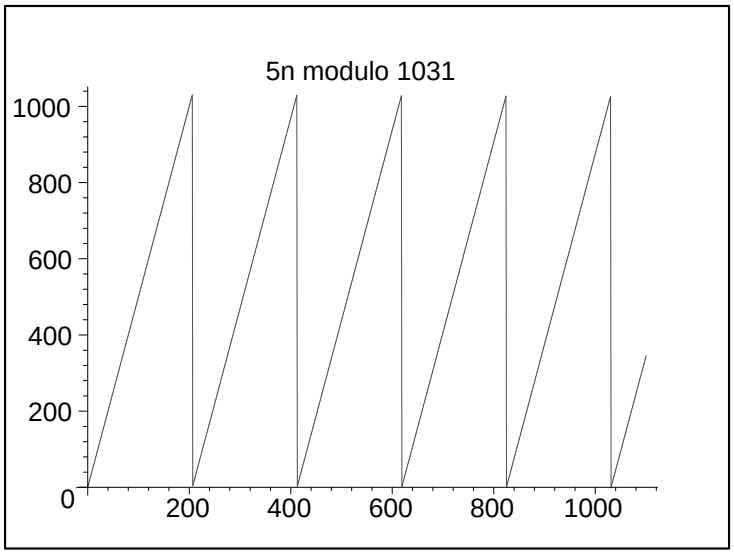
$$\begin{array}{l|l|l|l} 2^0 \equiv & 3^0 \equiv & 5^0 \equiv & 6^0 \equiv \\ 2^1 \equiv & 3^1 \equiv & 5^1 \equiv & 6^1 \equiv \\ 2^2 \equiv & 3^2 \equiv & 5^2 \equiv & 6^2 \equiv \\ 2^3 \equiv & 3^3 \equiv & 5^3 \equiv & 6^3 \equiv \\ 2^4 \equiv & 3^4 \equiv & 5^4 \equiv & 6^4 \equiv \\ 2^5 \equiv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

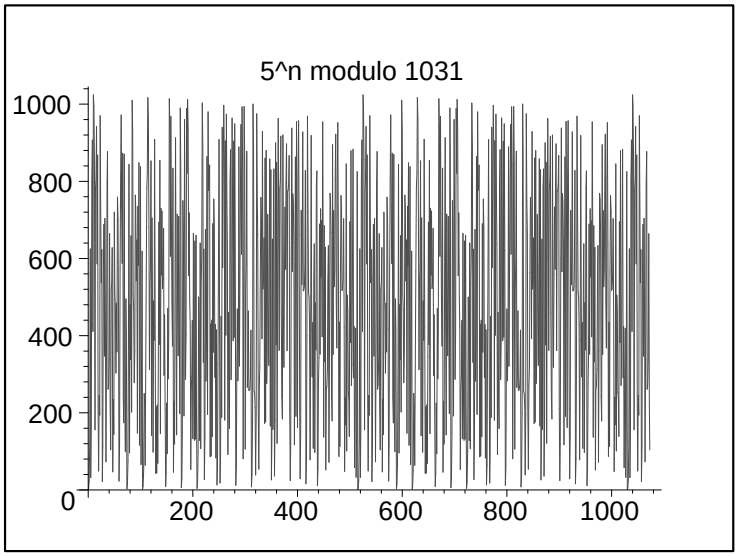
En módulo 12:

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

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.

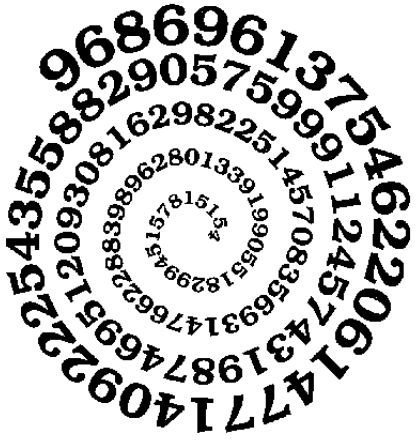
¿Todavía crees que factorizar es fácil? Pues inténtalo con el número $n = 23360947609$. ¡Glub!. . . El "primer" número primo que divide a este n es $p = 152041$. ¿Cuánto habrías tardado en encontrarlo?

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

778707749817125772467962926386356373289912154831438167899885040445364023527381951378636565439121201039712282212072035 7