MUJERES Y CRIPTOGRAFÍA

28 de noviembre de 2007

Paz Morillo

1. Un poco de historia

La relación entre las mujeres y la criptografía (escritura secreta) se remonta a tiempos muy, muy antiguos. Una de las primeras referencias de esta relación la hallamos en el Kama-Sutra, siglo IV después de Cristo. En este libro se describen las 64 artes que las mujeres deben estudiar y el arte nº45, *mlecchita-vikalda*, es el de la escritura secreta.

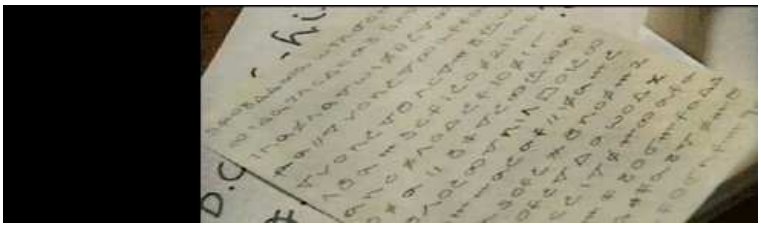
La mujer debe aprender mlecchita--vikalda para esconder sus relaciones amorosas. Se trata de un cifrado de sustitución, es decir, cada letra tiene su correspondiente símbolo de cifrado. A veces pares de letras o incluso palabras muy usadas se corresponden con un único símbolo.

Para comprender mejor el cifrado de sustitución veamos un ejemplo. En la siguiente tabla se muestra en una primera fila un alfabeto aleatorio y en la segunda fila el correspondiente alfabeto cifrado.

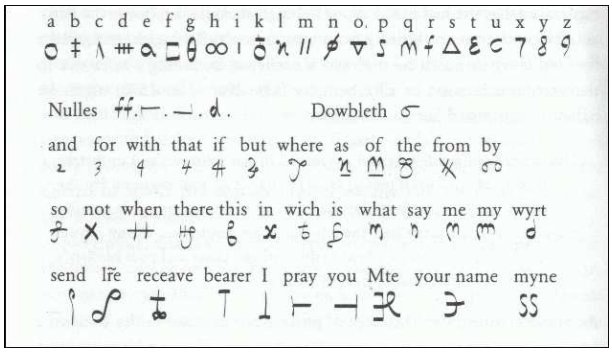
O	Y	D	M	P	F	V	C	R	E	H	S	I	N	U	B	A	Y
W	T	B	J	K	X	G	R	C	I	Q	Z	E	L	A	D	U	T

Para cifrar un mensaje se van sustituyendo las letras de la primera fila por las correspondientes en la segunda fila, así el mensaje "Buenos días" quedaría cifrado como " Dailwz beuz ".

Este tipo de cifrado por sustitución es uno de los métodos más utilizados en la criptografía clásica. Lo volvemos a encontrar en el siglo XVI cuando **María Estuardo** planea el asesinato de su prima Elisabeth I para recuperar el reinado en Escocia, conspirando para ello con Anthony Babington. La correspondencia entre María y Anthony se realiza mediante textos cifrados por sustitución. En la siguiente imagen podemos ver uno de estos textos.

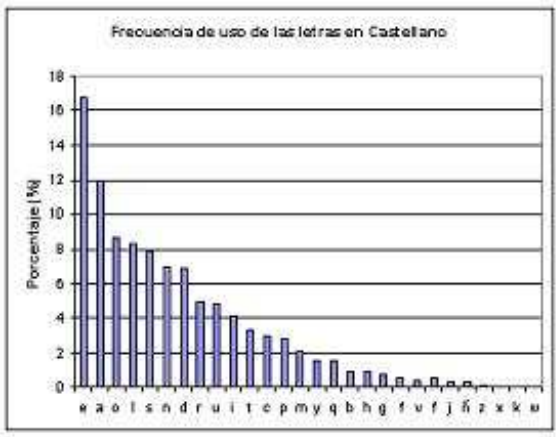


A continuación tenemos su *nomenclátor* (catálogo de nombres). Naturalmente, este tipo de diccionario tenía que poseerlo tanto el que cifraba, como el que descifraba los mensajes.



Estos métodos de sustitución fueron criptoanalizados con el denominado *Análisis de frecuencias*. Si observamos un texto escrito en castellano, en

seguida nos daremos cuenta de que la letra que más aparece es la *e*. Podemos contar el número total de letras y mirar cuál es la proporción de cada una de las letras del alfabeto, es decir, con qué frecuencia aparece cada letra. Por ejemplo, a continuación se muestra una lista de las frecuencias con que cada letra del alfabeto aparece en castellano.



Si se intenta ocultar cada letra sustituyéndola por otra (cifrado por sustitución), aún se pueden reconocer las letras originales, ya que las características frecuenciales de las letras originales pasan directamente a las nuevas. Así, si en un texto castellano cifrado , la letra que más aparece es la *u*, podemos pensar que la *u* está sustituyendo a la *e*.

La debilidad de este método de sustitución tuvo consecuencias terribles para María Estuardo: fue ejecutada en 1587.

Como último ejemplo de una mujer que cifraba mensajes con un método de los llamados clásicos, podemos citar a la conocida actriz **Hedy Lamarr** (1913-2000).

Obligada a casarse con un militar nazi, éste no la dejaba salir de casa y la obligó a dejar su incipiente carrera de actriz. Hedy Lamarr, en aquel entonces Hedwig Eva Maria Kiesler, aprovechó el encierro para terminar sus estudios de ingeniería. Consiguió escapar de su marido saltando por la ventana del cuarto de baño de un restaurante. De ahí huyó a París, Londres y finalmente a Hollywood, donde reemprendió su carrera de actriz bajo la protección del cineasta Louis Mayer. Debido al resentimiento que profesaba por el régimen nazi se puso a trabajar en nuevas tecnologías militares. Los diferentes gobiernos de la época eran reacios a la utilización de misiles teledirigidos, por miedo a que las señales de control fueran interceptadas por el enemigo. Hedy Lamarr y G. Antheil diseñaron un sistema de comunicaciones secreto. Este sistema (pionero de la modulación de señales en espectro extendido) usaba un par de tambores perforados y sincronizados para cambiar entre 88 frecuencias y se usó para construir torpedos teledirigidos por radio imposibles de detectar por los enemigos.

A lo largo del siglo XX se va efectuando el cambio del lápiz y papel a la máquina. Así llegamos a la máquina Enigma utilizada en la Segunda Guerra mundial.

La máquina Enigma funciona como una máquina de escribir, pero cada vez que se teclea una letra, debido al funcionamiento interno de cables y rotores, se ilumina otra letra que corresponderá al cifrado de la tecleada.

Para que el receptor del mensaje pueda descifrarlo es necesario que conozca la disposición de la máquina. Así, como en los ejemplos anteriores, es necesaria la existencia de un libro de claves para ser utilizado por el emisor y el receptor. Además, para aumentar la seguridad, las claves deben cambiarse a menudo.

En este momento debemos mencionar a **Mavis Lever**. En 1940 en Bletchley Park había un grupo de criptoanalistas ingleses dirigido por D. Knox que realizaba trabajos para romper cifrados alemanes durante la Segunda Guerra Mundial. Su conciencia y su sentido del deber (ya mostrados durante la guerra civil española) hicieron que M.Lever se presentase como enfermera al estallar la guerra, sin embargo sus conocimientos de alemán y sus habilidades hicieron que fuera enviada al equipo de Knox. Se cuenta que Knox elegía a sus trabajadores entre las chicas más guapas de Bletchley, lo que sí es cierto es que su grupo estaba formado por chicas conocidas como las "chicas Dilly".

Uno de los métodos utilizados para descifrar los mensajes alemanes cifrados con Enigma, era intentar imaginar qué cuatro letras había usado el operador de radio alemán como clave de cifrado. Por suerte para los criptoanalistas de Bletchley Park, las claves alemanas no eran generadas de forma aleatoria. En palabras de la propia M.Lever "soy la experta mundial en tacos alemanes de cuatro letras".

Otra hazaña de Mavis fue la siguiente: un texto cifrado no contenía ninguna L y como las máquinas Enigma no son recíprocas, una letra nunca se transforma en sí misma al cifrarla, así dedujo que el mensaje en claro estaba constituido únicamente por la letra L y se había emitido para engañar al enemigo. Los logros obtenidos por las chicas de Knox son de una extraordinaria lucidez.

Para saber más sobre Mavis Lever y sobre la máquina Enigma se puede recurrir al Boletín Enigma, una publicación mensual del profesor A.Quirantes de la Universidad de Granada [1].

2. Criptografía de clave pública

El nacimiento de la criptografía científica se suele fechar en 1948 con el artículo de Shannon sobre la *Teoría de la Información y la Comunicación Secreta* [9]. En este artículo se formulan en términos matemáticos conceptos como *seguridad incondicional*, *secreto perfecto*, ... Aunque las limitaciones de la criptografía de clave privada quedaban claras, durante mucho tiempo, los únicos métodos de cifrado que se utilizan son los simétricos. El emisor y

el receptor deben acordar a priori cuál es la clave con la que se van a cifrar y descifrar los mensajes.

Hay que esperar hasta 1976 para el nacimiento de la *criptografía de clave pública* o asimétrica. W.Diffie y M.Hellman sentaron las bases de la criptografía moderna en su artículo "*New directions in Cryptography*" [4]. En la criptografía de clave pública cada usuario tiene un par de claves, una pública y otra privada. La clave pública se deposita en una especie de listín telefónico al que todo el mundo puede acceder y la clave privada se mantiene en secreto, la pública servirá para cifrar los mensajes y la privada para descifrarlos. Se puede pensar en un buzón en el que cualquiera puede dejar un mensaje que sólo puede ser leído por el poseedor de la llave.

El modelo matemático en el que se basa la criptografía de clave pública es el de las *funciones unidireccionales con trampa* (one-way trapdoor functions), funciones fáciles de calcular pero cuya inversa es difícil de obtener salvo que se tenga una cierta información adicional (la trampa). Pero ¿cuál es el significado de "difícil"?, es decir, ¿qué tipo de problemas son "difíciles" de resolver? Una definición simple de problema difícil es aquel para el que no se conoce ningún algoritmo que en un tiempo razonable nos dé la solución.

2.1. Criptosistema de M.O.Rabin

Uno de los problemas de esta categoría es el de la extracción de raíces cuadradas en Z_n, que dio lugar al criptosistema de Rabin (Breslau, Alemania (ahora Wroclaw, Polonia), 1931) [7]. Veamos este problema con un poco más de detalle y el correspondiente método de cifrado.

El conjunto Z_n, enteros módulo n, se puede representar como $Z_n = \{0, 1, 2, \ldots, n-1\}$. Así, $Z_6 = \{0, 1, 2, 3, 4, 5\}$. Las operaciones modulares (operaciones en Z_n) se realizan como en los enteros, es decir, $3 + 4 = 7$ y $4 * 4 = 16$, sin embargo, para que el resultado de la operación siga dentro del conjunto, a veces hay que realizar una operación adicional y es restar al resultado obtenido tantas veces n como sea necesario, para obtener un valor entre 0 y $n - 1$. Así por ejemplo $3 + 4 = 1(= 7 - 6)$ y $4 * 4 = 4(= 16 - 2 * 6)$ en módulo 6.

Antes de explicar el criptosistema de Rabin es conveniente aclarar el concepto de raíces cuadradas en operaciones modulares. Se dice que la raíz de un número es aquel que multiplicado por sí mismo, da ese número. Pues bien, en aritmética modular, esto sigue siendo así. Pero claro, un número al cuadrado en módulo n puede ser mayor que n, por lo que al hacer módulo, se reduce

su valor. Por lo tanto, un mismo número puede tener varias raíces. En los reales, un número tiene 2 raíces reales (la positiva y la negativa), pero cuando n es por ejemplo el producto de 2 primos, existen valores que tienen 4 raíces distintas módulo n. Por ejemplo, en Z_{15} se tiene que $1^2 = 4^2 = 11^2 = 14^2 = 1$.

La función elevar al cuadrado en Z_n, siendo n producto de dos primos de especiales características (por ejemplo, han de ser de gran tamaño), pertenece a la categoría de funciones unidireccionales con trampa. Es una función fácil de calcular (multiplicar el número por sí mismo), pero difícil de invertir. Esto se debe a que la extracción de raíces cuadradas módulo n es difícil salvo que se conozca la factorización de n (la trampa).

Veamos el funcionamiento del criptosistema de Rabin.

Cada usuario elige una pareja de primos p y q, cada uno igual a 3 módulo 4, y forma el producto $n = p * q$. La clave pública del usuario será n y su clave privada p y q. Para cifrar un mensaje m se eleva al cuadrado módulo la clave pública del destinatario, $c = m^2 \mod n$. Dado un texto cifrado c, se calculan las 4 raíces cuadradas de c módulo n. Una de ellas será el propio m.

Si los primos p y q son iguales a 3 módulo 4 existen fórmulas sencillas para hallar las raíces (usando p y q). En efecto, primero se hallan los valores a y b que satisfacen la ecuación $a * p + b * q = 1$ y luego $s = c^{(q+1)/4} \mod q$ y $r = c^{(p+1)/4} \mod p$. Entonces los valores $x = (a * p * s + b * q * r) \mod n$, $y = (a * p * s - b * q * r) \mod n$ dan lugar a las 4 raíces, que serán $\pm x$, $\pm y$. Para distinguir el m que codifica el mensaje de las otras raíces, será necesario incluir información redundante.

Quien quiera descifrar el mensaje sin conocer la clave privada, es decir el valor de p y q, lo tiene bastante difícil, ya que los métodos más eficientes que se conocen en la actualidad para extraer raíces cuadradas utilizan un tiempo equivalente al que se necesitaría por prueba y error, es decir, ir elevando al cuadrado los sucesivos números $1, 2, 3, \ldots$ y ver cuál coincide con el que se tiene.

3. Tal Rabin

Ahora es el momento de presentar a una de las mujeres de más importancia en la criptografía moderna: se trata de **Tal Rabin** (Israel, 1962), hija de M.O. Rabin.

Es la directora del *Cryptography and Privacy Research Group* en el centro de investigación de IBM. Su currículo es muy amplio y tiene grandes trabajos en diversos campos dentro del área de la criptografía. Uno de los más destacados es el diseño de protocolos distribuidos para, por ejemplo, la firma digital, donde se trata de generar una firma electrónica entre un colectivo de usuarios.

Veremos la firma presentada por Tal Rabin en su artículo titulado *Robust and efficient sharing of RSA functions* de 1996 [5]. Este artículo muestra un esquema de firma digital distribuida, obtenida a partir del criptosistema RSA [8]. Antes de entrar en más o menos detalle en el esquema de firma expliquemos brevemente cuáles son los conceptos necesarios para su comprensión.

El método de cifrado RSA (iniciales de sus autores Rivest, Shamir y Addleman), fue el primer criptosistema de clave pública propuesto (1978). Se basa en la dificultad de factorizar un número entero grande (como el mencionado criptosistema de Rabin). En este caso también se trabaja en Z_n siendo n el producto de dos primos grandes p y q que se mantendrán en secreto, ahora la función que se utiliza para el cifrado no es elevar al cuadrado sino elevar a una potencia e que formará parte de la clave pública del usuario y cuyo único requisito es que no tenga factores en común con $(p-1)(q-1)$. Gracias a este requisito, existirá un número d satisfaciendo $ed = 1 \mod (p-1)(q-1)$ y por el Teorema de Fermat, cualquier número x verificará que $x^{ed} = x \mod n$. En la actualidad, el único método que se conoce para calcular este valor d, a partir de n y e, utiliza la factorización de n.

El concepto de firma digital de mensajes se puede entender como un método electrónico que garantiza la identidad del remitente del mensaje. Es decir, el emisor ha de mostrar el resultado de alguna operación que sólo él

puede haber realizado correctamente. Por ejemplo, usando el criptosistema RSA el usuario que ha hecho públicas n y e es el único que conoce d y, por tanto, el único que puede calcular $x^d \mod n$ para un x fijado. Así, este valor serviría como firma digital del mensaje x. Cualquiera puede verificar la validez de la firma elevando a e, que es público, y viendo que así se recupera el mensaje que está firmado, esto es, $(x^d)^e = x \mod n$.

Por último, qué significa *firma digital distribuida*. En este caso se supone que hay un grupo de usuarios que de alguna forma comparten la información secreta d asociada a la clave pública n, e (sin que ninguno conozca el valor de d). De esta forma se asegura que es necesaria la colaboración de un subgrupo de usuarios para firmar cualquier mensaje. En criptografía se usa el término *esquemas para compartir secretos* para designar este tipo de situaciones.

El esquema de compartición de secretos más conocido se debe a Shamir (el mismo del RSA) que lo propuso en 1979 [10]. Es un esquema para compartir secretos de umbral. El término *umbral* hace referencia al hecho de que el número de usuarios que debe unirse para recuperar el secreto debe superar un cierto umbral. La técnica propuesta por Shamir se basa en que un polinomio de grado $t-1$ está determinado por sus t coeficientes $p(z) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1}$, por tanto a partir del conocimiento de t valores $p(z_i) = y_i$ puede obtenerse dicho polinomio y por tanto cualquier otro valor $p(z)$, en particular el valor $p(0) = a_0$. Por otra parte si sólo se conocen menos de t valores, hay muchos polinomios de grado $t-1$ que toman esos valores y, en particular, muchos valores distintos en el punto 0 (término independiente) que son coherentes con esos menos de t valores.

Ahora que sabemos estos conceptos veamos cuál es el esquema de firma distribuida presentado por T. Rabin y sus colegas.

Un usuario especial denominado *repartidor* genera unas claves RSA, recordemos, clave pública $n(= pq), e$ y clave privada p, q, d. Mediante el esquema de Shamir obtiene los *fragmentos* de la clave d, generando un polinomio $P(z) = d + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1}$ y repartiendo a cada usuario P_i el valor $d_i = P(z_i)$ (los valores z_i son asociados a los participantes al inicio del protocolo). Llegado el momento de la firma colectiva de un mensaje m, cada usuario genera su firma parcial $m^{d_i} \mod n$. La firma total m^d se puede obtener a partir de al menos t valores de esas firmas parciales mediante una fórmula:

$$m^d = m^{P(0)} = m^{\sum_{i=0}^{t-1} \lambda_i d_i} = \prod_{i=0}^{t-1} m^{d_i \lambda_i} \mod n$$

donde los valores λ_i son los coeficientes de interpolación de Lagrange.

4. Lenore Blum

Si bien la hija de Rabin usó la función RSA y no la de Rabin, otra matemática **Lenore Blum** (Nueva York, 1943), usó la dificultad de la raíz cuadrada para, en 1984 diseñar con su marido Manuel Blum y un colega M. Shub, un generador de números pseudoaleatorios [2], el BBS.

L.Blum con el protagonista de la serie Numb3rs

De nuevo consideramos n un módulo RSA $n = pq$ con p y q primos grandes iguales a 3 módulo 4. A partir de un valor inicial, *semilla*, x_0, se calculan iterativamente los valores $x_{i+1} = x_i^2 \mod n$. En cada paso se toma como bit aleatorio, el bit que indica la paridad de x_i, es decir un valor par da lugar al bit 0 y un valor impar al bit 1.

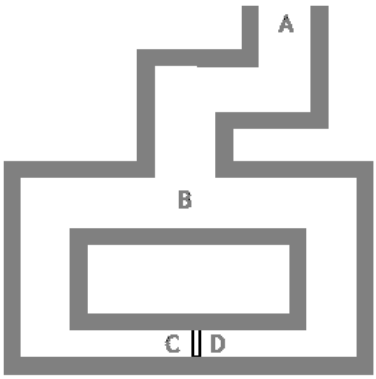
Por ejemplo, para $p = 11$ y $q = 19$ con semilla 5 se obtiene la secuencia de números 25, 207, 4, 16, 47, 119, 158, 93, ..., que da lugar a la secuencia de bits 11001101. Si los primos son elegidos adecuadamente la secuencia de bits así obtenida es indistinguible de una secuencia realmente aleatoria, como la que se obtendría lanzando una moneda y poniendo 0 o 1 según saliera cara o cruz, respectivamente.

L.Blum es bien conocida por su activa participación en la Asociación de mujeres matemáticas, ha escrito un libro titulado Women and numbers y es madre de Avrim Blum, profesor de Computer Science en Carnegie Mellon.

5. Shafi Goldwasser

Para el final he dejado a la que se considera una de los fundadores de la criptografía moderna, **Shafi Goldwasser** (Nueva York, 1958).

Shafi Goldwasser es codirectora del *Cryptography and Information Security Group* en el MIT. Es difícil hacer una pequeña biografía que dé idea de sus contribuciones al mundo de la criptografía actual, pero podríamos destacar que es co-inventora de las *Zero-Knowledge Proof*, demostraciones de conocimiento cero: una persona trata de demostrar a otra que sabe algo, sin enseñarle o transmitirle ese algo. En 1989 J.J.Quisquater y otros colegas en su artículo "*How to explain zero knowledge proof to your children*" muestran esa idea mediante un ejemplo muy sencillo. Veámoslo.



Peggy quiere demostrar a Victor que sabe las palabras secretas (clave) para abrir una puerta mágica de una cueva (problema, criptosistema), sin decir esas palabras delante de Victor (sin enseñarle la clave).

La manera es la siguiente:

- Victor empieza en el punto A
- Peggy entra en la cueva y llega a la puerta, por el lado C o por el D (es igual)
- Cuando ya no ve a Peggy, Victor va hacia el punto B
- Victor avisa a Peggy de que va a llegar al lado C (o D).
- Si Peggy está en ese lado le espera, si no, usa las palabras mágicas para abrir la puerta y volverla a cerrar, apareciendo en el lado correcto.
- Victor llega a la puerta C (o D) y encuentra a Peggy, y también comprueba que la puerta está cerrada.

Si este protocolo («demostración») se realizara sólo una vez, Victor pensaría que Peggy ha tenido suerte. Así que se repiten todos los pasos tantas veces como se quiera. Por tanto Peggy ha demostrado a Victor que sabe las palabras mágicas para abrir la puerta sin revelárselas.

S. Goldwasser ha recibido el *Gödel Prize* en dos ocasiones una en 1993 y otra en 2001. En 1984 diseñó con Manuel Blum (esposo de Lenore) un criptosistema que usa el generador de BBS para generar la clave [3].

Veamos el funcionamiento del método de cifrado. De nuevo las claves son tipo RSA, la pública es n y la secreta p, q primos de gran tamaño e iguales a 3 módulo 4, tales que $n = pq$. Para cifrar un mensaje m, primero se codifica como una secuencia de L bits $m = m_0 m_1 \cdots m_{L-1}$. Ahora, se toma como semilla un valor aleatorio r, $1 < r < n$ y con él se genera la secuencia de L bits $b = b_0 b_1 \cdots b_{L-1}$ tal como se ha explicado en el generador BBS. Finalmente, el texto cifrado se obtiene como $c = m \oplus b$, $y = r^{2^L} \mod n$.

Para descifrar el mensaje, lo primero que hace el receptor legítimo es buscar la semilla r, ya que con ella podrá obtener la secuencia de bits b (como hiciera el cifrador) y obtener el mensaje como $m = c \oplus b$. Sin entrar en demasiado detalle, el receptor conoce p y q y del conocimiento de y obtiene r de forma muy similar a como sacábamos raíces cuadradas en el sistema de Rabin.

Para acabar nada mejor que las palabras de **Carolina Herschel** (1750-1848) la primera mujer que descubrió un cometa.

"*Sometimes when I am alone in the dark, and the universe reveals yet another secret, I say the names of my long lost sisters, forgotten in the books that record our science- Aglaonice of Thessaly, Hypatia, Hildegard, Catherine Hevelius, Maria Agnesi -as if the stars themselves could remember ...*"

Referencias

[1] A.Quirantes. Boletin Enigma. `http://www.cripto.es/` .

[2] L.Blum, M.Blum y M.Shub. A Simple Unpredictable Pseudo-Random Number Generator. *SIAM Journal on Computing*, vol 15, pp. 364-383 (1986).

[3] M.Blum y S. Goldwasser. An Efficient Probabilistic Public Key Encryption Scheme which Hides All Partial Information. *CRYPTO'84*, pp. 289-299 (1985).

[4] W. Diffie y M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, vol IT-22, pp. 644-654 (1976).

[5] R.Gennaro, S.Jarecki, H.Krawczyk and T.Rabin. Robust and Efficient Sharing of RSA Functions. *CRYPTO'96*, pp. 157-172 (1996).

[6] J.J.Quisquater, L.C.Guillou y T.A.Berson. How to Explain Zero-Knowledge Protocols to Your Children. *CRYPTO'89*, pp. 628-631 (1989).

[7] M.O.Rabin, Digitalized signatures and public key functions as intracable as factorization. *MIT/LCS/*, vol 212, (1979).

[8] R.L.Rivest, A.Shamir y L.Addleman, A method for obtaining digital signatures and public-key cryptosystem. *Comm. ACM*, vol 21, pp. 120-126 (1978).

[9] C.Shanon. A Mathematical Theory of Communication. *Bell System Technical Journal*, vol 27, pp. 379-423, 623-656 (1948).

[10] A.Shamir. How to share a secret. *Comm. ACM*, , vol 22, pp. 612-613 (1979).

[11] S.Singh. The code book. *Madrid. Debate Editorial*, (1999).