Criptografía

Susana Puddu

Supongamos que Juan quiere enviar un mensaje a Pedro de forma tal que únicamente Pedro sea capaz de entender su contenido. Una manera ingenua de hacer esto es reemplazar cada letra, signo de puntuación, espacio, etc. del mensaje original por un número de dos cifras, según una tabla de conversión convenida previamente entre Juan y Pedro que sólo ellos dos conocen. De esta manera Juan, utilizando la tabla, convierte el texto en un número y se lo envía a Pedro, quien recupera el mensaje original utilizando a su vez la tabla de conversión.
Por ejemplo, si el mensaje fuese ESTO ES UN SECRETO y utilizamos la tabla de conversión

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19

T	U	V	W	X	Y	Z	espacio
20	21	22	23	24	25	26	00

el número que recibiría Pedro sería 05192015000519002114001905031805 2015
Sin embargo, esta no es una manera segura ya que es posible descifrar el mensaje comparando la frecuencia con la que aparece cada uno de los números de dos cifras con la frecuencia estadística que tiene cada letra. Por ejemplo, que el número 05 aparezca más veces que cualquier otro indica que probablemente sea una A o una E (que son las letras que más frecuentemente aparecen en cualquier texto).
Veamos otras formas más seguras de enviar mensajes. La idea general es aplicar al mensaje una cierta transformación (es decir, encriptarlo) de forma tal que ningún intruso que intercepte el mensaje encriptado sea capaz de aplicarle la transformación inversa. Observemos que la transformación inversa debe ser mantenida en secreto siempre, mientras que la que encripta puede ser tanto pública como privada. Esto se debe a que existen ciertas funciones, llamadas *de una sola vía*, que son sencillas de evaluar pero cuya inversa es muy difícil de determinar. Por lo tanto, si la transformación que se utiliza para encriptar es de una sola vía, no es necesario que sea mantenida en secreto.

Claves privadas. En este caso la transformación que encripta el mensaje utiliza una *clave* que sólo es conocida por Juan y Pedro. Unicamente quienes conozcan la clave son capaces de encriptar el mensaje. De esta manera, cuando Juan envía a Pedro un mensaje encriptado utilizando la clave que ambos convinieron previamente y que sólo ellos conocen, Pedro sabe con certeza que el mensaje proviene de Juan ya que nadie más podría ser capaz de encriptarlo. Veamos ahora un ejemplo que tiene la particularidad de que la transformación

que se utiliza para encriptar es la misma que la que se utiliza para desencriptar. Es decir, en este ejemplo, la transformación que encripta coincide con su inversa. Esta clase de transformaciones se denominan *involuciones*.
En primer lugar, Juan y Pedro eligen como clave un string de 30 dígitos binarios (es decir, tal que cada dígito sea cero o uno) que mantienen en secreto. Supongamos que la clave elegida sea

$$101000110110101100101101001011$$

Ahora, Juan convierte el mensaje en un string de dígitos binarios reemplazando cada letra por un string de cinco dígitos binarios según una tabla de conversión previamente acordada con Pedro. Por ejemplo, la tabla de conversión puede obtenerse de la tabla

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19

T	U	V	W	X	Y	Z	espacio
20	21	22	23	24	25	26	00

reemplazando cada número de dos cifras por su representación en base 2. De esta manera, cada letra S del mensaje original será reemplazada por el string 10011, ya que esta es la representación de 19 en base 2. Luego de reemplazar cada letra por su correspondiente string de cinco dígitos binarios, Juan parte el string total obtenido en bloques de 30 dígitos binarios cada uno. Ahora nuestro mensaje se ha convertido en

$$\text{bloque 1: } \underbrace{00101}_{E}\underbrace{10011}_{S}\underbrace{10100}_{T}\underbrace{01111}_{O}\ \underbrace{00000}_{\text{espacio}}\ \underbrace{00101}_{E}$$

$$\text{bloque 2: } \underbrace{10011}_{S}\ \underbrace{00000}_{\text{espacio}}\ \underbrace{10101}_{U}\underbrace{01110}_{N}\ \underbrace{00000}_{\text{espacio}}\ \underbrace{10011}_{S}$$

$$\text{bloque 3: } \underbrace{00101}_{E}\underbrace{00011}_{C}\underbrace{10010}_{R}\underbrace{00101}_{E}\underbrace{10100}_{T}\underbrace{01111}_{O}$$

A continuación, Juan transforma, utilizando la clave, cada uno de estos bloques (que llamaremos bloques originales) en un nuevo bloque binario (que llamaremos bloques transformados) poniendo un cero en el i-ésimo lugar del bloque transformado si el i-ésimo dígito de la clave coincide con el i-ésimo dígito del bloque original y poniendo un uno en otro caso.
Por ejemplo, en nuestro caso el primer dígito del bloque 1 original es 0 y el primer dígito de la clave es 1. Como no coinciden, el primer dígito del bloque transformado será 1. Análogamente, el segundo dígito del bloque 1 original es 0 y el segundo dígito de la clave es 0. Como coinciden, el segundo dígito del bloque transformado será 0.

bloque 1 original: 0 0 1 0 1 1 0 0 1 1 1 0 1 0 0 0 1 1 1 1 0 0 0 0 0 0 0 1 0 1

clave: 1 0 1 0 0 0 1 1 0 1 1 0 1 0 1 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1

bloque 1 transformado: 1 0 0 0 1 1 1 1 1 0 0 0 0 0 1 1 1 1 0 1 1 1 0 1 0 0 1 1 1 0

Ahora hacemos lo mismo con los restantes dos bloques:

bloque 2 original: 1 0 0 1 1 0 0 0 0 0 1 0 1 0 1 0 1 1 1 0 0 0 0 0 0 1 0 0 1 1

clave: 1 0 1 0 0 0 1 1 0 1 1 0 1 0 1 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1

bloque 2 transformado: 0 0 1 1 1 0 1 1 0 1 0 0 0 0 0 1 1 1 0 0 1 1 0 1 0 1 1 0 0 0

bloque 3 original: 0 0 1 0 1 0 0 0 1 1 1 0 0 1 0 0 0 1 0 1 1 0 1 0 0 0 1 1 1 1

clave: 1 0 1 0 0 0 1 1 0 1 1 0 1 0 1 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1

bloque 3 transformado: 1 0 0 0 1 0 1 1 1 0 0 0 1 1 1 1 0 1 1 1 0 1 1 1 0 0 0 1 0 0

Finalmente, Juan envía a Pedro los bloques transformados.

Para desencriptar el mensaje, Pedro efectua en cada bloque recibido la misma operación, es decir, utilizando la clave reconstruye los bloques originales comparando el i-ésimo dígito del bloque transformado con el i-ésimo dígito de la clave. Si estos coinciden significa que el i-ésimo dígito del bloque original era un cero y si no coinciden que era un uno. Para ejemplificar, desencriptemos el segundo bloque:

bloque 2 transformado: 0 0 1 1 1 0 1 1 0 1 0 0 0 0 0 1 1 1 0 0 1 1 0 1 0 1 1 0 0 0

clave: 1 0 1 0 0 0 1 1 0 1 1 0 1 0 1 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1

bloque 2 original: 1 0 0 1 1 0 0 0 0 0 1 0 1 0 1 0 1 1 1 0 0 0 0 0 0 1 0 0 1 1

Por último, Pedro descifra el mensaje reemplazando cada string de cinco dígitos binarios por la correspondiente letra según la tabla de conversión.

La ventaja de este sistema radica en que una misma letra puede resultar transformada en diferentes strings según sea su ubicación en el texto. Por ejemplo, la primera E de nuestro mensaje (representada por los primeros cinco dígitos del bloque 1) se transformó en 10001 (primeros cinco dígitos del bloque 1 transformado), la segunda (representada por los últimos cinco dígitos del bloque 1) en 01110 (últimos cinco dígitos del bloque 1 transformado), la tercera en 10001 y la cuarta en 10111. También, la primera S se transformó en 11110, la segunda en 00111 y la tercera en 11000. Además, diferentes letras pueden resultar transformadas en el mismo string. Por ejemplo, tanto la segunda E como la C se transformaron en 01110. Esto hace que sea prácticamente imposible desencriptar el mensaje sin conocer la clave. En este caso, la cantidad de posibles claves de 30 dígitos binarios es 2^{30} pero está claro que para mensajes más largos podríamos partir el mensaje binario original en bloques de 100 dígitos y, por lo tanto, utilizar claves de 100 dígitos

binarios. En tal caso la cantidad de posibles claves sería enorme (2^{100}) lo que hace que ninguna persona que no conozca la clave pueda determinarla por ensayo y error (es decir, probando con cada posible clave hasta obtener un texto coherente).

Como vemos, la seguridad de este método radica en la privacidad de la clave. Nos preguntamos entonces cómo pueden hacer Juan y Pedro para acordar una clave con total certeza de que sólo ellos la conozcan. Obviamente, la manera más segura es acordar una clave sin tener que transmitirla, ya que al transmitirla se corre el riesgo de que alguien la intercepte. El siguiente método, ideado por W. Diffie y M. Hellman, logra este objetivo: primero, Juan y Pedro eligen un número primo p y un entero a coprimo con p tal que $r_p(a^j) \neq 1$ para todo $1 \leq j < p-1$. Un tal entero a se llama una raíz primitiva módulo p (observemos que para cualquier primo p siempre existe al menos una raíz primitiva módulo p). Tanto p como a no necesitan guardarse en secreto, sino que pueden ser conocidos por cualquier persona. Luego Juan elige un número natural k menor que $p-1$ y tal que $a^k > p$ y, a su vez, Pedro elige un número natural r menor que $p-1$ y tal que $a^r > p$. Los números k y r son secretos, k es conocido sólo por Juan y r es conocido sólo por Pedro. Juan envía a Pedro el número $b = r_p(a^k)$ y Pedro envía a Juan el número $c = r_p(a^r)$. Entonces Juan calcula $r_p(c^k)$ y Pedro calcula $r_p(b^r)$.

Como $c \equiv a^r \ (p)$ entonces $c^k \equiv (a^r)^k = a^{rk} \ (p)$. Del mismo modo, como $b \equiv a^k \ (p)$ entonces $b^r \equiv (a^k)^r = a^{rk} \ (p)$. Luego, $c^k \equiv b^r \ (p)$, de donde $r_p(c^k) = r_p(b^r)$. Este número $r_p(c^k) = r_p(b^r)$, que tanto Juan como Pedro conocen pero que nunca fue transmitido, será la clave acordada. Observemos que si lo que quisieran es una clave binaria, basta tomar entonces la representación en base 2 de $r_p(c^k) = r_p(b^r)$.

Para fijar ideas, supongamos que el primo convenido entre Juan y Pedro sea $p = 127$ y que la raíz primitiva módulo p sea $a = 3$ (dejamos a cargo del lector verificar que 127 es primo y que 3 es una raíz primitiva módulo 127). Supongamos además que Juan elige $k = 16$ y Pedro elige $r = 30$ y veamos cómo hacen Juan y Pedro para obtener la clave. Primero, Juan calcula $b = r_p(a^k) = r_{127}(3^{16}) = 71$ y se lo envía a Pedro y Pedro calcula $c = r_p(a^r) = r_{127}(3^{30}) = 38$ y se lo envía a Juan. Luego, como Juan conoce $c = 38$ y $k = 16$, puede calcular $r_p(c^k) = r_{127}(38^{16}) = 76$. Análogamente, como Pedro conoce $b = 71$ y $r = 30$, puede calcular $r_p(b^r) = r_{127}(71^{30}) = 76$. Por lo tanto, la clave acordada (que es conocida por ambos pero que nunca fue transmitida) es 76. Si quisieran una clave binaria, podrían tomar, por ejemplo, la representación en base 2 de 76 que es 1001100.

En la realidad, el primo p elegido es un número de muchísimas más cifras. Esto produce, por un lado, que la clave resulte un número de muchas más cifras (cosa que ya vimos que es conveniente) y, por otro, que el método sea seguro ya que cuando p es un primo muy grande y a es una raíz primitiva módulo p entonces no existe ningún método eficiente que permita calcular k a partir de p, a y $r_p(a^k)$ y, por lo tanto, si un intruso interceptara la comunicación entre Juan y Pedro y lograra conocer $b = r_p(a^k)$ y $c = r_p(a^r)$, no pudiendo determinar k y r le sería imposible calcular la clave.

Finalmente, veamos cómo pueden hacer Juan y Pedro para determinar b, c y la clave rápidamente. Juan necesita calcular $b = r_{127}(3^{16})$ y $r_{127}(38^{16})$. Esto lo puede hacer de la siguiente manera:

$$3^{2^0} = 3^1 = 3 \equiv 3 \quad (127)$$
$$3^{2^1} = 3^{2^0.2} = (3^{2^0})^2) \equiv 3^2 = 9 \quad (127)$$
$$3^{2^2} = 3^{2^1.2} = (3^{2^1})^2) \equiv 9^2 = 81 \quad (127)$$
$$3^{2^3} = 3^{2^2.2} = (3^{2^2})^2) \equiv 81^2 = 6561 \equiv 84 \quad (127)$$
$$3^{2^4} = 3^{2^3.2} = (3^{2^3})^2) \equiv 84^2 = 7056 \equiv 71 \quad (127)$$

$$38^{2^0} = 38^1 = 38 \equiv 38 \quad (127)$$
$$38^{2^1} = 38^{2^0.2} = (38^{2^0})^2) \equiv 38^2 = 1444 \equiv 47 \quad (127)$$
$$38^{2^2} = 38^{2^1.2} = (38^{2^1})^2) \equiv 47^2 = 2209 \equiv 50 \quad (127)$$
$$38^{2^3} = 38^{2^2.2} = (38^{2^2})^2) \equiv 50^2 = 2500 \equiv 87 \quad (127)$$
$$38^{2^4} = 38^{2^3.2} = (38^{2^3})^2) \equiv 87^2 = 7569 \equiv 76 \quad (127)$$

Como $16 = 2^4$, entonces Juan obtiene que $b = r_{127}(3^{16}) = r_{127}(3^{2^4}) = 71$ y la clave es $r_{127}(38^{16}) = r_{127}(38^{2^4}) = 76$.
A su vez, Pedro necesita calcular $c = r_{127}(3^{30})$ y $r_{127}(71^{30})$. Ahora el exponente, 30, no es una potencia de 2. Sin embargo, puede proceder de manera similar, hallando primero el desarrollo en base 2 de 30, que es 11110. Esto significa que $30 = 1.2^4+1.2^3+1.2^2+1.2^1+0.2^0$ y, por lo tanto,

$$3^{30} = 3^{2^4+2^3+2^2+2^1} = 3^{2^4}.3^{2^3}.3^{2^2}.3^{2^1}$$

y

$$71^{30} = 71^{2^4+2^3+2^2+2^1} = 71^{2^4}.71^{2^3}.71^{2^2}.71^{2^1}$$

con lo cual Pedro puede calcular c y la clave de la siguiente manera:

$$3^{2^0} = 3^1 = 3 \equiv 3 \quad (127)$$
$$3^{2^1} = 3^{2^0.2} = (3^{2^0})^2) \equiv 3^2 = 9 \quad (127)$$
$$3^{2^2} = 3^{2^1.2} = (3^{2^1})^2) \equiv 9^2 = 81 \quad (127)$$
$$3^{2^3} = 3^{2^2.2} = (3^{2^2})^2) \equiv 81^2 = 6561 \equiv 84 \quad (127)$$
$$3^{2^4} = 3^{2^3.2} = (3^{2^3})^2) \equiv 84^2 = 7056 \equiv 71 \quad (127)$$

$$71^{2^0} = 71^1 = 71 \equiv 71 \quad (127)$$
$$71^{2^1} = 71^{2^0.2} = (71^{2^0})^2) \equiv 71^2 = 5041 \equiv 88 \quad (127)$$
$$71^{2^2} = 71^{2^1.2} = (71^{2^1})^2) \equiv 88^2 = 7744 \equiv 124 \quad (127)$$
$$71^{2^3} = 71^{2^2.2} = (71^{2^2})^2) \equiv 124^2 = 15376 \equiv 9 \quad (127)$$
$$71^{2^4} = 71^{2^3.2} = (71^{2^3})^2) \equiv 9^2 = 81 \quad (127)$$

Luego,

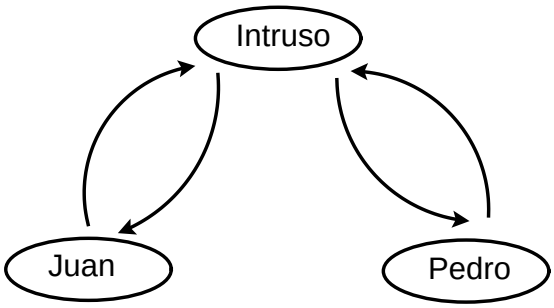
$$3^{30} = 3^{2^4+2^3+2^2+2^1} = 3^{2^4}.3^{2^3}.3^{2^2}.3^{2^1} \equiv 71.84.81.9 =$$
$$= 5964.729 \equiv 122.94 = 11468 \equiv 38 \quad (127)$$

y

$$71^{30} = 71^{2^4+2^3+2^2+2^1} = 71^{2^4}.71^{2^3}.71^{2^2}.71^{2^1} \equiv 81.9.124.88 =$$
$$= 729.10912 \equiv 94.117 = 10998 \equiv 76 \quad (127)$$

de donde finalmente obtiene que $c = r_{127}(3^{30}) = 38$ y la clave es $r_{127}(71^{30}) = 76$.

Si el lector ya está convencido de que esta manera de acordar una clave es segura, imagine la siguiente situación: un intruso ha "pinchado" la comunicación entre Juan y Pedro de manera tal que cuando Juan o Pedro envían un mensaje quien realmente lo recibe es el intruso. Además, el intruso puede enviar mensajes a Pedro haciéndose pasar por Juan y a Juan haciéndose pasar por Pedro.



Ahora, cuando Juan envía a Pedro el número $b_1 = r_p(a^k)$ el intruso lo recibe y, haciéndose pasar por Pedro, envía a Juan el número $c_1 = r_p(a^s)$. Ahora ambos calculan la clave $K_1 = r_p(c_1^k) = r_p(b_1^s)$. Por otro lado, el intruso envía a Pedro, haciéndose pasar por Juan, el número $b_2 = r_p(a^t)$ y Pedro envía al intruso, creyendo que es Juan, el número $c_2 = r_p(a^r)$. Finalmente, ambos calculan la clave $K_2 = r_p(c_2^t) = r_p(b_2^r)$. Ahora Juan cree que la clave acordada es K_1, Pedro cree que es K_2 y el intruso conoce tanto K_1 como K_2. De esta manera, cada vez que Juan le envíe a Pedro un mensaje, el mensaje estará encriptado usando la clave K_1 y el intruso será quien lo reciba. Entonces el intruso puede desencriptarlo y

i) encriptar nuevamente el mensaje pero ahora usando la clave K_2 y enviárselo a Pedro, quien pensará que proviene de Juan.

ii) idem i) pero alterando previamente el contenido del mensaje.
iii) no reenviar el mensaje a Pedro y responderle a Juan haciéndose pasar por Pedro usando la clave K_1.
Claramente, lo mismo sucede cuando Pedro envía un mensaje a Juan...

Claves públicas. En este caso la transformación que encripta el mensaje utiliza una clave que es de conocimiento público. Cualquier persona tiene acceso a la clave y, por lo tanto, puede encriptar un mensaje. Obviamente, en este caso no puede usarse la misma clave para encriptar y desencriptar, por lo tanto, cada usuario del sistema debe elegir dos claves: una pública, que utilizarán los demás para encriptar los mensajes que le envíen y una privada que sólo él conoce con la cual puede desencriptarlos.
Describiremos ahora uno de los sistemas más populares de clave pública, conocido como RSA y creado por Rivest, Shamir y Adleman en 1978 que se basa en el siguiente corolario del teorema de Fermat

Corolario. Sea $n = p.q$ donde p y q son primos positivos distintos y sea a un entero. Si a es coprimo con n entonces $a^{(p-1)(q-1)} \equiv 1\ (n)$.

Demostración: Por el teorema de Fermat, como $p \nmid a$ pues a es coprimo con $n = p.q$ se tiene que $a^{p-1} \equiv 1\ (p)$ y como $q \nmid a$ pues a es coprimo con $n = p.q$ se tiene que $a^{q-1} \equiv 1\ (q)$. Luego,

$$a^{(p-1)(q-1)} = \left(a^{p-1}\right)^{q-1} \equiv 1\ (p)$$

y

$$a^{(p-1)(q-1)} = \left(a^{q-1}\right)^{p-1} \equiv 1\ (q)$$

Por lo tanto, como p y q son coprimos, se tiene que $a^{(p-1)(q-1)} \equiv 1\ (p.q)$, es decir, $a^{(p-1)(q-1)} \equiv 1\ (n)$ $\square$

El sistema RSA. En este sistema, cada usuario fabrica dos claves, una pública y una privada, de la siguiente manera: en primer lugar, elige dos primos distintos p y q y calcula su producto $n = p.q$. Luego elige un número natural e menor que $(p-1)(q-1)$ y que sea coprimo con $(p-1)(q-1)$ y calcula, utilizando el algoritmo de Euclides, un número natural d tal que $e.d \equiv 1\ ((p-1)(q-1))$.
El par (n, e) constituye la clave pública que permite al resto de los usuarios encriptar los mensajes que le envíen, mientras que la terna (p, q, d) debe ser mantenida en secreto y constituye la clave privada que le permitirá desencriptar los mensajes que reciba. En resumen, cada usuario j dispone de una clave pública (n_j, e_j) y de una privada (p_j, q_j, d_j) donde $n_j = p_j.q_j$ y $e_j.d_j \equiv 1\ ((p_j-1)(q_j-1))$. Además, todos disponen de una tabla de conversión común para transformar los mensajes en un número antes de encriptarlos.
Para enviar un mensaje encriptado a Pedro, cuya clave pública es (n, e), Juan transforma el mensaje en un número utilizando la tabla de conversión y lo parte en bloques $a_1, \ldots, a_s$ donde $a_i < n$ $(1 \leq i \leq s)$. Luego, para cada bloque a, Juan calcula el bloque transformado $b = r_n(a^e)$ y se lo envía a Pedro.

Para desencriptar cada bloque transformado b, Pedro utiliza su clave privada (p, q, d) que sólo él conoce y calcula $r_n(b^d)$, con lo cual obtiene el bloque original a. En efecto, como $e.d \equiv 1\ ((p-1)(q-1))$, entonces $e.d - 1 = k(p-1)(q-1)$ para algún $k \in N$. Como $b = r_n(a^e) \equiv a^e\ (n)$, se tiene que

$$b^d \equiv (a^e)^d = a^{e.d} = a^{1+k(p-1)(q-1)} = a.(a^{(p-1)(q-1)})^k \quad (n)$$

Veamos que $a.(a^{(p-1)(q-1)})^k \equiv a\ (n)$. Esto es claro cuando a es coprimo con n ya que en ese caso $a^{(p-1)(q-1)} \equiv 1 \quad (n)$. Pero también vale si a y n no son coprimos. En efecto, en tal caso se tiene que a es divisible por p o por q, pero no por ambos, ya que $n = p.q$ y $a < n$. Supongamos entonces que a es divisible por p y no por q. Entonces $a \equiv 0\ (p)$ y $a^{q-1} \equiv 1\ (q)$, de donde

$$a.(a^{(p-1)(q-1)})^k \equiv 0 \equiv a \quad (p)$$

y

$$a.(a^{(p-1)(q-1)})^k \equiv a.(a^{(p-1)(q-1)})^k = a.(a^{q-1})^{(p-1)k} \equiv a \quad (q)$$

Luego, como $n = p.q$ y p y q son primos distintos, resulta que $a.(a^{(p-1)(q-1)})^k \equiv a\ (n)$ de donde $b^d \equiv a\ (n)$ y, como a es un número natural menor que n entonces $a = r_n(b^d)$.
De esta manera, Pedro recupera cada bloque original y reconstruye el mensaje utilizando la tabla de conversión.
Observemos que para poder desencriptar, es necesario conocer d, que sólo puede calcularse conociendo $(p-1)(q-1)$. Dado que, para valores de n suficientemente grandes, $(p-1)(q-1)$ no se puede calcular sin conocer la factorización de n, la seguridad de este sistema descansa en el hecho de que para factorizar números grandes se requiere muchísimo tiempo. En la realidad, los primos p y q elegidos son números de más de 100 cifras, con lo cual resulta imposible determinar la factorización de $n = p.q$.

Autenticidad del emisor. Como ya observamos antes, cuando se utiliza para encriptar una clave privada la autenticidad del emisor está garantizada: cuando Juan envía a Pedro un mensaje encriptado utilizando una clave que ambos convinieron previamente y que sólo ellos conocen, Pedro sabe con certeza que el mensaje proviene de Juan ya que nadie más podría ser capaz de encriptarlo. En cambio, cuando se utiliza una clave pública esto no sucede. Supongamos que Pedro recibe un mensaje supuestamente enviado por Juan. Debido a que la clave pública de Juan es conocida por todos, Pedro no puede estar seguro de que el mensaje fue realmente enviado por Juan y no por otra persona. Supongamos que (n, e) y (m, r) son las respectivas claves púbicas de Pedro y Juan y que (p, q, d) y (p', q', s) son las claves privadas. Veamos cómo se puede hacer para garantizar la autenticidad del emisor del mensaje.

Supongamos que $n \leq m$. En este caso, Juan transforma el mensaje en un número y lo parte en bloques $a_1, \ldots, a_s$ donde $a_i < n$. Para encriptar cada bloque a, efectúa dos transformaciones: primero una utilizando la clave pública de Pedro y luego otra utilizando su propia

clave privada. Para obtener el bloque transformado Juan primero calcula $b = r_n(a^e)$, luego calcula $c = r_m(b^s)$ y envía c a Pedro. Para desencriptar el bloque transformado, Pedro utiliza la clave pública de Juan y su propia clave privada: calcula primero $r_m(c^r)$ que es igual a b pues $c^r \equiv b\ (m)$ y $b < n \leq m$. Una vez obtenido b, Pedro calcula $r_n(b^d)$ que resulta ser igual a a ya que $b^d \equiv a\ (n)$ y $a < n$.
Si, en cambio, $m < n$, Juan transforma el mensaje en un número que ahora parte en bloques $a_1, \ldots, a_s$, donde $a_i < m$. Ahora, para encriptar cada bloque a, realiza las mismas transformaciones que antes pero en orden inverso: primero calcula $b = r_m(a^s)$, luego $c = r_n(b^e)$. Para desencriptar el bloque transformado c, Pedro calcula primero $r_n(c^d)$ que es igual a b pues $c^d \equiv b\ (n)$ y $b < m < n$. Una vez obtenido b, Pedro calcula $r_m(b^r)$ que resulta ser igual a a ya que $b^r \equiv a\ (m)$ y $a < m$.

De esta manera, como d es conocido únicamente por Pedro, entonces nadie más puede desencriptar el mensaje y como s es conocido únicamente por Juan, ahora Pedro puede estar seguro de que él es quien envía el mensaje.