Rev.R.Acad.Cienc.Exact.Fís.Nat. (Esp)
Vol. 101, Nº. 2, pp 307-320, 2007
VIII Programa de Promoción de la Cultura Científica y Tecnológica

EL ARTE DE DISFRAZAR LA INFORMACIÓN: DE LA C A LA Q

ALBERTO GALINDO TIXAIRE *

* Real Academia de Ciencias Exactas, Físicas y Naturales. Departamento de Física Teórica. Facultad de Ciencias Físicas. Universidad Complutense. 28040 MADRID. España. agt@fis.ucm.es

I. INTRODUCCIÓN

Desde la antigüedad los seres humanos han tenido necesidad de disfrazar la información, haciéndola ininteligible salvo para los destinatarios de los mensajes. Los éforos de Esparta usaron la escítala para cifrar, a Julio César se le atribuye un criptosistema (sistema de cifrado) elemental para comunicarse con Cicerón y otros comandantes de las legiones de Roma, la hermosa María Estuardo de Escocia perdió literalmente su cabeza al ser interceptadas y descifradas por el fundador del servicio secreto británico unas cartas secretas suyas alentando una conspiración para acabar con Isabel de Inglaterra, la rotura del código de la máquina alemana Enigma para cifrar desafió a las mentes más brillantes de entre los Aliados, como Alan Turing, y hoy la civilización reposa en la seguridad de que muchos mensajes, con información muy valiosa, pueden ser cifrados de modo tal que solo los que disponen de la clave adecuada pueden descifrarlos y conocer su contenido original.

La criptografía es la ciencia y el arte que estudia los procedimientos de transformar la información, haciéndola incomprensible si no se dispone de la clave adecuada para desvelarla. Frente a la criptografía, el criptoanálisis pretende romper el secreto sin disponer de la clave. Si el profeta Daniel fue el primer criptoanalista que registra la historia, los *crackers* son su exponente oscuro en el mundo actual. Es evidente que un buen criptógrafo deber conocer lo mejor posible los métodos usados por los criptoanalistas, para robustecer sus propios sistemas de cifrado. La pugna constante a lo largo de los tiempos entre estos dos mundos que integran la criptología ha hecho que los procedimientos o algoritmos de cifrado hayan ido perfeccionándose. La disponibilidad de potentes ordenadores capaces de romper con gran facilidad códigos poco sofisticados ha obligado al uso de claves sumamente astutas y/o complejas para proteger los mensajes de alto valor estratégico.

El mundo "digital" en el que nos ha tocado vivir se sustenta en la seguridad de confidencialidad. Algún que otro ciudadano *A* es reacio a la compra "electrónica" en un establecimiento *B* por el temor a que un taimado criptoanalista *C*, que intercepta un mensaje cifrado que manda a *B* dicho comprador *A*, en el que figura el número de su tarjeta de crédito, logre descifrarlo y pueda usar ese número fraudulentamente. Existen sistemas de codificación muy buenos, como el RSA de clave pública. Pero su seguridad no está plenamente garantizada, y depende del desarrollo de ciertos algoritmos de cálculo. Solo se conoce un cifrador absolutamente seguro: el método Vernam o clave de "un solo uso". Es muy simple, pero requiere que *A* y *B* compartan en exclusiva una clave para cifrar y descifrar, clave que solo debe usarse una vez si no se quiere comprometer la seguridad del criptosistema.

Pretendemos hablar de la apasionante historia de la escritura secreta, que arrancó de Egipto hace 4000 años, intervino en la batalla de las Termópilas, hizo que Colón volviera encadenado a España, bien pudo evitar el desastre de Pearl Harbour, y hoy está pasando aceleradamente de la C a la Q, de la Criptografía basada en sistemas clásicos, a la Qriptografía en la que el principio de indeterminación de Heisenberg, y por

* Este texto fue esencialmente escrito en el primer semestre de 2006. Lo hemos mantenido, con alguna nota de actualización.

tanto, la propia naturaleza cuántica, es garante absoluto de un sistema de distribución de claves entre partes que permite aplicar simple y tranquilamente la cifra de "usar y tirar".

II. UN BREVE PASEO HISTÓRICO

Escribas egipcios, ya por allá al 1900 a.C., sustituían algunos signos jeroglíficos por otros arbitrarios para realzar su historia. Los alfareros de Mesopotamia, alrededor del 1500 a.C., usaban signos cuneiformes con valores silábicos poco frecuentes para ocultar sus técnicas de fabricación de cerámica esmaltada.[1]

También en la Biblia asoma la criptología en varias guisas, como, por ejemplo, en el método ATBASH para transformar la escritura, consistente en intercambiar la primera letra (א, *Álef*) del alfabeto hebreo o *alefato* (de 22 consonantes, algunas de ellas mudas en mayor o menor grado) con la última (ת, *Tav*), la segunda (ב, *Bet/Vet*) con la penúltima (ש, *Shin/Sin*), y así sucesivamente, hasta la undécima (כ, *Kaf/Jaf*) que se intercambiaba por la duodécima (ל, *Lámed*). Así, en el libro de Jeremías (25:26, 51:41) aparece dos veces la palabra *Babel* (בבל, Lamed/Bet/Bet) reemplazada por *Sheshakh* (ששכ, Kaf/Shin/Shin). ¿Qué pretendían los autores con ésto? Posiblemente, ninguna ocultación especial (pues del contexto se desprende enseguida de qué ciudad se trata); quizá solo el imprimir con ello un pequeño toque personal a la narración.

Hay un mensaje en la Biblia, sin embargo, que sin sufrir transformación alguna en sus símbolos, está rodeado de misterio. Aparece en el libro de Daniel, al hablar del festín del rey Baltasar, hijo de Nabucodonosor. Según cuenta el profeta, durante esta cena una mano fantasmagórica escribió sobre el muro estas palabras en arameo:

`MENE MENE TEQEL UFARSIN`

que significaban `MENE` = "contado", `TEQEL` = "pesado", `UFARSIN` = "dividido".[2] Ninguno de los

Figura 1. *El festín de Baltasar*, por Rembrandt (National Gallery, Londres).

sabios de Babilonia presentes en el convite supo leerlas (lo que resulta incomprensible) y menos darles un significado. Requerida la presencia de Daniel, este las leyó e interpretó para el rey: Dios ha *contado* los días de tu reinado y les ha señalado el límite; te ha *pesado* en la balanza, y te falta peso; tu reino se ha *dividido* y se lo entregan a medos y persas. El rey Baltasar de los caldeos fue asesinado esa noche y le sucedió el medo Darío. Rembrandt, en su célebre cuadro (Fig. 1), adopta la teoría de su amigo el rabino de origen portugués Menasseh ben Israel (Manoel Dias Soeiros), según el cual es posible que los sabios y magos de Babilonia no supieran leer el escrito porque en este se dispusieron las letras de cada palabra en vertical (de arriba a abajo), y luego las palabras de derecha a izquierda, tal como Rembrandt las pinta (`mene`, `mene`, `teqel`, `ufar`, `sin`, diviendo la última en dos), en lugar de seguir el tradicional sistema hebreo de escritura de derecha a izquierda.

Hace 25 siglos los éforos de Esparta intercambiaban mensajes secretos con sus generales mediante la *escítala*, un cilindro en el que se enrollaba una cinta de cuero, sobre la que, en sentido del eje, se escribía luego el mensaje. Desenrollada la cinta, el mensaje resultante a lo largo de la misma resultaba ininteligible. Solo colocando la cinta sobre otra escítala de

[1] Una excelente referencia para la historia de la criptología es: Kahn, D., THE CODEBREAKERS: THE STORY OF SECRET WRITING, Macmillan, New York 1967.

[2] En otras versiones de la Biblia, figuran como palabras escritas en el muro: `MANE`, `TECEL`, `FARES`, con igual lectura que la dada en el texto.

iguales dimensiones que la primera podía recuperarse el mensaje original. Este método de cifrar se conoce como método de transposición, consistente en desplazar los caracteres de su sitio, sin cambiarlos. y es la forma más elemental de aplicar el *principio de difusión* de Shannon: para robustecer una cifra o criptosistema, conviene difuminar o dispersar la información del texto claro por todo el criptograma. Así, el mensaje

NOLI␣OBSECRO␣ISTUM␣DISTURBARE

escrito sobre una escítala en que la cinta dé 10 vueltas, daría lugar, tras desarrollar la cinta, al criptograma

NRIOOSL␣TIIU␣SROTBBUASMRE␣ECD

El descifrado es bastante simple: escribir el criptograma en columnas sucesivas de *n* elementos, variando *n* hasta que la lectura luego por filas sucesivas corresponda a un mensaje inteligible.[3]

Dual a este principio, es el *principio de confusión*, formulado como el anterior por Shannon en 1949: para fortalecer la seguridad de un criptodistema, la relación entre la clave y el texto cifrado debe ser compleja. Su implementación más elemental consiste en cambiar los caracteres de la escritura por otros, pero sin moverlos de su sitio. De esta manera se altera la distribución estadística de los caracteres. Ejemplo famoso de este último proceder es la cifra de César (de la que habla el historiador Suetonio en LAS VIDAS DE LOS CÉSARES), utilizada por Julio César para comunicarse con los generales de las legiones desperdigadas por el imperio romano.[4] Es muy simple: sustituir cada letra del alfabeto por la que viene en este tres lugares más tarde. Así, el mensaje

VENI VIDI VICI

pasaría a ser el criptograma o mensaje cifrado

YHQL YLGL YLFL

Su descifrado es una operación trivial, bastando con sustituir cada letra del criptograma por la que viene en el alfabeto tres lugares antes.

El procedimiento cesáreo es un caso muy particular del método llamado de sustitución monoalfabética, consistente en reemplazar cada símbolo de la escritura por el correspondiente tras una permutación arbitraria, pero fija, del conjunto de símbolos (letras y signos de puntuación). Es claro que no sería muy indicado probar con cada una de las $28! \approx 3{,}05 \times 10^{29}$ permutaciones posibles de las 27 letras del alfabeto castellano más un signo blanco de separación de palabras (prescindimos de acentos, mayúsculas y otros signos ortográficos) hasta conseguir que de un criptograma obtenido por este método de sustitución monoalfabética surgiese un texto inteligible. Pero existe un buen procedimiento de descifrado para este tipo de criptogramas. Fue ideado por los árabes en el siglo IX, concretamente, por el famoso sabio persa Abu-Yusuf Ya'qub ibn Ishaq al-Kindi (800-873). Con él nace el criptoanálisis.

Autor de casi 300 libros sobre matemáticas, linguística, astronomía, música y medicina, al-Kindi presenta en su Manuscrito acerca del descifrado de mensajes criptográficos el método basado en las frecuencias con que cada símbolo aparece en un determinado idioma a lo largo de un texto cualquiera normal. Haciendo el análisis de frecuencias para el criptograma a descifrar, basta con correlacionar los símbolos de frecuencia similar en el texto estándar elegido para el análisis y en el criptograma para conseguir el descifrado. Esta idea básica funciona bastante bien, aunque las inevitables fluctuaciones estadísticas hacen que a menudo haya que recurrir al ingenio y al sentido común para establecer las correlaciones alu-

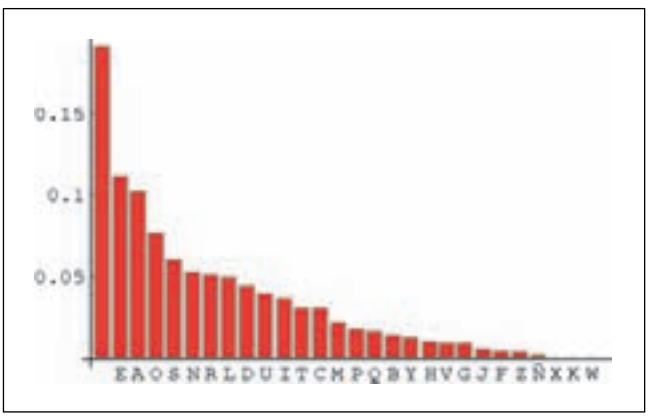

Figura 2. Frecuencias del espacio en blanco y de las letras en los diez primeros capítulos del Quijote.

[3] En el ejemplo anterior, $n = 3$.

[4] Una cifra análoga aparece en el Kama Sutra.

didas en casos en que varios símbolos presentan frecuencias muy similares. No hace falte advertir que cuanto más largo sea el texto estándar y el criptograma mejores serán las apreciaciones estadísticas.

Cada idioma tiene su tabla de frecuencias para textos normales y de gran longitud (para aminorar las fluctuaciones).[5] En la Fig. 2 podemos ver la tabla para el castellano.

El Cuadro I muestra la ordenación de las letras, de mayor a menor frecuencia, para distintos idiomas.

Deutsch	.....	ENIRSATUD	...
English	.....	ETAOINSHR	...
Español	.....	EAOSNRLDI	...
Français	.....	EAISTNRUL	...
Italiano	.....	EAIONLRTS	...

Cuadro I. Ordenación de las letras según sus frecuencias, de mayor a menor, en varios idiomas.

Hasta los siglos XIX y XX se avanzó relativamente poco en la criptografía, que se limitó a usar los sistemas antes expuestos y combinaciones o extensiones de los mismos. La llegada del telégrafo a principios del XIX invitó a meditar sobre sistemas de codificación y métodos criptográficos robustos con los que comprimir y ocultar la información transmitida por las líneas telegráficas. Las dos guerras mundiales del siglo XX impulsaron aún más el desarrollo de criptosistemas, y el uso generalizado de los medios electrónicos de comunicación para la alta política, las finanzas y el comercio a partir del tercio último del pasado siglo han convertido en tema de atención y preocupación prioritarias.

III. CIFRADO DE VERMAN

Gilbert Vernam fue un ingeniero de la ATT (American Telephone and Telegraph Co.) que propuso en 1917, siendo muy joven, el único criptosistema del que se puede probar que, debidamente usado, es inexpugnable con seguridad tanto mayor cuanto mayor sea la longitud del criptograma.[6]

Para cifrar por el método de Vernam se puede proceder de esta manera:[7]

1. Pásese a binario el texto llano a cifrar; por ejemplo, si el texto es

   `el␣siglo␣de␣los␣quanta`

   su expresión en binario es

   ```
   11001010110110000100000111100111
   11101001011001111111011000110111
   10010000011100100111001010010000
   00111011000110111101110011101000
   00011110001011101011110000111101
   11101111010001100011
   ```

2. Tómese una sucesión binaria aleatoria de longitud mayor o igual que la del texto binario a cifrar. Por ejemplo:

   ```
   00101101100110010011110001010100
   01111101111011011111000010000111
   10010000001011111001101111110010
   00100110111101111000001001101011
   11111101100000011000100001101111
   10001100111000000010000...
   ```

3. Sumemos término a término y módulo 2 (operación XOR) las dos secuencias anteriores. Así resulta el criptograma

   ```
   11100111010000010111110110110011
   10010100100010100001110011101000
   00000000010111011111010010110001
   00011101111011000101111101000001
   11100011101011110011010001010011
   01100011101001100 1011
   ```

[5] Insistimos en que sean textos ordinarios, estándar o normales en el idioma en cuestión, no sirviendo, por ejemplo, los lipogramas o textos en que no aparece nunca una determinada letra del alfabeto. Cuanto mayor sea la frecuencia de dicha letra en los textos ordinarios, más dificultad presenta el lipograma. Como ejemplo, citemos a Enrique Jardiel Poncela, quien en su relato UN MARIDO SIN VOCACIÓN (1926/27), omite sistemáticamente la "e". He aquí una muestra: *Un día —muchos lustros atrás—, cuando más olían las rosas y mayor sombra daban las acacias, un microbio muy conocido atacó, rudo y voraz, a Ramón Camomila: la furia matrimonial. "¡Hay un matrimonio próximo, pollos!", advirtió como saludo a su amigo Manolo Romagoso cuando subían juntos al casino y toparon con los camaradas más íntimos. (...) Y Ramón Camomila salió como una bala a buscar novia por la ciudad.*

[6] Vernam, G. S., *Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications*, J. Amer. Inst. Elec. Eng. 45, 109-115, 1926.

[7] En realidad, puede implementarse en cualquier base, por ejemplo en base 28 (correspondiente a nuestro alfabeto en minúsculas, sin acentos, y con ␣ como signo de espacio en blanco.

4. Si el destinatario del criptograma posee una réplica exacta de la secuencia aleatoria usada para encriptar, podrá recuperar el mensaje en claro restándola (o lo que es igual, sumándola, por ser aritmética binaria) del criptograma término a término y módulo 2. Para quien no disponga de esa copia, el criptograma recibido equivale a una secuencia aleatoria de la que no puede extraer un mensaje con sentido.
5. Ahora bien, si el mismo trozo de clave aleatoria se usa para cifrar dos textos distintos, una tercera persona en posesión de los dos criptogramas resultantes podrá obtener información valiosa simplemente sumando éstos módulo 2, pues tal operación eliminará la presencia por completo la presencia de la clave y el resultado será la suma de los mensajes originales. De aquí el nombre que se le da también a este método de cifrar: "cuaderno de usar y tirar", o "block de uso único".

La demostración, debida a Shannon, de la seguridad absoluta del sistema Vernam de cifrado es sumamente sencilla.[8] Se trata de probar que el disponer de un criptograma obtenido por el método Vernam no arroja ninguna información sobre el texto claro, llano, o texto original, en otras palabras, que la información relativa $I(M:C)$ entre los conjuntos *M* de textos claros y *C* de criptogramas es nula: $I(M:C)=0$.

Sean: *M* el conjunto de los textos claros, con distribución de probabilidad p_M; *K* el conjunto de claves, con probabilidades p_K; y $C:=\cup_{k\in K}E_k(M)$ el conjunto de los criptogramas, donde $E_k:m\mapsto E_k(m)$ es la transformación (inyectiva) de cifrado. Finalmente, sea $D_k:c\mapsto D_k(c)$ la transformación de descifrado; obviamente $D_k\circ E_k=\mathrm{id}_M$. En el conjunto *C* hay una distribución inducida de probabilidad p_C de los criptogramas dada por

$$p_C(c)=\sum_{k\in K:c\in E_k(M)} p_K(k)\,p_M\left(D_k(c)\right) \qquad (1)$$

Nótese también que $\sum_{k\in K:m=D_k(c)}p_K(k)$ es la probabilidad condicional $p_C(c|m)$ del criptograma *c* supuesto que *m* sea el texto llano. Luego el teorema de Bayes implica que

$$p_M(m|c)=\frac{p_M(m)\sum_{k\in K:m=D_k(c)}p_K(k)}{\sum_{k\in K:c\in E_k(M)}p_K(k)\,p_M\left(D_k(c)\right)}. \qquad (2)$$

Aplicando esto a nuestro caso, para mensajes binarios de longitud *N* tenemos $p_K(k)=2^{-N}$ (cada clave es una sucesión aleatoria de *N* bits), y

$$p_C(c)=2^{-N}\sum_{k\in K:c\in E_k(M)}p_M\left(D_k(c)\right)=2^{-N}\sum_{k\in K}p_M(c-k).$$

Pero $\sum_{k\in K}p_M\left(D_k(c)\right)=\sum_{m\in M}p_M(m)=1$, pues D_k es una biyección de $E_k(M)$ sobre *M*. Luego

$$p_M(m|c)=p_M(m), \qquad (3)$$

y por tanto la recepción del criptograma *c* no añade información alguna sobre el mensaje original *m*. Dicho de otro modo, $H(M)=H(M|C)$, y por tanto $I(M:C)=0$, como queríamos demostrar.

Veamos, para concluir esto, que la seguridad está comprometida cuando la longitud de la clave aleatoria es menor que la del texto claro. De las propiedades de la entropía de Shannon se deduce que

$$\begin{aligned} H(M,K,C)&=H(M|K,C)+H(K|C)+H(C),\\ &=H(K|M,C)+H(M|C)+H(C), \end{aligned} \qquad (4)$$

y como cada clave y criptograma determina el texto claro, $H(M|K,C)=0$, por lo que

$$H(K|M,C)=H(K|C)-H(M|C), \qquad (5)$$

y por tanto

$$H(K|C)\geq H(M|C). \qquad (6)$$

Como quiera que $I(M:C)=H(M)-H(M|C)$, y además $H(K)\geq H(K|C)\geq H(M|C)$, resulta

$$I(M:C)=H(M)-H(M|C)\geq H(M)-H(K). \qquad (7)$$

Luego si queremos que $I(M:C)=0$, forzosamente deberá cumplirse

$$H(K)\geq H(M). \qquad (8)$$

[8] Ver, por ejemplo, D.R. Stinson, CRYPTOGRAPHY. THEORY AND PRACTICE, CRC Press, Boca Raton 1995.

En consecuencia, para la seguridad absoluta de un método de cifrado es condición necesaria que la entropía del conjunto de claves sea igual o mayor que la del conjunto de textos claros. En particular, este es el caso de la cifra Vernam, pues en ella se tiene: 1/ $|H|=|K|=|C|$; 2/ por ser las claves secuencias aleatorias de bits, $H(K)=\log_2|K|$; y 3/ $H(M)\leq \log_2|M|=\log_2|K|=H(K)$.

Figura 3. Hoja de cifrado Vernam utilizada por Che Chevara.

La cifra Vernam ha sido y es ampliamente utilizada. Che Guevara la empleó para comunicarse confidencialemente con Fidel Castro desde Bolivia (Fig. 3). La Casa Blanca y el Kremlin recurren a ella para su comunicación mutua sobre temas de alta seguridad. Su uso descuidado por el matrimonio Rosenberg y por Fuchs, espías atómicos que pasaron información vital sobre las armas atómicas desde los EEUU a la vieja URSS, y que reutilizaron varias veces la misma clave aleatoria para sus cifrados, permitió su desenmascaramiento.

IV. CIFRADO DE CLAVE PÚBLICA

El imperativo de usar sólo una vez la clave aleatoria del cifrado Vernam es un obstáculo a su uso generalizado. La reposición constante de nuevas sucesiones aleatorias, compartidas por remitente y destinatario, plantea un importante problema de seguridad que ensombrece los méritos propios indiscutibles de este criptosistema.

En la década de los 70 los estadounidenses Diffie y Hellman[9], y Merkle[10] propusieron la criptografía de clave pública (PKC) que permite a dos usuarios, que nunca se han conocido, comunicarse secretamente a través de un canal público.[11]

La idea, cuando ya se conoce, es realmente simple. Supongamos que existe un procedimiento públicamente conocido $k(X)$ de cifrado $m\mapsto c_{k(X)}(m):=E_{k(X)}(m)$ tal que su inversión $c_{k(X)}(m)\mapsto E^{-1}_{k(X)}\left(c_{k(X)}(m)\right)=m$ es realmente costosa en tiempo salvo para la persona X que ha preparado la clave $k(X)$ y dispone explícitamente de la clave inversa $D_{k(X)}$. Diremos en ese caso que la función $E_{k(X)}$ es de dirección única con "puerta trasera". Cada persona X que quiere recibir y mandar información confidencial elige una tal clave $k(X)$ y la hace pública. Si otra persona Y quiere transmitirle un mensaje cifrado que solo X pueda descifrar basta con que lo cifre mediante la clave $k(X)$ de X y se lo mande a este. Si otro, Z, lo intercepta, no podrá descifrarlo en la práctica, pues la inversión de la clave pública $E_{k(X)}$ le llevará eones. Sólo X, que ha preparado astutamente $k(X)$, dispone de la clave inversa que le permite descifrar sin ningún esfuerzo.

Más aún. La PKC permite la firma digital. Si el remitente Y quiere "firmar" su mensaje a X, de forma que este sepa que el mensaje recibido proviene de Y y no de otro, basta que el mensaje m a enviar por Y a X tenga un apéndice f_Y, la firma o nombre de Y , debidamente transformado antes a $D_{k(Y)}(f_Y)$, de modo que Y envía a X el mensaje compuesto

$$\left(E_{k(X)}(m)/D_{k(Y)}(f_Y)\right). \qquad (9)$$

A su recepción, X lo descifra como

---

9 W. Diffie, M.E. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory **22**, 644-654 (1976).

10 R.Merkle, *1974 CS244 Project Proposal*. Primer documento, no publicado, describiendo la criptografía pública. Ver `http://www.merkle.com/merkleDir/papers.html`

11 Al desclasificar documentación secreta, el GCHQ (Government Communications Headquarters) británico ha desvelado que varios matemáticos y criptógrafos (James Ellis, Clifford Cocks y Malcolm Williamson) a su servicio ya se habían adelantado varios años a Hellmann y a sus dos estudiantes Diffie y Merkle en el descubrimiento de la PKC y de algunas de sus implementaciones, como el famoso sistema RSA que luego comentaremos.

$$\left(D_{k(X)}\left(E_{k(X)}(m)\right)\Big/E_{k(Y)}\left(D_{k(Y)}(f_Y)\right)\right)=(m/f_Y), \qquad (10)$$

con su clave privada y la pública de Y. Sólo Y es capaz de cifrar su firma de modo que al transformarla con su clave pública aparezca su nombre.

Decíamos que la PKC se basa en el uso de funciones unidireccionales con puerta trasera, funciones g de complejidad polinómica, esto es, $g\in\mathbf{P}$, tales que sus inversas satisfagan $g^{-1}\in\mathbf{NP}\setminus\mathbf{P}$. El problema es que no se conoce ninguna función para la que estemos absolutamente seguros de la dificultad de su inversión. Se sabe, eso sí, de funciones para cuyas inversas no disponemos ahora de algoritmos de cálculo que permitan evaluarlas en tiempo polinómico, pero nadie sabe si en el futuro tales algoritmos se encontrarán. De hecho, en el año 1994 se produjo un espectacular revuelo en este campo, ya que el sistema de clave pública RSA (iniciales de Rivest, Shamir y Adleman) que comentaremos a continuación, y cuya seguridad reside en la dificultad de factorizar números enteros N muy grandes, vio como en el campo de la computación cuántica aparecía un algoritmo, debido a Shor,[12] que permitía, en principio, factorizar en tiempo polinómico en el número de cifras de N. De momento, los ordenadores cuánticos a gran escala quedan aún lejanos, y el método se sigue utilizando para cifrar, pero se está ojo avizor sobre los avances matemáticos que conduzcan a algoritmos que permitan romper el criptosistema de clave pública RSA, u otros, con ordenadores clásicos.

Como funciones útiles en la actualidad para la criptografía PKC se tienen, entre otras, estas:

1. El producto de enteros $n_1n_2...n_k=n$ (fácil) y la factorización de enteros $n=p_1^{n_1}p_2^{n_2}...p_k^{n_k}$ (difícil), a no ser que se disponga de información adicional (como conocer, por ejemplo, los factores primos p_j de n). El sistema RSA está basado en esta función.[13]
2. El cálculo de potencias $a^n=b$ en un cuerpo finito (o de Galois) GF_q es un problema computacionalnente sencillo, pero no en general su cálculo inverso, esto es, el cálculo de logaritmos discretos $n=\log_a b$. El criptosistema ElGamal se apoya en esta función.[14]
3. El conjunto de puntos de las curvas elípticas sobre un cuerpo finito de característica ≥4 es un grupo abeliano (ver Fig. 4). La operación $\{P,n\}\mapsto Q=nP$ es computacionalmente fácil, Pero la operación inversa $\{P,Q\}\mapsto n="Q/P"$ es difícil. En este hecho se apoya la criptografía sobre curvas elípticas.[15] Quizás no nos sorprenda mucho esta dificultad en el cálculo de la inversión de $\{P,n\}\mapsto Q=nP$ viendo el crecimiento exponencial con n^2 de la *altura* $\max(|a_n|,|b_n|,|c_n|,|d_n|)$ de cada punto $nP=(a_n/b_n,c_n/d_n)$, a través de la Fig. 5.
4. Sea un cuerpo cuadrático imaginario $F:=\mathbb{Q}(\sqrt{D})$, donde D es un entero negativo libre de cuadrados. Si I, J son ideales en F, su producto IJ es el ideal formado por los elementos de F que son

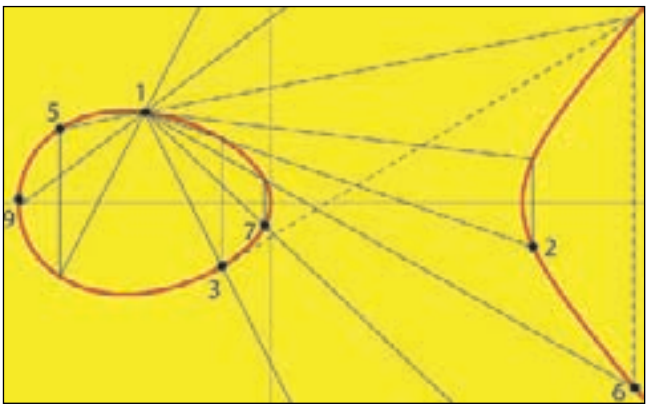

Figura 4. Curva elíptica $y^2=x(x^2-36)$ y puntos de la forma nP, con $P=(-3,9)$, y $n=1,...,9$. Los numeros en el gráfico indican el valor de n asociado. Cada punto nP se ha obtenido gráficamente como $(n-1)P+P$. Los puntos para $n=4,8$ caen fuera de los límites del dibujo. Se ilustra con línea discontinua la obtención alternativa de $6P$ como $3P+3P$.

[12] P.W. Shor, *Algorithms for Quantum Computation: Factoring and Discrete Logarithms*, Proc. 35th Annual Symposium on Foundations of Computer Science, ed. S. Goldwasser (IEEE Press, Bellingham), 124-134, 1994.

[13] R. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, **21** (2), 120-126 (1978).

[14] T. ElGamal, *A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*, IEEE Transactions on Information Theory, IT-**31**, n. 4, 469-472 (1985).

[15] V. Miller, *Uses of elliptic curves in cryptography*, Lecture Notes in Computer Science 218, 417-426 (1985) (Advances in Cryptology-CRYPTO '85, Springer-Verlag); N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation **48**, 203-209 (1987).

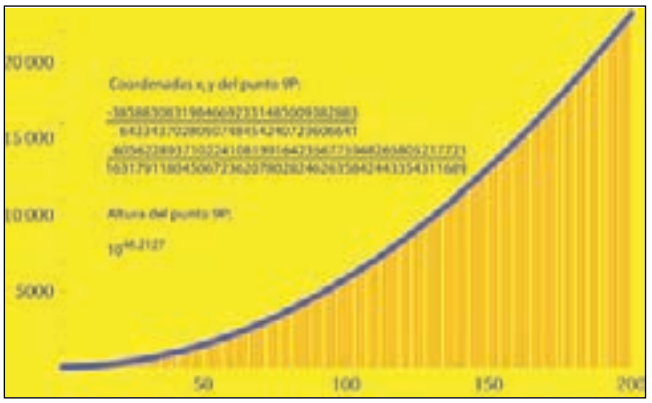

Figura 5. Curva del $\log_{10}$ de las alturas de los 200 primeros puntos *nP* considerados en la figura anterior. Damos las coordenadas del punto 9*P*. Puede verse que la altura crece como $O(10^{n^2})$.

sumas finitas $\sum x_k y_k$, con $x_k \in I$, $y_k \in J$. El problema de calcular $J = I^n$ es fácil. Por contra, la búsqueda de $n := \log_I J$ es computacionalmente difícil. En esto se basa el criptosistema de clave pública debido a Buchmann-Williams.[16]

El algoritmo de Shor rompe la dificultad en la inversión de las funciones base de los tres primeros sistemas que acabamos de mencionar, haciendo inseguros esos criptosistemas el día en que la computación cuántica a gran escala sea una realidad. Otro algoritmo cuántico más reciente y más potente, debido a Hallgren, hace lo mismo con el problema inverso en el criptosistema de Buchmann-Williams.[17]

A. Generación de clave compartida

Diffie y Hellman[18] fueron los primeros en proponer un sencillo procedimiento para que dos personas cualesquiera *X*, *Y* puedan generar y compartir una clave aleatoria que solo ellos conocerán, y que podrá servirles para intercambiarse mensajes cifrados con total seguridad si mantienen la precaución de no usar la clave más de una vez.

Esas personas acuerdan utilizar un mismo entero $g \in \mathbb{F}_q$, generador del grupo multiplicativo $\mathbb{F}_q^*$. Tanto el cuerpo $\mathbb{F}_q$ como g son públicos. Ambos *X* e *Y* eligen secretamente sendos exponentes privados n_X, n_Y en el intervalo $[1, q-1]$, y hacen públicos los resultados g^{n_X}, g^{n_Y}. Pues bien, la clave a compartir es simplemente $g^{n_X n_Y}$, clave que solo ellos pueden calcular: *X* la obtiene tomando el resultado público g^{n_Y}, y elevándolo a la potencia de exponente n_X que él solo conoce; e *Y* la obtiene partiendo de g^{n_X}, y elevándolo a su exponente privado n_Y. La seguridad del método reside en que para una tercera persona *Z*, conocedora únicamente de los datos públicos $\mathbb{F}_q, g, g^{n_X}, g^{n_Y}$, la obtención de $g^{n_X n_Y}$ es, en la actualidad, un problema computacionalmente duro, al menos tanto como el problema del logaritmo discreto, pues es claro que si fuera fácil obtener los exponentes n_X, n_Y de los datos públicos este sistema no sería fiable.

B. Método RSA

El sistema RSA de clave pública es el más popular, con seguridad basada en la dificultad de factorizar enteros grandes. La clave pública de *X* consiste en un par de números enteros $\big(N(X), c(X)\big)$, el primero muy grande, digamos de un millar de dígitos, y el otro en el intervalo $\big(1, \phi\big(N(X)\big)\big)$ y coprimo con $\phi\big(N(X)\big)$, siendo ϕ el indicador o función indicatriz de Euler ($\phi(n)$ es el número de coprimos con *n* en el intervalo $[1, n]$).

Tras transformar el remitente *Y* su mensaje *M* en secuencia de números (binarios, decimales, o en la base que se convenga), lo rompe en bloques $B < N(X)$ de longitud máxima, cifra cada bloque *B* según

$$B \mapsto C_X(B) := B^{c(X)} \mod N(X)$$

y manda la secuencia de criptogramas $C_X(B)$ a *X*. Denotemos esta operación de cifrado como $M \mapsto C_X(M)$.

El destinatario *X* descifra cada $C_X(B)$ como

$$C_X(B) \mapsto B := C_X(B)^{d(X)} \mod N(X)$$

16 J.A. Buchmann, H.C. Williams, *A key-exchange system based on imaginary quadratic fields*, Journal of Cryptography, **1**, 107-118 (1988).

17 Hallgren, S., *Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem*, Proceedings of the 34th Annual ACM Symposium on Theory of Computing, 653-658 (2002).

18 W. Diffie, M.E. Hellman, *loc. cit.*

donde el exponente $d(X)$ para el descifrado es la clave privada de X, y que no es otro que la solución a

$$c(X)d(X)=1 \mod \phi(N(X))$$

Esa solución es

$$d(X)=c(X)^{\phi(\phi(N(X)))-1} \mod \phi(N(X)).$$

El descifrado lo indicaremos por $C_X(M)\mapsto D_X(C_X(M))=M$, donde el símbolo D_X alude a la clave privada o secreta de X. En principio, cualquiera puede calcular $d(X)$, pues se conocen $c(X)$ y $N(X)$, y así romper el secreto. Y aquí es donde entra ahora la astucia de X. Para ponérselo muy difícil a una tercera persona Z, mejor es que se atenga a ciertas normas, entre las que destacan las siguientes:

- Debe X escoger el módulo $N(X)$ como producto de dos primos enormes y aleatorios (de al menos medio millar de dígitos cada uno) p_1, p_2, y no muy próximos entre sí (basta que las longitudes de sus expresiones difieran en unos pocos bits), pues de lo contrario a Z, que conoce $N(X)$, no le costaría mucho encontrar dichos factores. Hay que evitar tomar primos que estén en tablas o sean de formas muy especiales. Los algoritmos conocidos de primalidad facilitan la elección de p_1, p_2.
- Como X conoce p_1, p_2, sabe ya calcular $\phi(N(X))$ como $(p_1-1)(p_2-1)$. Ahora tiene que escoger X un entero $d(X)$ (su clave privada) al azar en el intervalo $(1,\phi(N(X)))$, coprimo con $\phi(N(X))$, y calcular la clave pública $c(X)$ mediante $c(X)=d(X)^{\phi(\phi(N(X)))-1} \mod \phi(N(X))$, o mejor aún, usando el clásico algoritmo de Euclides.
- El número $d(X)$ no debe ser pequeño, para evitar que se pueda encontrar por prueba y error. Por eso conviene comenzar fijando la clave privada. Pero también hay que procurar que $c(X)$ no resulte demasiado pequeño, pues de lo contrario la interceptación de un mismo mensaje enviado a varios destinatarios con la misma clave pública aunque distintos módulos podría conducir sin mucho esfuerzo a su descifrado.

Cualquier persona que sólo conozca $N(X)$ pero no sus factores, aparentemente[19] tendrá primero que factorizar $N(X)$ para calcular $\phi(N(X))$, y con ello poder hallar el exponente para descifrar; pero factorizar un número de 1000 dígitos le llevaría a un supercomputador de 1000 Tflops unos 10^{17} años con el mejor algoritmo hoy conocido.

1. Un ejemplo práctico

Supongamos que la clave pública de X es el par de enteros:

$N(X)=$
25827284609103229171264345702644582573285897308839584715021483652919127678846322507033416095782767571848884487167464643241591821718810128287151803616030490319468215436312960045846629568787293882672502414853

$c(X)=7482620483517369$

y que Y quiere mandar a X este mensaje

```
Gravitatem␣in␣corpora␣universa␣
          fieri␣...
```

Primero lo transforma en número mediante un procedimiento convenido públicamente, y que puede consistir, por ejemplo, en reemplazar cada carácter z por su código ASCII menos 32: $\#(z)=\mathrm{ASCII}(z)-32$. De este modo, el mensaje anterior se convierte en el mensaje M dado por este número:

3982658673846584697700737800677982807982650085787386698283650070736982730014141 4

Su cifrado $C_X(M)$ es

$C_X(M)=$
2298016187879956669249924676843201291328535359628009168521829458283505306888152918011891391395663643672134348735403808791691144577301842706460159822177606679794144297221284689340415853472670419881348640625 5

Para descifrar el mensaje recibido, X aplica su clave privada. Hasta este momento, es el único que la cono-

[19] "Aparentemente", porque se ignora si existen o no procedimientos alternativos para descifrar $C_X(B)$ que no pasen por la obtención del exponente inverso, o si el cálculo de éste exige forzosamente conocer los factores primos de N.

ce, pero como piensa cambiar de inmediato su clave pública por otra más segura (dados los tiempos que corren), nos autoriza a hacerla pública aquí:

$d(X) =$
15612316042772942908476960237785255816222650264548214062249151955883494346298625387472091609474328238534371484182499816428240426723144585334345621432432382247832895040226734114223827494435274812517427336157

El lector no tendrá dificultad en comprobarla sabiendo que $N(X) = p_1 p_2$, siendo p_1, p_2 los siguientes primos:

$p_1 =$
25782112983162066965574348370667745263115517969260361901338029443631059816114242364704348997476862450 27

$p_2 =$
10017520529046887334320471395922235351755553148570843883640372997638277230691068526640428184762272624439

Pequeñas variaciones en el mensaje original producen distorsiones exageradas en el criptograma correspondiente. Por ejemplo, el texto M' dado por

Gravitaten␣in␣corpora␣universa␣ fieri␣...

difiere solo en una letra del anterior, pero su cifrado resulta muy distinto al de M:

$C_X(M') =$
17365780329918613123227703743378086098207664218801417133752283829906176833206154287445793028410246595594516809393421963293495433419255131273152208943996589649445606203314045244952099968205621554360788723710

En noviembre de 2005 se anunció la factorización del RSA-640, un número semiprimo de 640 bits (193 dígitos) que tiene dos factores primos de 320 bits cada uno. Requirió 4.5 meses de cálculo con unas 80 CPUs a 2.2 GHz. Por ello se recomienda, como norma de seguridad, utilizar números $N(X)$ de al menos 1024 bits, sugiriendo llegar a los 2048 bits si la información es de capital importancia.

V. GENERACIÓN CUÁNTICA DE CLAVES Y SU DISTRIBUCIÓN

Ya hemos dicho que sobre la seguridad de los criptosistemas de clave pública conocidos pende como espada de Damocles la amenaza de su rotura mediante la computación cuántica.[20] Pero los mismos principios físicos que rigen estos ataques propician a la vez mecanismos de salvaguarda. Concretamente, vamos a ver cómo las leyes cuánticas hacen posible sistemas de generación y distribución de claves aleatorias compartidas exclusivamente por dos sujetos X e Y, de modo que estos pueden hacer uso de ellas para transmitirse información cifrada que nadie más puede descifrar. Van a ser aspectos intrínsecos de la naturaleza, como la linealidad de la evolución cuántica y el principio de indeterminación, los garantes insobornables de la seguridad.

El pionero y, en los comienzos, incomprendido visionario en este poderoso campo de la información cuántica fue Wiesner.[21] Sus amigos Bennett y Brassard recogieron su antorcha, y con aceite propio, engendraron la criptografía cuántica.[22] Como dice Brassard:[23]

> *Quantum cryptography is the only approach to privacy ever proposed that allows two parties (who do not share a long secret key ahead of time) to communicate with provably perfect secrecy under the nose of an eavesdropper endowed with unlimited*

---

20 Galindo, A., *Quanta e información*, Revista Española de Física **14** (Número especial: Cien años de quanta), 30-48 (2000).
Galindo, A., Martín-Delgado, M.A., *Information and computation: classical and quantum aspects*, Rev. Mod. Phys. **74**, 347-423 (2002).
A. Galindo, DEL BIT AL QUBIT, Memoria de 101 pág. con el texto de la Lección Inaugural de Curso Académico 2001-2002, publicado por la Universidad Complutense.

21 Wiesner, S., *Conjugate coding*, SIGACT News **15:1**, 78-88 (1983). (Manuscrito *circa* 1970.)

22 C.H. Bennett, G. Brassard, S. Breidbart, S. Wiesner, *Quantum cryptography, or Unforgeable subway tokens*, en ADVANCES IN CRYPTOLOGY: PROCEEDINGS OF CRYPTO '82, Santa Barbara, Plenum Press, pp. 267-275, August 1982.
C.H. Bennett, G. Brassard, S. Breidbart, *Quantum Cryptography II : How to reuse a one-time pad safely even if P=NP*, Rejected from 15th Annual ACM Symposium on Theory of Computing, Boston, May 1983. Historical document dated "November 1982" available from the first two authors.

23 G. Brassard, *Brief History of Quantum Cryptography: A Personal Perspective*, arXiv:quant-ph/0604072 v1.

computational power and whose technology is limited by nothing but the fundamental laws of nature.

El primer protocolo de distribución cuántica de claves se debe a Bennett y Brassard.[24] Por eso se conoce como protocolo BB84.

Su primera implementación experimental fue también impulsada por estos autores.[25] Cuenta Brassard que el ruido de la fuente de alimentación usada para accionar las células de Pockel en el prototipo de esta realización era tal que podían "oirse" los fotones y sus polarizaciones, de modo que el protocolo solo aseguraba la confidencialidad de la clave en el caso de que los posibles espías fueran sordos como tapias.

Más tarde se propusieron otros protocolos, como el B92 debido a Bennett,[26] o el de Ekert[27] basado en el entrelazamiento y las desigualdades de Bell. Aquí ilustraremos las ideas básicas con el B92.

VI. PROTOCOLO B92

La forma técnica de explicar este protocolo es mediante partículas de spin $\frac{1}{2}$, o bien con fotones polarizados. Para hacer esto más asequible, lo ilustraremos con unas cajas C muy especiales, que usamos idealmente para simular las propiedades de aquellos (Fig. 6). Se trata de unas cajas que, miradas de frente, muestran el interior de color rojo (cajas C_R) o de color verde (cajas C_V). Si las cajas rojas de frente C_R las miramos luego de lado, constatamos que en un 50% de los casos su interior nos aparecerá como rojo (cajas C^R), y en el otro 50% de los casos como verde (cajas C^V), y que, después de haber sido observadas de lado, han perdido su característica anterior de ser de tipo C_R, para pasar a ser de tipo C^R o C^V de acuerdo con el color observado de lado. Otro tanto nos pasa al mirar de lado las cajas que de frente eran verdes. Y viceversa; las cajas que de lado son rojas, al mirarlas después de frente las vemos rojas o verdes con igual probabilidad, y cambian consecuentemente de tipo. Y lo mismo pasa con las que de lado son verdes. Supongamos ahora unos filtros F también especiales (que van a hacer el papel de analizadores de polarización). Los hay de cuatro tipos: F_R,F_V, y F^R,F^V.

Los F_R actúan de esta manera:

1/ Dejan pasar todas las cajas C_R sin cambiarlas.

2/ Bloquean (no dejan pasar) las cajas C_V.

3/ A las cajas C^R,C^V las dejan pasar solo en un 50% de los casos, y a aquellas que pasan, las cambian en cajas C_R.

De forma análoga (con los cambios oportunos de R por V y/o de subíndice por superíndice) actúan los otros filtros. Como ilustración, ver Fig. 7.

Dos personajes, Alicia y Benito, alejados entre sí, quieren intercambiarse una clave binaria aleatoria. Proceden del siguiente modo (Fig. 8):

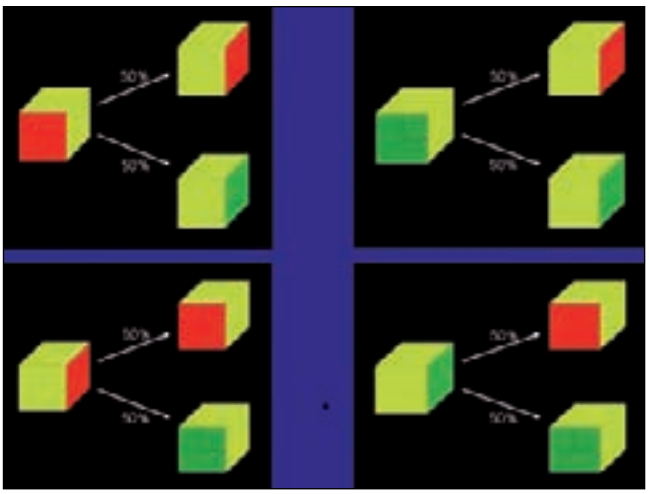

Figura 6. Cajas especiales vistas de frente y de lado.

[24] C.H. Bennett, G. Brassard, *Quantum cryptography and its application to provably secure key expansion, public-key distribution, and coin-tossing*, Proceedings of IEEE International Symposium on Information Theory, St-Jovite, Canada, page 91, September 1983; *Quantum cryptography: Public key distribution and coin tossing*, Proceedings of IEEE International Conference on Computers, Systems & Signal Processing, Bangalore, India, pp. 175-179, December 1984; *The dawn of a new era for quantum cryptography: The experimental prototype is working*, Sigact News **20** (4), 78-82 (1989).

[25] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, *Experimental quantum cryptography*, Journal of Cryptology **5** (1), 3-28 (1992).

[26] C.H. Bennett, *Quantum cryptography using any two nonorthogonal states*, Phys. Rev. Lett. **68**, 3121-3124, (1992).

[27] A.K. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67** (6), 661-663 (1991).

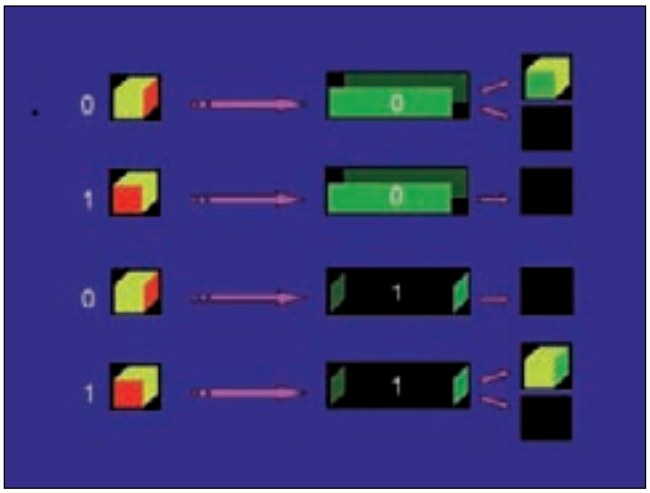

Figura 7. Efecto de los filtros F_V, F^V sobre las cajas C_R, C^R que les llegan.

1/ Alicia se prepara una sucesión aleatoria $a_1a_2...$ de bits 0 y 1.

Asimismo, Benito se prepara otra sucesión aleatoria $b_1b_2...$ de bits 0 y 1.

2/ Para cada $i = 1,2, ...$, Alicia le manda a Benito sucesivamente, por un canal de transporte que no altera el estado de las cajas —en la práctica será un canal cuántico, como, por ejemplo, una fibra óptica en muchos de los casos en que las cajas son fotones— una caja

$$C^R \quad \text{si } a_i = 0, \qquad C_R \quad \text{si } a_i = 1.$$

3/ Benito somete la caja recibida a un filtro

$$F_V \quad \text{si } b_i = 0, \qquad F^V \quad \text{si } b_i = 1.$$

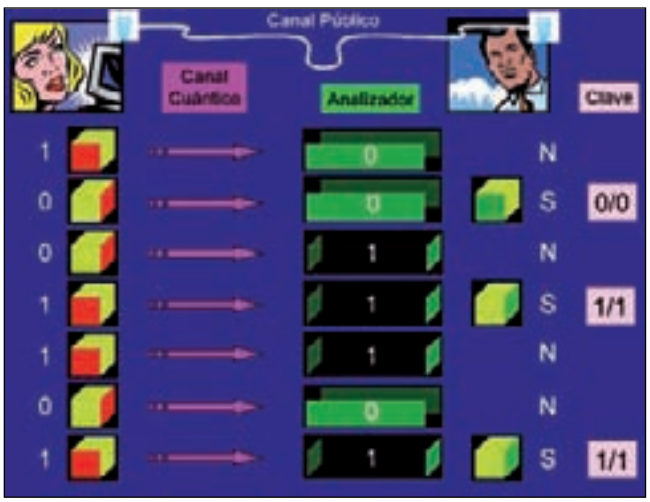

Figura 8. Realización del protocolo entre Alicia y Benito.

Si tras el filtro aparece una caja (no hay bloqueo), Benito escribe $s_i = S$; de lo contrario, define $s_i = N$. Así Benito engendra una nueva sucesión $s_1s_2...$ formada por *S*s y *N*s. ¡Obsérvese que $s_i = S$ sólo si $a_i = b_i$!

4/ Terminado el envío, Benito comunica pública y abiertamente (por teléfono, carta, o a grito pelado si es preciso) a Alicia los índices $i_1, i_2,...$ para los cuales $s_{i_k} = S$. De ese modo Alicia extrae de su secuencia inicial $a_1a_2...$ una subsecuencia, igualmente aleatoria, $a_{i_1}a_{i_2}$ ..., que coincide exactamente con la $b_{i_1}b_{i_2}$ ... de Bob. Esta será la secuencia aleatoria compartida por ambos y que solo ellos conocen. Fin del protocolo.

Por ejemplo, si

$$a_1a_2... = 10011011100101100 1011...$$
$$b_1b_2... = 00111011100111010 1001...,$$

una posibilidad sería

$$s_1s_2... = \texttt{NSNSNNSNNSNSNNNNSNNNN...}$$

con lo que la clave binaria aleatoria a compartir empezaría por

$$\texttt{011100...}$$

Es fácil ver que el número de *S*s sobre *N*s es asintóticamente 1/3, y que las poblaciones de 0s y de 1s en la clave final están equilibradas.

Imaginemos ahora que un personaje “malévolo”, un espía de apellido innombrable y conocedor del protocolo B92, quiere obtener información sobre tal clave. Podría, por ejemplo, conseguir observar durante su trayecto hasta Benito las cajas enviadas por Alice, y luego permitirles continuar su camino. Pero como no sabe si la caja *i*-ésima es de tipo C_R o C^R, si mira equivocadamente de lado a una C_R la mitad de las veces la verá como C^R, y la otra mitad como C^V, afectando con ello al tipo de la caja, y por tanto muy posiblemente al resultado obtenido por Benito con sus analizadores (Fig. 9). Se puede comprobar que, en efecto, esta estrategia de interceptar-reenviar por parte del espía tiene repercusiones detectables por Alicia y Benito: el cociente de *S*s sobre *N*s para a ser asintóticamente $3/5$, las claves finales de Alicia y Bob no coinciden, y si, por ejemplo, el espía es perezoso y siempre mira de frente las cajas interceptadas, las poblaciones de 0s y 1s están claramente desequilibradas, habiendo el doble de 0s que de 1s en la de Alicia, y la mitad de 0s que de 1s en la de Benito.

Figura 9. Perturbación producida por un espía perezoso en el protocolo entre Alicia y Benito.

En resumen, la "escucha" del espía en el canal cuántico, con la estrategia simple de interceptar-reemitir, altera el ritmo de generación de la clave secreta, la equidistribución de los 0s y 1s en la clave, y la igualdad de secuencias clave de Alicia y Benito.

En general, la imposibilidad cuántica de conocer el estado de un sistema cuya preparación se ignora si solo se dispone de una copia del mismo (no hay clonación cuántica de estados distintos no ortogonales) hace que la acción del espía deje un rastro inevitable; por eso siempre detectarán los "buenos" el fisgoneo del espía y podrán interrumpir el proceso de generación de claves hasta mejor ocasión, o continuar, una vez desechada la parte de clave más afectada, si ven que la información obtenida por el espía no compromete seriamente la seguridad en el uso de la clave restante.

Aunque el espía fuera mucho más sagaz, y en lugar de esta vulgar estrategia adoptara otra más inteligente, se ha demostrado que estos protocolos son incondicionalmente seguros ante cualquier ataque informático por sofisticado que sea. Aún así, siempre aparecen agujeros insospechados en torno a la implementación práctica de los protocolos por los que colarse la curiosidad por conocer lo prohibido.

VII. ESTADO DE LA CRIPTOGRAFÍA CUÁNTICA Y PERSPECTIVAS

En 1991 se implementó el protocolo BB84 en los laboratorios de IBM. Se generó una clave compartida entre dos puestos a 30 cm de distancia, mediante el envío por el aire de fotones polarizados. En los años siguientes se han ido experimentado otros protocolos como el B92 y los basados en el entrelazamiento.

Existen ya empresas de producción y venta de sistemas de criptografía cuántica.[28]

También la banca se ha apuntado a los nuevos tiempos en lo que a la criptografía atañe. La prensa mundial resaltó la primera transferencia bancaria realizada en Viena en 2004 bajo la (en principio) absoluta seguridad proporcionada por la criptografía cuántica, entre el Ayuntamiento de la ciudad y la Bank Austria Creditanstalt.[29]

La distribución cuántica de claves por fibra óptica ha alcanzado los 148.7 km de distancia con el protocolo BB84.[30][31]

Para terminar, diremos que a pesar de la seguridad perfecta (teórica) que brinda la criptografía cuántica, al lado de los físicos e ingenieros que desarrollen los protocolos hacen falta también los *crackers* cuánticos que

[28] En octubre de 2007 se usó la tecnología de encriptación cuántica desarrollada por la firma suiza *Id Quantique* para trasmitir al capitolio los resultados del cantón de Ginebra en las pasadas elecciones suizas.

[29] A. Poppe, A. Fedrizzi, T. Loruenser, O. Maurhardt, R. Ursin, H. R. Boehm, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, A. Zeilinger, *Practical Quantum Key Distribution with Polarization-Entangled Photons*, Opt. Express **12**, 3865-3871 (2004); arXiv:quant-ph/0404115v2.

[30] P.A. Hiskett, D. Rosenberg, C.G. Peterson, R.J. Hughes, S. Nam, A.E. Lita, A.J. Miller, J.E. Nordholt, *Long-distance quantum key distribution in optical fibre*, New J. Phys. **8**, 193(1-7) (2006).

[31] A través del aire la marca superior está en 144 km, entre las islas de La Palma y Tenerife de nuestro archipiélago canario. Ver: Tobias Schmitt-Manderbach, Henning Weier, Martin FÄurst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G. Rarity, Anton Zeilinger, Harald Weinfurter, *Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km*, Phys. Rev. Lett. **98,** 010504(1-4) (2007).

descubran lagunas en las implementaciones. No se conoce ninguna versión cuántica del sistema PKC. Quién sabe si la criptografía de clave pública sobrevivirá, al ataque cuántico, con funciones unidireccionales clásicamente tratables cuyas inversas sean cuánticamente intratables. Finalmente, para que la todavía muy joven criptografía cuántica sea competitiva con los métodos clásicos de cifrado y descifrado tendrá que dar un salto transcontinental en las distancias alcanzadas (¿repetidores cuánticos?) y lograr ritmos varios órdenes de magnitud más altos en la generación de claves.