

(12) SOLICITUD INTERNACIONAL PUBLICADA EN VIRTUD DEL TRATADO DE COOPERACIÓN EN MATERIA DE PATENTES (PCT)

(19) Organización Mundial de la
Propiedad Intelectual
Oficina internacional



(10) Número de Publicación Internacional
WO 2012/152956 A1

(43) Fecha de publicación internacional
15 de noviembre de 2012 (15.11.2012) **WIPO | PCT**

- (51) Clasificación Internacional de Patentes:
H04L 9/06 (2006.01)
- (21) Número de la solicitud internacional:
PCT/ES2011/070331
- (22) Fecha de presentación internacional:
9 de mayo de 2011 (09.05.2011)
- (25) Idioma de presentación: español
- (26) Idioma de publicación: español
- (71) Solicitantes (*para todos los Estados designados salvo US*):
PÉREZ I GIL, Antoni [ES/ES]; C/ Gravador Selma, 5º -11, E-46001 Valencia (ES). **PONS GRAU, Vicent** [ES/ES]; Polo y Peyrolón, 6 12ª, E-46021 Valencia (ES). **SOLA PALERM, Enrique** [ES/ES]; Passeig de l'Albereda, 12 - 2ª, E-46010 Valencia (ES).
- (72) Inventor; e
- (71) Solicitante : **MARTINEZ SANCHO, Vicent** [ES/ES]; C/ Ribera 19 - 1ª, E-46002 Valencia (ES).
- (74) Mandatario: **CHANZA JORDAN, Dionisio**; Pza Alfonso El Magnanimo, 13, E-46003 Valencia (ES).
- (81) Estados designados (*a menos que se indique otra cosa, para toda clase de protección nacional admisible*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) Estados designados (*a menos que se indique otra cosa, para toda clase de protección regional admisible*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), euroasiática (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europea (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- Publicada:
— con informe de búsqueda internacional (Art. 21(3))

(54) Title: SHANNON SECURITY DOUBLE SYMMETRICAL CRYPTOGRAM METHOD BY CODING INFORMATION FOR TELEMATIC AND ELECTRONIC TRANSMISSION

(54) Título : PROCEDIMIENTO DE DOBLE CRIPTOGRAMA SIMETRICO DE SEGURIDAD DE SHANNON POR CODIFICACION DE INFORMACION PARA TRANSMISION TELEMATICA Y ELECTRONICA.

(57) Abstract: An invention in the field of information society for making data and information inaccessible to unauthorized persons in order to protect the privacy of data and information during electronic transmission using a cryptographic method for reliable, fast and secure encryption widely used in industry (private and public telecommunications sectors, computing, national defence, computer programs, electronic payment transactions and banking operations, cryptography of musical and audiovisual works and digital signatures and certificates) by means of the use of the following technical means in sequential and successive order: 1. an alphanumeric matrix, 2. a numerical remainder base matrix, 3. an equivalence key, 4. an equivalence table, 5. a reduced remainder or template cryptogram, 6. a protocol key, 7. a coding algorithm, 8. a final remainder cryptogram and 9. a decoding algorithm.

(57) Resumen: Una invención en el ámbito de la sociedad de la información para dotar una inaccesibilidad de los datos y de información frente a personas no autorizadas para proteger la privacidad en la transmisión electrónica de datos e información mediante un procedimiento de criptografía para un cifrado fiable, rápido y seguro de amplia aplicación industrial (sectores privados y públicos de las telecomunicaciones, informática, Defensa nacional, programas de ordenador, transacciones de pagos electrónicos y operaciones bancarias, criptografía de obras musicales y audiovisuales, y firmas y certificados digitales) mediante el empleo de medios técnicos por orden secuencial y sucesivo de: 1º. Una matriz alfanumérica, 2º. una matriz base de residuos numéricos, 3º. una clave de equivalencias, 4º. una tabla de equivalencias, 5º. un criptograma reducido de residuos o plantilla, 6º. una clave de protocolo, 7º. un algoritmo de codificación, 8º. un criptograma final de residuos y 9º. un algoritmo de decodificación.



WO 2012/152956 A1

PROCEDIMIENTO DE DOBLE CRIPTOGRAMA SIMETRICO DE SEGURIDAD DE SHANNON POR CODIFICACION DE INFORMACION PARA TRANSMISION TELEMATICA Y ELECTRONICA.

5

DESCRIPCION

Sector técnico

10

La invención que se protege en esta patente, consiste en un procedimiento criptográfico simétrico en el que el *texto claro* se cifra y el *criptograma final* se descifra, mediante la aplicación sucesiva de dos claves consecutivas que denominamos *la clave de equivalencias* y *la clave de protocolo*, cada una de las cuales ya proporciona en el proceso de cifrado un *Criptograma Seguro de Shannon*, en el que además también están presentes las otras dos condiciones de Shannon, la *Confusión* y la *Difusión*. Con esto se consigue una total ininteligibilidad e inescrutabilidad en la información transmitida.

20

Con ello se obtiene un tratamiento y una transmisión de datos o informaciones cifradas fiables, rápidas y seguras de amplia aplicación industrial en los sectores privados y públicos de las telecomunicaciones, informática, Defensa nacional, y en particular en programas de ordenador o softwares, transacciones de pagos electrónicos y operaciones bancarias, criptografía de 25 obras musicales y audiovisuales, y firmas y certificados digitales.

30

En resumen, en la sociedad de la información se demanda y requiere de un incremento de los usos y aplicaciones de la criptografía en aras de dotar una inaccesibilidad de los datos y de información a personas no autorizadas con la finalidad de proteger la privacidad.

Técnica anterior

La transmisión de información confidencial entre dos interlocutores, dos
5 instituciones, dos organismos, etc., es, desde siempre, una de las cuestiones
que exige un mayor esfuerzo para resolver un aspecto principal sin el cual
dicha información deja de ser segura: el cifrado del mensaje ha de ser
inescrutable para que en el supuesto que dicho mensaje sea interceptado por
un tercero, éste no pueda descifrar su contenido.

10

Esta cuestión es, por lo tanto, de suma importancia tanto en el mundo
financiero como en el comercial y, desde luego, también en la protección de
datos por los organismos estatales. Actualmente hay diversos lenguajes de
cifrado cada uno de los cuales suele agruparse en una de las siguientes dos
15 grandes familias, o bien como *sistema de cifrado simétrico* o bien como *sistema
de cifrado asimétrico*. Este último es muy seguro, pero no por eso resulta
imposible romperlo por el procedimiento llamado *fuerza bruta* con procesadores
cada vez más potentes que, con tiempo suficiente, acaban averiguando los
números primos a partir de cuyo producto se ha construido el criptograma. Y no
20 es nada fácil descubrir y almacenar números primos suficientemente grandes.
Por lo que respecta a los sistema de cifrado simétrico, uno de los lenguajes
más solventes continua siendo el llamado *algoritmo DES, Data Encryption
Standard*. En su procedimiento más simple el algoritmo DES consta de 2^{56}
claves, lo que significa que si se dispone de un ordenador capaz de realizar un
25 millón de operaciones por segundo, se tardarían más de 2200 años en probar
todas las claves. A pesar de eso, actualmente se recomienda que la clave
tenga 128 bits, con lo cual el ordenador anterior necesitaría de 10^{24} años para
agotar todas las posibilidades.

30

El sistema de cifrado que aquí presentamos es de la clase simétrica.
Como se verá es muy fácil de manejar. Además, su versatilidad le convierte en
inexpugnable incluso para ordenadores de potencia de cálculo muy superior a
la de los actuales e incluso, sin ningún género de duda, para el ordenador del

futuro. Como expondremos más adelante, los 10^{24} años que requiere el DES con clave de 128 bits, resulta un intervalo a todos los efectos prácticos infinitesimal comparado con el tiempo que el mismo ordenador necesitaría para probar todas las posibilidades de codificar un texto con nuestro sistema, a
5 pesar de que proporcionemos parcialmente información tanto de las que denominamos *clave de equivalencias* como de la *clave de protocolo* que usemos para la codificación de nuestro mensaje.

La resistencia de los criptogramas actuales al ataque de un extraño se
10 fundamenta, por una parte, en el cumplimiento de las dos condiciones de Shannon, *Confusión* y *Difusión*, y, por otra, en la consecución de un proceso cifrador que tienda al proceso ideal llamado *Criptograma Seguro de Shannon*. Claude E. Shannon es considerado el padre de la criptografía matemática. En sus dos trabajos principales: *A Mathematical Theory of Communication* (C. E.
15 SHANNON: *A Mathematical Theory Communication, The Bell System Technical Journal, Vol. 27, pp. 379-423, 623-656, July, October, 1948*) y *Communication Theory of Secrecy Systems* (C. E. SHANNON: *Communication Theory of Secrecy Systems, The Bell System Technical Journal, Vol. 28-4, pp. 656-715, 1949*), se establece una sólida base teórica tanto para la criptografía
20 como para el criptoanálisis. Todos los lenguajes de cifrado ideados hasta la fecha combinan las dos condiciones expuestas por Claude Shannon en sus estudios criptográficos: La *Confusión* que trata de ocultar la relación entre el texto claro y el texto cifrado mediante, por ejemplo, sustituciones y la *Difusión* que diluye la redundancia del texto claro repartiéndola a lo largo del texto
25 cifrado mediante, por ejemplo, transposiciones. Asimismo, todos estos lenguajes tienden a formularse teniendo como objetivo el *Criptograma Seguro de Shannon*, que comentamos a continuación.

Un Criptograma Seguro de Shannon es aquél en que se verifica que la
30 cardinalidad del espacio de claves es igual o mayor que la cardinalidad del espacio de mensajes. Este criterio es equivalente a decir que un criptograma es *seguro* si la cantidad de información que aporta el hecho de conocer el

mensaje cifrado sobre la *entropía* del texto claro vale cero. O dicho en otras palabras: cuando el conocimiento de cualesquiera textos cifrados correspondientes a unos determinados textos claros no aporta *ninguna* información sobre otros criptogramas cuyo texto claro deseamos averiguar, podemos decir que ese lenguaje criptográfico verifica la condición de Criptograma Seguro de Shannon. A continuación exponemos la situación actual y luego la compararemos con nuestra *Criptografía de Residuos*.

Si consideramos todos los textos claros posibles de un determinado idioma hemos de concluir que dicho número es infinito. Si nos limitamos a las frases con sentido literario, es decir, inteligibles para cualquier persona con formación lingüística suficiente, dicho número continúa siendo infinito, pero, no obstante, es posible ordenarlo asociando a cada frase un número natural. Esto nos indica que *la cardinalidad del espacio de los mensajes es Aleph-0*. Teniendo esto en cuenta señalaremos algunas cualidades de los criptogramas actuales, tanto de aquellas que se encuentran dentro de la llamada *Criptografía asimétrica* como aquellas que son características de la *Criptografía simétrica*.

Todos los *algoritmos de cifrado asimétrico* se basan en el trabajo publicado por *Whitfield Diffie* y *Martin Hellman: New Directions in Cryptography (IEEE Transactions on Information Theory 22, año 1976; pp. 644-654)*. En todos ellos: RSA, Diffie-Hellman, ElGamal, Rabin, DSA, etc., es obvio que se hace uso de la condición de *Confusión de Shannon* y, además, también todos ellos satisfacen la condición de *Criptograma Seguro de Shannon*, ya que el conjunto de los números primos consta de infinitos elementos. Pero, no obstante, presentan un inconveniente que repercute en consecuencias prácticas peligrosas para la seguridad del mensaje transmitido: Si bien el espacio de las claves (privada y pública) es Aleph-0, ya que el espacio de los números primos es Aleph-0, por lo que *estamos ante un Criptograma Seguro de Shannon*, tenemos el inconveniente insuperable de que no podemos generar números primos mediante una expresión matemática. Por lo cual, si bien disponemos de una cantidad infinita de números primos, tan sólo

conocemos una porción finita de ellos. De este conjunto de números primos conocidos o que conoceremos, siempre en cantidad finita, hay unos, los números primos pequeños que determinan claves cortas, o si se quiere débiles, fáciles de reventar y, por otra, los excesivamente grandes que conforman claves tan largas que convierten el proceso de cifrado en poco manejable por la lentitud con que se realiza. Por ejemplo, mientras que para algoritmos simétricos se considera segura una clave de 128 bits, para algoritmos asimétricos se recomiendan claves de no menos de 2048 bits, pero esto trae aparejado que estos cifradores tengan una velocidad de cifrado del orden de mil veces inferior a los primeros. Además la conjunción de muchos ordenadores muy potentes puede romper claves asimétricas, consideradas largas, en poco tiempo.

Respecto de la criptografía simétrica hemos de hacer las siguientes consideraciones:

A). En primer lugar, una gran parte de los *algoritmos de cifrado simétrico* dividen el mensaje que se desea codificar en bloques de tamaño fijo y aplican sobre cada uno de ellos una serie de operaciones de confusión por sustitución y de difusión, generalmente, por transposición. Estos algoritmos suelen englobarse bajo el nombre de *cifrados por bloques*. La mayoría de éstos intercalan las operaciones de confusión y de difusión mediante una combinación que se conoce como *cifrado de producto* que da lugar a una estructura que se denomina *Red de Sustitución-Permutación* o *Substitution-Permutation network* (verbigracia, MANUEL JOSÉ LUCENA LÓPEZ: *Criptografía y seguridad en computadores*, pág. 141, Versión 4-0.7.53, 8 de marzo 2009, Universidad de Jaén). Otra estructura, similar a la anterior, y muy aceptada es la llamada *Red de Feistel* (*The Feistel Network*) que empleada en muchos algoritmos, como DES, Lucifer, FEAL, CAST, Blowfish, etc. fue introducida por *Horst Feistel* en su artículo *Cryptography and Computer Privacy* (*Scientific American*, Vol. 228, No. 5, 1973.). Pues bien, todos los cifrados por bloques trabajan con cadenas fijas de n bits a las que se aplican

alternativamente procesos de sustitución en las llamadas S-cajas (S-boxes) y de permutación en las P-cajas (P-boxes). El hecho de que los bits empleados sean los asociados al código ASCII o a cualquiera de sus variantes, determina que el espacio de las claves que pueda ser utilizado sea siempre de cardinalidad finita. *En consecuencia, ningún cifrado simétrico por bloques da lugar a Criptogramas Seguros de Shannon.* Esta es la razón por la cual el conocimiento del texto cifrado asociado a un texto claro da lugar a informaciones que pueden conducir al rompimiento del sistema.

10 B). El algoritmo IDEA (*Internacional Data Encryption Algorithm*) es un cifrador por bloques diseñado por XUEJIA LAI y JAMES L. MASSEY de la Escuela Politécnica Federal de Zúrich que fue descrito por primera vez en 1991 (X. Lai, J. L. Massey and S. Murphy: *Markov ciphers and differential cryptanalysis*, Advances in Cryptology – Eurocrypt '91, Springer-Verlag, 1992, pp. 17-38). Como ocurre con los otros algoritmos de cifrado por bloques, IDEA se basa en los conceptos de confusión y difusión de Shannon. Aunque presenta diferencias notables con los anteriores cifradores, por ejemplo con DES (Ver, por ejemplo, MANUEL JOSÉ LUCENA LÓPEZ: *Criptografía y seguridad en computadores*, pág. 150, Versión 4-0.7.53, 8 de marzo 2009, Universidad de Jaén), tampoco es un Criptograma Seguro de Shannon, ya que su espacio de claves, aunque muy grande: $2^{128} \approx 3.4 \times 10^{38}$, es de cardinalidad finita.

25 C). El AES (*Advanced Encryption Standard*) o *Algoritmo Rijndael*, nombre este último que es un acrónimo de sus dos autores (Joan Daemen and Vincent Rijmen: *The Design of Rijndael: AES – The Advanced Encryption Standard*, Springer-Verlag, 2002), es otro sistema de cifrado por bloques, diseñado para manejar longitudes de clave y de bloque variables, ambas comprendidas entre los 128 y los 256 bits. El AES no posee estructura de red de Feistel. Aunque este cifrador realiza varias de sus operaciones internas a nivel de byte, interpretando éstos como elementos de un cuerpo de Galois $GF(2^8)$, el AES continua teniendo asociado un espacio de claves de

30

cardinalidad finita. Por lo tanto, el AES no es un Criptograma Seguro de Shannon.

D). En último lugar consideraremos los llamados *Cifrados de Flujo*. La característica general de estos algoritmos es el uso “de un generador pseudoaleatorio que permite cifrar mensajes de longitud arbitraria combinando el mensaje con la secuencia mediante una operación *or exclusivo byte a byte*, en lugar de dividirlos en bloques para codificarlos por separado” (MANUEL JOSÉ LUCENA LÓPEZ: *Criptografía y seguridad en computadores*, pág. 167, Versión 4-0.7.53, 8 de marzo 2009, Universidad de Jaén). Para la exposición que aquí estamos haciendo solo nos interesa añadir que ninguno de estos cifradores es un Criptograma Seguro de Shannon, ya que cuando se emplea un generador tenemos, como mucho, tantas secuencias distintas como posibles valores iniciales de la semilla, lo que significa que el espacio de las claves siempre es de cardinalidad inferior al de los mensajes.

La relación de los algoritmos y protocolos criptográficos más usuales considerados como estándares y que, por tanto, pueden considerarse como acreditados, a modo ilustrativo y no limitativo, es la siguiente:

20

a. TDEA (Triple Data Encryption Algorithm, Triple Algoritmo de Cifrado de Datos): SP 800-20, SP800-38B y SP 800-67 del NIST ([NIST, SP800-20], [NIST, SP800-38B], [NIST, SP800-67]).

25

b. AES (Advanced Data Encryption, Cifrado de Datos Avanzado): FIPS 197 y SP800-38B del NIST ([NIST, FIPS197], [NIST, SP800-38B]) y la Suite B de la NSA ([NSA, SuiteB]).

30

c. DH o DHKA (Diffie-Hellman Key Agreement, Acuerdo de Clave de Diffie-Hellman): ANSI X9.42 ([ANSI, X9.42]) y PKCS #3 de los laboratorios RSA ([RSALab, 1993]).

MQV (Menezes-Qu-Vanstone Key Agreement, Acuerdo de Clave de Menezes-Qu-Vanstone): ANSI X9.42 ([ANSI, X9.42]), ANSI X9.63 ([ANSI, X9.63]) e IEEE 1363 [IEEE, 1363].

5 e. ECDH (Elliptic Curve Diffie-Hellman, Acuerdo de Clave de Diffie- Hellman con Curvas Elípticas): ANSI X9.63 ([ANSI, X9.63]), IEEE1363 ([IEEE, 1363]), IEEE1363a ([IEEE, 1363a]) y la Suite B de la NSA ([NSA, SuiteB]).

10 f. ECMQV (Elliptic Curve Menezes-Qu-Vanstone, Acuerdo de Clave de Menezes-Qu-Vanstone con Curvas Elípticas): Suite B de la NSA ([NSA, SuiteB]) y SEC 1 del SECG ([SECG, SEC1]).

15 g. DSA (Digital Signature Algorithm, Algoritmo de Firma Digital): ANSI X9.30 ([ANSI, X9.30-1]), FIPS 186-2 ([NIST, FIPS186-2]) y FIPS 186-3 ([NIST, FIPS186-3]).

20 h. ECDSA (Elliptic Curve Digital Signature Algorithm, Algoritmo de Firma Digital con Curvas Elípticas): ANSI X9.62 ([ANSI, X9.62]), FIPS 186-2 ([NIST, FIPS186-2]), SP 800-57A del NIST ([NIST, SP800-57A]), la Suite B de la NSA ([NSA, SuiteB]) y SEC 1 del SECG ([SECG, SEC1]).

i. RSA (Criptosistema RSA): ANSI X9.44 ([ANSI, X9.44]), FIPS 186-2 ([NIST, FIPS186-2]) y PKCS #1 de los laboratorios RSA ([RSALab, 2002]).

25 j. ECIES (Elliptic Curve Integrated Encryption Scheme, Esquema de Cifrado Integrado con Curvas Elípticas): ANSI X9.63 ([ANSI, X9.63]), IEEE1363a ([IEEE, 1363a]) e ISO 18033-2 ([ISOIEC, 18033-2]).

30 k. SHA (Secure Hash Algorithm, Algoritmo Resumen Seguro): FIPS180-1 ([NIST, FIPS180-1]), la Suite B de la NSA ([NSA, SuiteB]) y FIPS180-2 ([NIST, FIPS180-2]).

I. HMAC (Hash Message Authentication Code, Código de Autenticación de Mensaje con Resumen): ANSI X9.71 ([ANSI, X9.71]) y FIPS 198 ([NIST, FIPS198]).

5 En España, la página web del Organismo de Certificación del Centro Criptológico Nacional español (actualmente en el año 2011 http://www.oc.ccn.cni.es/ProdCert_es.html) y el portal de Common Criteria (<http://www.commoncriteriaportal.org/products/>); reúnen e identifican el catálogo de algoritmos y protocolos criptográficos conocidos y públicos.

10

 Finalmente, pueden ser tenidas en cuenta la Patente japonesa JP2005212788 NEC CORPORATION (2005) sobre un aparato y método de encriptar y desencriptar, o la Patente francesa FR2884995 de VIACCESS (2006) sobre un procedimiento de transmisión seguro con cifrado/descifrado de información. Todas ellas como procedimientos alternativos de codificación de información que emplean un solo criptograma, y no dos como la invención que se plantea en la cual se hace uso de dos criptogramas consecutivos, cada uno de los cuales ya es un criptograma seguro de Shanonn.

20

Problema técnico

25 La finalidad de la criptografía reside en lograr la máxima inescrutabilidad, o lo que es lo mismo minimizar al máximo su vulnerabilidad y obtener una gran seguridad en el mensaje (información o datos) de no interceptación por terceros no autorizados, ajenos al receptor y el emisor. Y ello, tanto en **soportes de información** (p.ej., un CD-Rom, una videoconsola, una unidad de memoria flash, un PC) como para su **comunicación, difusión y reproducción**. El problema con el que se enfrentan todos los tipos de cifrado es el del ataque o intromisión no deseada en la vía de comunicación, entre el emisor y el receptor del mensaje, de un tercer agente (pirata) que extrae el

30

texto claro cuando conoce las claves que han sido utilizadas para codificarlo. Actualmente, y para cualquier tipo de cifrado, el método de ataque más simple es el llamado *fuerza bruta*. Este se lleva a cabo probando una por una cada clave posible, proceso que se realiza haciendo uso de ordenadores cada vez con mayor potencia de cálculo. La posibilidad de descubrir la clave *precisa* con que se ha cifrado un mensaje disminuye a medida que aumenta su longitud. Esta circunstancia obliga, como ya hemos comentado en la introducción de esta exposición, a aumentar cada vez más el tamaño de la clave. Por otra parte, el criptoanálisis ofrece alternativas teóricas para romper, por ejemplo, las dieciséis rondas completas de DES con menos complejidad que un ataque por fuerza bruta. Pero tanto el *criptoanálisis diferencial*, como el *criptoanálisis lineal*, como el *ataque mejorado de Davies* requieren de entre 2^{40} y 2^{50} textos claros conocidos para poder romper las 16 rondas completas de DES. Esta exigencia determina que cualquiera de estos ataques teóricos resulte inviable a efectos prácticos.

20 *Solución técnica*

Una solución que se propone es la de integrar un doble criptograma mediante la que aquí denominamos *Criptografía de Residuos*. A través de ésta hacemos uso de las operaciones de *Confusión* y de *Difusión*. Concretamente en el proceso que conduce del *texto claro* a la *plantilla* o *criptograma reducido de residuos*. Pero en la *Criptografía de Residuos* se añade una tercera operación: la *Transformación* de cada residuo de la *plantilla* mediante el algoritmo de codificación en una secuencia de tantos dígitos como ordene el índice j de la *clave de protocolo*. Esta tercera operación está basada en un teorema numérico que nosotros llamamos *Teorema de los Residuos*.

La Transformación es la operación que hace que el Criptograma de Residuos presente un cambio cualitativo definitivo respecto a los otros lenguajes criptográficos actuales. Cambio cualitativo, en nuestra opinión comparable al que la Difusión representó para la sola presencia de la Confusión (por ejemplo, en el *cifrado de César*). Esta operación convierte al *Criptograma de Residuos*, con toda probabilidad, en el único sistema de cifrado simétrico *fácilmente manejable* que cumple el requisito de *Criptograma Seguro de Shannon*.

En efecto, al igual que el espacio de los mensajes, también es Aleph-0 la cardinalidad asociada al espacio de los elementos (agrupaciones de residuos) que integran la totalidad de las *tablas de equivalencias* y también es Aleph-0 o mayor la cardinalidad asociada al espacio de las *claves de protocolo*, conceptos técnicos que más adelante se describen. Por tanto disponemos en el criptograma de residuos de una doble cardinalidad Aleph-0 o mayor en la parte de las claves, mientras que es Aleph-0 la correspondiente al espacio de los mensajes, cumpliéndose por lo tanto el requisito de Shannon de criptograma seguro.

En conclusión, es el único procedimiento de cifrado de mensajes, datos e información que cumple el requisito de criptograma seguro de Shannon, por partida doble y consecutivamente. Por consiguiente, se logra un proceso de cifrado indescifrable por terceros.

Además, la invención que se presenta para codificación segura de información observa y permite adaptarse a las medidas de seguridad que vienen indicadas y reguladas por las normativas españolas y europeas de Telecomunicaciones y Sociedad de la Información. Así como, a los estándares de la *International Organization for Standardization* (ISO), y Recomendaciones de la Unión Internacional de Telecomunicaciones (UIT), en particular en la Serie X sobre Redes de Datos y Comunicación entre sistemas abiertos las

Normas UIT-T X.272 sobre Compresión y privacidad de datos por redes de retransmisión de tramas (versión 03/2000), UIT-T X.273 y UIT-T X.274 sobre Interconexión de sistemas abiertos y Protocolos de Seguridad (versión 07/1994).

5

Descripción de las figuras

Para una mejor comprensión de las características generales anteriormente mencionadas, se acompañan varios dibujos a la presente invención los cuales exponen como se especifica a continuación:

10

Figura 1: Organigrama de funcionamiento para la transmisión de información entre dos partes mediante un correo electrónico con las siguientes etapas: Una primera fase de codificación que realiza el emisor del mensaje, seguida de una segunda y última fase de decodificación que resuelve el destinatario o receptor pudiendo así éste leer el texto que le ha remitido el primero a través, por ejemplo, de un e-mail.

15

Modo de realización de la invención

20

A continuación describimos la realización de la invención junto con cada uno de los medios empleados. Son elementos o medios técnicos empleados, los siguientes:

25

1. *Una matriz alfanumérica*
2. *Una matriz base de residuos numéricos*
3. *Una clave de equivalencias*
4. *Una tabla de equivalencias*
5. *Un criptograma reducido de residuos o plantilla*
6. *Una clave de protocolo*
7. *Un algoritmo de codificación*
8. *Un criptograma final de residuos*
9. *Un algoritmo de decodificación*

30

1.La Matriz alfanumérica

La matriz alfanumérica está constituida por todos los caracteres alfanuméricos que nos sirven para escribir un texto claro o texto ordinario. Los caracteres se pueden ordenar de la forma que quiera el usuario. En el caso de la Tabla.1, por comodidad, hemos decidido construir una matriz 11x11 cuyos elementos son precisamente los caracteres alfanuméricos latinos del teclado del ordenador con el cual estamos escribiendo este texto.

**Tabla.1. MATRIZ ALFANUMÉRICA.
Tipo Teclado de ordenador personal**

0	1	2	3	4	5	6	7	8	9	Ç	1
A	B	C	D	E	F	G	H	I	J	K	2
L	M	N	O	P	Q	R	S	T	U	V	3
W	X	Y	Z	Ñ	ı	ı	"	.	\$	€	4
&	/	()		?	¿	^	`	~	,	5
	-	[]	{	}	<	>	;	:	_	6
:	'	ç	a	b	c	d	e	f	g	h	7
i	j	k	l	m	n	o	p	q	r	s	8
t	u	v	w	x	y	z	ñ	*	±	=	9
ú	ó	ò	í	@							10
é	è	á	à	%							11
1	2	3	4	5	6	7	8	9	10	11	

10

La última columna y la última fila no forman parte, naturalmente, de la matriz. Simplemente este orlado nos sirve para localizar más rápidamente el lugar de la matriz que ocupa un determinado elemento suyo. Como se puede observar hay tres elementos de la matriz que se han sombreado: aquí representaran, para esta matriz, el espaciado del teclado, los tres. También se

15

destaca en la matriz que hay otros diez elementos "blancos": éstos pueden expresar cualquier otro elemento ya ubicado en otro lugar, o el propio espaciado o, simplemente, pueden significar elementos que no ocuparán espacio en el criptograma final, o sea, como si no existiesen. Esta posibilidad

5 proporciona una herramienta potente para escribir el criptograma final con presencia de secuencias de dígitos que, en realidad, servirán sólo para confundir el posible ataque de un pirata, es decir, de un tercero que intenta descifrarlo.

10 2. La Matriz base de residuos numéricos

Entenderemos en todo lo que sigue por *residuo numérico* o, simplemente, *residuo* a cada uno de los números naturales comprendidos entre el 1 y el 9, ambos inclusive. En esta exposición representaremos

15 genéricamente a los nueve residuos por el símbolo \mathfrak{R} .

Llamaremos entonces *matriz base de residuos numéricos* a cualquier ordenación de residuos, pares de residuos, ternas de residuos, etc., *todos diferentes* y que se distribuyan de forma arbitraria pero ordenada para que

20 cada una de estas agrupaciones de residuos quede localizada en un determinado lugar de la distribución. Si, por ejemplo, nuestra *matriz base de residuos numéricos* se confecciona solamente con residuos simples, la matriz constará como máximo de nueve elementos: 1, 2, 3, 4, 5, 6, 7, 8, 9. Si deseamos construir una *matriz base de residuos numéricos binaria* o de

25 *segundo orden*, es decir, cuyos elementos estén formados solamente por grupos de pares de residuos, entonces dispondremos de matrices con un número máximo de elementos de $9^2 = 81$. Una *matriz base de residuos numéricos ternaria* o de *tercer orden* estará constituida por agrupaciones de tres residuos, siendo entonces la dimensión máxima de estas matrices aquella

30 que se halla conformada por $9^3 = 729$ elementos, etc. Los elementos $a(i_n, i_{n-1}, i_{n-2}, \dots, i_2, i_1)$ de una *matriz de residuos numéricos de orden n* se obtienen de la siguiente expresión general:

$$a(i_n, i_{n-1}, \dots, i_2, i_1) = 10^{n-1}i_n + 10^{n-2}i_{n-1} + \dots + 10i_2 + i_1 \quad (2.2.1)$$

donde $i_j = 1, 2, \dots, 9; \quad j = 1, 2, \dots, n$

siendo n el número de residuos que se agrupan para formar cada elemento de la matriz. Estos elementos se pueden ordenar como elementos de matrices cuadradas a partir de $n=2$. En este caso tendremos una matriz 9x9, tomando la expresión (2.2.1) la forma:

$$a(i_2, i_1) = 10i_2 + i_1 \quad (2.2.2)$$

donde $i_j = 1, 2, \dots, 9; \quad j = 1, 2$

Si $n=3$ la matriz será de 27x27, ya que $9^3=729=27 \times 27$, en cuyo caso la expresión (2.2.1) toma la forma:

$$a(i_3, i_2, i_1) = 10^2i_3 + 10i_2 + i_1 \quad (2.2.3)$$

donde $i_j = 1, 2, \dots, 9; \quad j = 1, 2, 3$

Si $n=4$ la matriz será de 81x81, puesto que $9^4=6561=81 \times 81$, etc.

15

Si en (2.2.2), el índice i_2 expresa la fila de la matriz 9x9 y el índice i_1 la columna entonces la *matriz base de residuos numéricos binaria* presenta el ordenamiento que se puede ver en la Tabla.2.

En la Tabla.3. mostramos la *matriz base de residuos numéricos ternaria*. Obsérvese que sus 729 elementos los hemos ordenado mediante 9 anidamientos (los 9 valores que aquí toma el tercer subíndice i_3) a partir de la matriz binaria. De la misma manera ordenaremos las matrices de orden superior cuando deseemos utilizarlas.

25

Como en el caso de la matriz alfanumérica, también a estas matrices le hemos añadido el orlado formado por la última columna y la última fila, las cuales únicamente sirven para observar fácilmente el lugar que ocupa cada par o cada terna de residuos mediante el número de fila y de columna.

5

**Tabla 2. Matriz base de residuos
numéricos binaria**

11	12	13	14	15	16	17	18	19	1
21	22	23	24	25	26	27	28	29	2
31	32	33	34	35	36	37	38	39	3
41	42	43	44	45	46	47	48	49	4
51	52	53	54	55	56	57	58	59	5
61	62	63	64	65	66	67	68	69	6
71	72	73	74	75	76	77	78	79	7
81	82	83	84	85	86	87	88	89	8
91	92	93	94	95	96	97	98	99	9
1	2	3	4	5	6	7	8	9	

Tabla.3. Matriz base de residuos numéricos ternaria

111	112	113	114	115	116	117	118	119	200	201	202	203	204	205	206	207	208	209	311	312	313	314	315	316	317	318	319	1	
121	122	123	124	125	126	127	128	129	200	202	203	204	205	206	207	208	209	321	322	323	324	325	326	327	328	329	2		
131	132	133	134	135	136	137	138	139	200	203	204	205	206	207	208	209	331	332	333	334	335	336	337	338	339	3			
141	142	143	144	145	146	147	148	149	200	204	205	206	207	208	209	341	342	343	344	345	346	347	348	349	4				
151	152	153	154	155	156	157	158	159	200	205	206	207	208	209	351	352	353	354	355	356	357	358	359	5					
161	162	163	164	165	166	167	168	169	200	206	207	208	209	361	362	363	364	365	366	367	368	369	6						
171	172	173	174	175	176	177	178	179	200	207	208	209	371	372	373	374	375	376	377	378	379	7							
181	182	183	184	185	186	187	188	189	200	208	209	381	382	383	384	385	386	387	388	389	8								
191	192	193	194	195	196	197	198	199	200	209	391	392	393	394	395	396	397	398	399	9									
200	201	202	203	204	205	206	207	208	209	511	512	513	514	515	516	517	518	519	600	601	602	603	604	605	606	607	608	609	10
200	202	203	204	205	206	207	208	209	521	522	523	524	525	526	527	528	529	600	602	603	604	605	606	607	608	609	11		
200	203	204	205	206	207	208	209	531	532	533	534	535	536	537	538	539	600	603	604	605	606	607	608	609	12				
200	204	205	206	207	208	209	541	542	543	544	545	546	547	548	549	600	604	605	606	607	608	609	13						
200	205	206	207	208	209	551	552	553	554	555	556	557	558	559	600	605	606	607	608	609	14								
200	206	207	208	209	561	562	563	564	565	566	567	568	569	600	606	607	608	609	15										
200	207	208	209	571	572	573	574	575	576	577	578	579	600	607	608	609	16												
200	208	209	581	582	583	584	585	586	587	588	589	600	608	609	17														
200	209	591	592	593	594	595	596	597	598	599	600	609	18																
711	712	713	714	715	716	717	718	719	800	801	802	803	804	805	806	807	808	809	911	912	913	914	915	916	917	918	919	19	
721	722	723	724	725	726	727	728	729	800	802	803	804	805	806	807	808	809	921	922	923	924	925	926	927	928	929	20		
731	732	733	734	735	736	737	738	739	800	803	804	805	806	807	808	809	931	932	933	934	935	936	937	938	939	21			
741	742	743	744	745	746	747	748	749	800	804	805	806	807	808	809	941	942	943	944	945	946	947	948	949	22				
751	752	753	754	755	756	757	758	759	800	805	806	807	808	809	951	952	953	954	955	956	957	958	959	23					
761	762	763	764	765	766	767	768	769	800	806	807	808	809	961	962	963	964	965	966	967	968	969	24						
771	772	773	774	775	776	777	778	779	800	807	808	809	971	972	973	974	975	976	977	978	979	25							
781	782	783	784	785	786	787	788	789	800	808	809	981	982	983	984	985	986	987	988	989	26								
791	792	793	794	795	796	797	798	799	800	809	991	992	993	994	995	996	997	998	999	27									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27			

3. La Clave de equivalencias

5

Una vez escogida una determinada *matriz base de residuos numéricos*, hemos de introducir la **clave de equivalencias**. Ésta va a actuar sobre la *matriz base de residuos numéricos* y la transformará en otra *matriz base reordenada de residuos numéricos*, es decir, en una nueva matriz en la que algunas o todas las agrupaciones de residuos permutaran sus lugares entre sí. Como la *matriz base de residuos numéricos* será una matriz de dimensión $m \times n$ (m filas y n columnas), aunque nosotros preferimos ordenar los

10

elementos como matriz cuadrada, como acabamos de mostrar, la *clave de equivalencias* consistirá en la introducción de dos conjuntos de números entre el 1 y m el primero y entre el 1 y n el segundo. En esta exposición cada número de ambos conjuntos irá separado por una coma de sus vecinos y ambos
 5 conjuntos separados entre sí por un guión (-).

A continuación describiremos cómo actúa la *clave de equivalencias* y con este propósito y para hacernos comprender mejor, supondremos que hemos escogido la *matriz base de residuos numéricos ternaria* de la Tabla.3.
 10 Como ésta es una matriz 27×27 , una matriz cuadrada, en este caso $m = n = 27$. Supongamos que escogemos la *clave de equivalencias* 3, 27, 18, 9, 5, 21 – 7, 1, 9, 3. Para esta clave el programa de permutación de lugares actuará así: permutará la fila 3 por la 27, a continuación permutará las filas 18 y 9 a la que seguirá la permutación de las filas 5 y 21. Es decir, la operación de
 15 permutación de filas se realiza identificando cada número de la clave en posición impar con la fila que numéricamente designe dicho número, permutando esta fila su lugar con la que designe el siguiente número de clave, de posición par, y así sucesivamente hasta agotar el número par de parejas numéricas introducidas en el conjunto de la clave de la izquierda del guión de
 20 separación. Sobre esta última ordenación actuará ahora la parte derecha del guión de la clave de equivalencias que hemos escogido. En este caso se permutarán las columnas 7 y 1 y las columnas 9 y 3.

En el supuesto que alguna, o ambas, de las secuencias anteriores de la
 25 *clave de equivalencias*, constasen de una cantidad impar de números, el último de estos sería superfluo, ya que intercambiaría su lugar (fila o columna) consigo mismo. La distribución obtenida como resultado de este proceso es la *matriz base reordenada de residuos numéricos ternaria*.

30 A título de ejemplo y para seguir mejor las explicaciones ulteriores, en la Tabla.4. se expone una *matriz base reordenada de residuos numéricos ternaria*, obtenida, con una determinada clave de equivalencias, de la *matriz*

base de residuos numéricos ternaria representada en la Tabla.3. Sobre la matriz expresada en la Tabla.4 hemos sombreado 4 matrices menores 11x11 que forman parte de la total y tales que *no tienen ningún elemento en común*. Esto lo hemos hecho con el propósito de que ayude al lector en una mejor comprensión de los argumentos que posteriormente expondremos.

Tabla.4. Matriz base reordenada de residuos numéricos ternaria

123	114	113	114	115	116	117	118	119	121	122	123	124	125	126	127	131	129	131	132	133	134	135	136	137	138	139	1
153	142	143	144	145	146	147	148	149	151	152	153	154	155	156	157	161	159	161	162	163	164	165	166	167	168	169	2
183	172	173	174	175	176	177	178	179	181	182	183	184	185	186	187	191	189	191	192	193	194	195	196	197	198	199	3
213	212	213	214	215	216	217	218	219	221	222	223	224	225	226	227	231	229	231	232	233	234	235	236	237	238	239	4
253	242	243	244	245	246	247	248	249	251	252	253	254	255	256	257	261	259	261	262	263	264	265	266	267	268	269	5
283	272	273	274	275	276	277	278	279	281	282	283	284	285	286	287	291	289	291	292	293	294	295	296	297	298	299	6
313	312	313	314	315	316	317	318	319	321	322	323	324	325	326	327	331	329	331	332	333	334	335	336	337	338	339	7
353	342	343	344	345	346	347	348	349	351	352	353	354	355	356	357	361	359	361	362	363	364	365	366	367	368	369	8
383	372	373	374	375	376	377	378	379	381	382	383	384	385	386	387	391	389	391	392	393	394	395	396	397	398	399	9
413	412	413	414	415	416	417	418	419	421	422	423	424	425	426	427	431	429	431	432	433	434	435	436	437	438	439	10
453	442	443	444	445	446	447	448	449	451	452	453	454	455	456	457	461	459	461	462	463	464	465	466	467	468	469	11
483	472	473	474	475	476	477	478	479	481	482	483	484	485	486	487	491	489	491	492	493	494	495	496	497	498	499	12
513	512	513	514	515	516	517	518	519	521	522	523	524	525	526	527	531	529	531	532	533	534	535	536	537	538	539	13
553	542	543	544	545	546	547	548	549	551	552	553	554	555	556	557	561	559	561	562	563	564	565	566	567	568	569	14
583	572	573	574	575	576	577	578	579	581	582	583	584	585	586	587	591	589	591	592	593	594	595	596	597	598	599	15
613	612	613	614	615	616	617	618	619	621	622	623	624	625	626	627	631	629	631	632	633	634	635	636	637	638	639	16
653	642	643	644	645	646	647	648	649	651	652	653	654	655	656	657	661	659	661	662	663	664	665	666	667	668	669	17
683	672	673	674	675	676	677	678	679	681	682	683	684	685	686	687	691	689	691	692	693	694	695	696	697	698	699	18
713	712	713	714	715	716	717	718	719	721	722	723	724	725	726	727	731	729	731	732	733	734	735	736	737	738	739	19
753	742	743	744	745	746	747	748	749	751	752	753	754	755	756	757	761	759	761	762	763	764	765	766	767	768	769	20
783	772	773	774	775	776	777	778	779	781	782	783	784	785	786	787	791	789	791	792	793	794	795	796	797	798	799	21
813	812	813	814	815	816	817	818	819	821	822	823	824	825	826	827	831	829	831	832	833	834	835	836	837	838	839	22
853	842	843	844	845	846	847	848	849	851	852	853	854	855	856	857	861	859	861	862	863	864	865	866	867	868	869	23
883	872	873	874	875	876	877	878	879	881	882	883	884	885	886	887	891	889	891	892	893	894	895	896	897	898	899	24
913	912	913	914	915	916	917	918	919	921	922	923	924	925	926	927	931	929	931	932	933	934	935	936	937	938	939	25
953	942	943	944	945	946	947	948	949	951	952	953	954	955	956	957	961	959	961	962	963	964	965	966	967	968	969	26
983	972	973	974	975	976	977	978	979	981	982	983	984	985	986	987	991	989	991	992	993	994	995	996	997	998	999	27
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	

Aquello que aquí nos interesa resaltar ahora es que con la *clave de equivalencias* adecuada podemos obtener de *la matriz base de residuos numéricos inicial* cualquier particular *matriz base reordenada de residuos numéricos* que nos interese.

Con ello, concurren infinitas posibilidades de matrices base reordenadas de que podemos disponer. Pero incluso en el caso de que nos ciñéramos a matrices de residuos ternarias, disponemos de la fabulosa cantidad de 729! (factorial de 729) ordenaciones posibles de las 729 ternas de residuos. Es
5 decir, de [aproximadamente 68×10^{1770} *matrices base reordenada de residuos numéricos ternarias*].

Ante esta enorme cantidad, el número de claves del algoritmo DES resulta infinitesimal a todos los efectos prácticos, como ya hemos adelantado
10 anteriormente. Un ordenador tan potente que fuese capaz de descartar una tabla de equivalencias por segundo, y el número de éstas es siempre igual o mayor que el número de matrices base reordenadas como veremos en el apartado siguiente, necesitaría más de 2×10^{1764} años para agotar todas las
posibilidades

15

4. La Tabla de equivalencias

A partir de la *matriz alfanumérica* (Tabla.1) y de la *matriz base reordenada de residuos numéricos* que hemos escogido aquí como ejemplo
20 (Tabla.4), construiremos la ***tabla de equivalencias***. Esta se conforma haciendo corresponder cada elemento de la *matriz alfanumérica* con uno o más de los elementos de la *matriz base reordenada de residuos numéricos*. Esta correspondencia se puede realizar de cualquier manera que puedan imaginar,
25 o pactar, los interlocutores que desean transmitirse información, respetando tan solo un requisito: que no haya ningún elemento de la *matriz base reordenada de residuos numéricos* que se corresponda con más de uno de los elementos de la *matriz alfanumérica*. Naturalmente, esta condición se exige con el objeto de que el criptograma resultante no presente ambigüedades o multiplicidades.

30

Si bien la *tabla de equivalencias* se puede conformar de cualquier manera, para los casos de construcción de programas de ordenador es preferible realizar la correspondencia mediante alguna conexión matemática, procedimiento que, en general, presenta también una gran versatilidad. A título de ejemplo consideremos la *matriz alfanumérica* representada en la Tabla.1 y la *matriz base reordenada de residuos numéricos* de la Tabla.4. Entre las muchas correspondencias de tipo matemático que se pueden realizar, respetando el requisito anterior de que ningún elemento de la matriz base se corresponda con más de uno de los de la matriz alfanumérica, podemos construir, por ejemplo, la siguiente:

Representemos a los elementos de la *matriz alfanumérica* mediante la notación algebraica: $A_{i,j}$ tal que $i, j = 1, 2, \dots, 11$, y a los elementos de la *matriz base reordenada* mediante la notación $B_{k,l}$ tal que $k, l = 1, 2, \dots, 27$. Una de las correspondencias posibles, y que justifica los sombreados que hemos hecho sobre la matriz de la Tabla.4 para mayor claridad del lector, es la que expresa la relación siguiente:

$$A_{i,j} \leftrightarrow B_{i,j}, B_{i,16+j}, B_{16+i,j}, B_{16+i,16+j} \quad (2.4.1)$$

tal que $i, j = 1, 2, \dots, 11$

En esta relación el símbolo \leftrightarrow se debe entender como la expresión de la correspondencia del elemento que se halla a su izquierda con los elementos situados a su derecha. Por ejemplo, al elemento $A_{3,8}$ de la matriz alfanumérica (Tabla.1) que es ocupado por la letra S, le corresponden los elementos $B_{3,8}, B_{3,24}, B_{19,8}$ y $B_{19,24}$ de la matriz base reordenada (Tabla.4), es decir, las ternas de residuos 178, 196, 718 y 736.

5 El Criptograma reducido de residuos o plantilla

5 Como resultado de “filtrar” el texto claro, es decir, el mensaje con caracteres alfanuméricos ordinarios que se desea codificar, a través de la tabla de equivalencias se obtiene una primera codificación que aquí denominaremos *Criptograma reducido de residuos* o, simplemente, *plantilla*. Para fijar mejor las ideas ilustraremos con un ejemplo el procedimiento.

10 Supongamos que el emisor desea codificar la frase: *la reunión es mañana jueves*, y que ha escogido como *tabla de equivalencias* la descrita por la relación (2.4.1). Pues bien, *una* de las muchas *plantillas* que tiene asociada esta frase de acuerdo con la opción escogida viene representada en la Tabla.5.

15 **Tabla.5. Plantilla**

L	a	r	e	u	n	i	ó	n	e	s			
188	314	982	351	318	372	346	358	972	364	976	336	352	451
m	a	ñ	a	n	a		j	u	e	v	e	s	
345	332	378	844	876	862	438	342	389	848	373	866	899	

20 Debajo de cada carácter alfabético hemos escrito una de las ternas de residuos que le corresponde de acuerdo con la relación escogida (2.4.1).

25 Se observará que la plantilla expresa ya un criptograma potente, ya que al hacer uso de la correspondencia múltiple no se ha repetido ninguna terna – puede comprobarse que las ternas debajo de cada carácter alfabético o del propio espaciado son todas distintas-. Pero como se verá a continuación el criptograma final es infinitamente más complejo e indescifrable que el dado por la plantilla.

6. Una Clave de protocolo

Obtenida la *plantilla* estamos en condiciones de culminar la última etapa del proceso que conduce al *criptograma final*. Este se consigue después de someter consecutivamente a cada uno de los residuos \mathfrak{R} que conforman la plantilla a la acción de un *algoritmo de codificación*. Pero a su vez este algoritmo actúa según las directrices que le impone la *clave de protocolo*. Así que vamos a describir con suficientes detalles este proceso fundamental en la que aquí denominamos *criptografía de residuos*.

La *clave de protocolo* viene dada por una secuencia arbitraria, que se tendrá que pactar entre los dos interlocutores, de *números naturales* de la que se excluye el cero. En esta exposición, los naturales escogidos se encontrarán separados por una coma y serán designados *índices del protocolo*. Son, por ejemplo, posibles *claves de protocolo* las secuencias: 3, 12, 5, 2, 5, 6 y 2, 3, 4, 5, 10, 61, 3, 9, 22, 35, 5, 4, etc. Así, si escogemos como *clave de protocolo* la secuencia 3, 12, 5, 3, 5, 6 y la aplicamos a la plantilla de la Tabla.5 anterior, el efecto conseguido será el siguiente: Esta clave le va a exigir al *algoritmo de codificación* que convierta el primer residuo de la plantilla, el 1 en este caso, en una secuencia de 3 dígitos ya que 3 es el índice de protocolo que le corresponde. El segundo residuo es 8 y como el segundo índice de protocolo es 12, el algoritmo de codificación debe asociar a este residuo una secuencia de 12 dígitos. A continuación viene como residuo otro 8, pero ahora 5 es el índice de protocolo correspondiente, así que el algoritmo de codificación le asociará a este residuo una secuencia de 5 dígitos. Así se continuará hasta llegar al sexto residuo de valor 4 al cual el algoritmo de codificación le asociará una secuencia de 6 dígitos, ya que es 6 el índice de protocolo que le corresponde.

30

Continuando con el ejemplo, para el residuo que ocupa el séptimo lugar de la plantilla que en este caso tiene valor 9, se parte de la situación en que se

recorren todos los índices que conforman la clave del protocolo, y se abren toda una serie de posibilidades para proseguir con la codificación conducente al criptograma final. Por ejemplo, y es lo que haremos nosotros después para continuar, podemos reiniciar la secuencia de la clave de protocolo tantas veces como haga falta hasta completar la plantilla. Pero podemos también decidir que la secuencia de la clave de protocolo actúe cíclicamente, es decir, según el ordenamiento: 3, 12, 5, 3, 5, 6, **12, 5, 3, 5, 6, 3**, 5, 3, 5, 6, 3, 12, 3, **5, 6, 3, 12, 5**, 5, 6, 3, 12, 5, 3, **6, 3, 12, 5, 3, 5**, etc. Hay tantas posibilidades como inventiva tengan y pacten los interlocutores. Respecto del valor de los índices de protocolo, debe quedar claro que cuanto más grandes, más largo será el criptograma final. No obstante, hemos de reconocer que a veces puede ser conveniente conformar un criptograma de gran extensión. Por otra parte, como también comentaremos más adelante, se pueden construir también cantidades ingentes de criptogramas que representan a distintos textos *constando todos exactamente del mismo número de dígitos* en su criptograma final.

7.El Algoritmo de codificación

Como acabamos de decir, el *algoritmo de codificación* nos permite asociar a cada residuo \mathfrak{R} de la plantilla una secuencia que consta de j dígitos, siendo j , precisamente, el índice de protocolo de la clave de protocolo que hemos elegido. El algoritmo de codificación se puede construir de muy diferentes formas. Para esta exposición y teniendo presente que un ordenador actual difícilmente puede operar con exactitud con números enteros de más de 15 dígitos, nos hemos decidido por el algoritmo de codificación cuya descripción exponemos a continuación y para el cual el obstáculo de enteros con más de 15 dígitos desaparece. Este es nuestro algoritmo:

Para un determinado *índice de protocolo* j , el programa comprobará si su valor concreto está entre 1 y 3, ambos inclusive, o si, por el contrario j es mayor que 3.

Si j es menor o igual que 3 el programa empezará generando un número aleatorio A comprendido entre 1 y 9, ambos inclusive. A continuación el programa asociará al residuo \mathfrak{R} el número natural de j dígitos dado por la expresión

5
$$\mathfrak{R} + A \times (10^{j-1} - 1)$$

En el caso que el índice del protocolo j sea igual o mayor que 4, el programa empezará generando el número aleatorio

$$A = \text{ENTERO} (\text{ALEATORIO}() \times (j-2) + 1)$$

10

Este número está comprendido entre 1 y $(j-2)$. Pues bien, justamente en la posición A del total de las j posiciones que van a ocupar los j dígitos de que consta la secuencia asociada al residuo \mathfrak{R} , se va a colocar como dígito, precisamente, el residuo \mathfrak{R} . Exceptuando ahora las posiciones $(j-1)$ y j , tendremos todavía $(j-3)$ posiciones, todas ellas situadas a la izquierda de las dos anteriores que son las últimas. Pues bien, para estas $(j-3)$ posiciones el programa generará aleatoriamente un número natural entre el 0 y el 9, ambos incluidos. En la penúltima posición, es decir, en la posición $(j-1)$, el programa anotará el dígito p que resulta de la operación

15

20
$$p = \sum_{k=1}^{j-2} (\text{digitos posiciones } k) - 9 \times \text{ENTERO} \left[\frac{\sum_{k=1}^{j-2} (\text{digitos posiciones } k)}{9} \right]$$

Finalmente, en la última posición, es decir, la posición j , el programa anotará el dígito que resulta de la operación

$$\mathfrak{R} - \sum_{k=1}^{j-2} (\text{digitos posiciones } k) - p - 9 \times \text{ENTERO} \left[\frac{\mathfrak{R} - \sum_{k=1}^{j-2} (\text{digitos posiciones } k) - p}{9} \right]$$

25

8. El Criptograma final

5 Cuando se aplique este algoritmo que acabamos de exponer consecutivamente a todos y cada uno de los residuos de la *plantilla*, obtendremos como resultado el *criptograma final* del texto que nos interesa codificar. Es este texto el que el emisor remitirá al receptor, a través de un e-mail o a través de cualquier otra vía que considere conveniente.

10

 A modo ilustrativo, la Tabla.6 muestra *un* criptograma final correspondiente a la plantilla de la Tabla.5 , es decir, al texto: *La reunión es mañana jueves*. Este criptograma consta de 462 dígitos y se ha obtenido haciendo uso de la *clave de protocolo* 3, 12, 5, 3, 5, 6 consecutivamente.

15 Hemos escrito en cursiva *un* delante de criptograma en la primera línea de este punto y aparte, porque la Tabla.6 muestra tan sólo *uno* de los criptogramas finales de un total de, prácticamente, infinitos criptogramas finales que podemos asociar a la misma frase y *con la misma clave de protocolo*, ya que los dígitos de que consta se han generado en su mayoría de forma aleatoria.

20 Naturalmente, el algoritmo decodificador del que hablaremos más adelante descifra el mensaje con independencia de cuál sea el criptograma final que se le presente. También debe comprenderse que la longitud del criptograma depende de la clave de protocolo que sea utilizada. Cuanto más grande sea la suma de los índices de la clave de protocolo, mayor será la longitud de la

25 cadena de dígitos que conforma el criptograma final. Por estas circunstancias podemos construir criptogramas finales, correspondientes a distintas frases, unas más largas, otras más cortas, con la misma cantidad de dígitos que uno de los criptogramas asociado a cualquier texto previamente escogido. Por ejemplo, está en nuestras manos construir una gran cantidad de criptogramas

30 todos de 462 dígitos, como el de nuestro ejemplo, y que cada uno de ellos corresponda a un texto diferente. Ésta propiedad es posible que sea una de las

que mejor exprese la potencia de nuestra criptografía de residuos cuando es comparada con cualquiera de las que, hasta ahora, se han ideado.

5 **Tabla.6. Un criptograma final de la expresión:**

La reunión es mañana jueves

1	8	1	3	2	6	7	4	5	0	4	3	1	8	1	0	8	4	8	6	3	6	3	5	0	6	1	7	5	3	0	8	2	4	0	0	9	2	4	9	
8	2	4	5	1	0	6	4	8	7	6	2	4	1	2	7	3	0	5	6	7	5	0	1	6	7	4	1	3	5	4	0	1	1	6	1	3	7	7	4	
1	4	2	0	8	6	4	8	3	1	8	4	8	9	7	6	1	0	2	4	2	2	0	3	9	7	8	1	2	3	2	4	8	3	7	2	2	6	3	6	
8	1	4	3	5	1	3	8	6	5	1	6	8	8	7	5	0	0	9	6	4	9	1	5	8	8	7	8	7	6	1	1	2	8	0	9	3	3	6	7	
1	8	2	6	1	2	7	5	3	4	1	8	9	4	8	7	2	7	2	6	1	1	9	8	6	1	4	5	8	6	3	6	3	7	7	3	9	4	7	1	
3	2	6	5	0	3	9	8	7	6	2	3	7	2	5	9	7	3	0	2	4	5	0	9	1	8	4	5	3	7	6	2	4	2	6	2	4	1	9	0	
3	1	2	2	4	1	1	5	6	4	4	8	2	3	8	6	1	5	3	9	0	6	0	3	5	7	7	6	3	1	1	2	3	1	8	2	3	9	2	7	
7	6	6	3	8	1	7	7	3	8	4	4	8	8	1	2	7	4	0	9	1	4	8	0	5	4	8	0	0	7	8	4	6	8	1	2	1	2	6		
7	1	8	6	2	7	6	8	3	1	1	6	7	0	5	1	4	1	2	7	4	3	6	8	5	6	6	3	8	6	6	6	8	2	2	4	0	2	8	3	
7	2	3	0	5	1	9	8	0	0	2	6	3	9	5	4	3	5	7	5	1	1	2	9	8	9	7	3	5	0	0	9	9	9	2	8	7	4	1	0	
8	9	6	5	8	6	0	1	8	1	3	5	6	9	5	7	5	4	3	7	5	0	5	1	8	3	2	7	8	9	9	5	5	8	6	9	8	8	5	6	
0	6	8	9	0	3	3	2	9	8	1	9	8	6	8	2	4	0	0	9	4	5																			

10 **9.- Algoritmo de decodificación**

El *criptograma final* es el que hace llegar el emisor al receptor. Naturalmente se supone que ambos interlocutores han pactado las claves usadas en la fase emisora, es decir la *clave de equivalencias* y la *clave de protocolo*, y también, es evidente, la *matriz base de residuos numéricos*. Admitido esto, el receptor ha de actuar de la siguiente manera: En primer lugar, y siguiendo exactamente los mismos pasos que previamente ha realizado el emisor, se construirá la *tabla de equivalencias*. El acto siguiente consiste, con ayuda de la *clave de protocolo*, en subdividir el criptograma final en secuencias consecutivas de dígitos cada una de las cuales tendrá tantos dígitos como exija el índice de protocolo *j* correspondiente. Para fijar mejor el razonamiento, la Tabla.7 nos muestra esta subdivisión mediante sombreados alternativos para el caso que el criptograma final fuese el mostrado en la Tabla.6.

Tabla.7. Un criptograma final de: *La reunión es mañana jueves*

1	8	1	3	2	6	7	4	5	0	4	3	1	8	1	0	8	4	8	6	3	6	3	5	0	6	1	7	5	3	0	8	2	4	0	0	9	2	4	9	
8	2	4	5	1	0	6	4	8	7	6	2	4	1	2	7	3	0	5	8	7	5	0	1	6	7	4	1	3	5	4	0	1	1	6	1	3	7	7	4	
1	4	2	0	8	8	4	8	3	1	8	4	8	9	7	6	1	0	2	4	2	2	0	3	9	7	8	1	2	3	2	4	8	3	7	2	2	8	3	8	
8	1	4	3	5	1	3	8	6	5	1	6	8	8	7	5	0	0	9	6	4	9	1	5	8	8	7	8	7	6	1	1	2	8	0	9	3	3	6	7	
1	8	2	6	1	2	7	5	3	4	1	8	9	4	8	7	2	7	2	6	1	1	9	8	6	1	4	5	8	6	3	6	3	7	7	3	9	4	7	1	
3	2	6	5	0	3	9	8	7	6	2	3	7	2	5	9	7	3	0	2	4	5	0	9	1	8	4	5	3	7	6	2	4	2	6	2	4	1	9	0	
3	1	2	2	4	1	1	5	6	4	4	8	2	3	8	6	1	5	3	9	0	6	0	3	5	7	7	6	3	1	1	2	3	1	8	2	3	9	2	7	
7	6	6	3	8	1	7	7	3	8	4	4	8	8	1	2	7	4	0	9	1	4	8	0	5	4	8	0	0	0	7	8	4	6	8	1	2	1	2	6	
7	1	8	6	2	7	6	8	3	1	1	8	7	0	5	1	4	1	2	7	4	3	8	8	5	6	6	3	8	6	6	6	8	2	2	4	0	2	8	3	
7	2	3	0	5	1	9	8	0	0	2	6	3	9	5	4	3	5	7	5	1	1	2	9	8	9	7	3	5	0	0	9	9	9	2	8	7	4	1	0	
8	9	6	5	8	6	0	1	8	1	3	5	6	9	5	7	5	4	3	7	5	0	5	1	8	3	2	7	8	9	9	5	5	8	6	9	8	8	5	6	
0	6	8	9	0	3	3	2	9	8	1	9	8	6	8	2	4	0	0	9	4	5																			

5

Cada una de estas secuencias de dígitos conforma un número natural que aquí vamos a representar por N_j , donde j expresa el índice de protocolo, es decir, el número de dígitos de que consta el anterior número natural. Pues bien, el receptor recuperará la *plantilla* del criptograma aplicando a cada una de

10 las secuencias N_j la expresión:

$$\mathfrak{R}(N_j) = \sum \text{digitos de } N_j - 9 \times \text{ENTERO} \left[\frac{\sum \text{digitos de } N_j}{9} \right]$$

15 Pero debemos advertir que cuando el resultado de la operación anterior dé 0 para el residuo, el programa ha de sustituirlo por un 9, ya que es este el residuo que le corresponde al cero.

20 Reproducida la *plantilla* solo queda ya un último acto: el receptor “filtra” la *plantilla* a través de la tabla de equivalencias y obtiene el texto claro, el texto escrito con caracteres alfanuméricos ordinarios.

25 Frente a poder considerar que las tablas de equivalencia con elementos constituidos por agrupaciones de n residuos, para n mucho mayor que la unidad producirían textos cifrados demasiado largos, hemos de manifestar que para agrupaciones de n residuos con n pequeña, por ejemplo, con $n=2$, es

decir, para matrices de residuos binarias disponemos ya de $81! \approx 23 \times 10^{129}$ matrices base reordenada de residuos numéricos binarias; que con $n=3$ el número de matrices base reordenada de residuos numéricos ternarias se eleva a $729! \approx 68 \times 10^{1770}$ y que con $n=4$ disponemos de $6561! \approx 203 \times 10^{22194}$ matrices base reordenada de residuos numéricos cuaternarias, etc. En segundo lugar, que la elección de una determinada base, binaria, ternaria, cuaternaria, etc. depende sólo de los interlocutores y que mientras éstos no digan qué base han escogido y cuáles son las claves utilizadas, el hipotético pirata no dispone de ningún argumento, ya que tiene ante sí infinitas posibilidades, que le permita empezar cualquier ataque con la garantía mínima de que alguno de los textos que pueda deducir tenga algo que ver con *aquél que verdaderamente* se han transmitido los interlocutores. Esto convierte ya a la plantilla o criptograma reducido de residuos en un potente criptograma, prácticamente indescifrable. Ilustraremos la última reflexión con un ejemplo. Consideremos el criptograma:

15

123456789161654353234439
367589992414457763212564

Este criptograma consta de 48 dígitos. Se observará que no contiene ningún cero. Puede uno pensar que está pues ante una plantilla o criptograma reducido de residuos. ¿Pero qué matriz base se ha utilizado para escribirlo? ¿Binaria? ¿Ternaria? ¿Cuaternaria? ¿De sexto orden? ¿De octavo? , Imposible contestar a estos interrogantes cuyo conocimiento es previo y necesario para poder plantearnos después cuál es el texto claro que puede esconder el criptograma. ¿Pero es que el anterior criptograma es un criptograma reducido de residuos, una plantilla? Anteriormente hemos argumentado que la ausencia de ceros nos ha llevado a suponer que pueda tratarse de una plantilla. Pero podemos probar que el anterior criptograma puede ser unas veces una plantilla y otras un criptograma final y que tanto en un caso como en otro la observación que aquí hemos hecho sobre la presencia de ceros (en el criptograma final) o su ausencia (en la plantilla) es una observación superflua. En efecto el *Teorema de los Residuos* nos permite

30

escribir plantillas con ceros incluidos y también hacer desaparecer todos los ceros de un criptograma final. Y lo que es más importante: *en todos los casos el criptograma resultante continúa conteniendo el texto claro que les interesa transmitir a los interlocutores.*

5

Finalmente, con respecto a la ventaja técnica de la inescrutabilidad del Criptograma de Residuos que permite un alto nivel de seguridad en la transmisión de información y datos, podemos demostrar que debido a la doble cardinalidad Aleph-0, la primera para el proceso que conduce a la *plantilla* y la segunda cuando se introduce la *clave de protocolo*, el Criptograma de Residuos es doblemente Criptograma Seguro de Shannon. Es decir, ya la *plantilla* o *criptograma reducido de residuos* es un Criptograma Seguro de Shannon. Justificaremos todavía más esta última conclusión con un ejemplo.

La mayor parte de los mensajes que se pueden escribir en un idioma que utiliza el alfabeto latino se puede hacer con 26 caracteres ortográficos, 10 numéricos, el espaciado y el punto. En total, 37 caracteres alfanuméricos. Supongamos pues que para escribir nuestro mensaje hacemos uso de la matriz alfanumérica de 40 caracteres que se muestra en la Tabla.8.

20

Tabla.8. Matriz alfanumérica de 40 caracteres

1	2	3	4	5	6	7	8	9	0	1
A	B	C	D	E	F	G	H	I	J	2
K	L	M	N	O	P	Q	R	S	T	3
U	V	W	X	Y	Z				.	4
1	2	3	4	5	6	7	8	9	10	

Como en los casos anteriores la última columna y la última fila sirven para localizar la posición de cada elemento en la matriz. Obsérvese que tres de los elementos de la matriz corresponden al espaciado, concretamente los elementos 47, 48 y 49 (el primer dígito expresa la fila y el segundo la columna).

25

Consideremos ahora que hemos enviado a nuestro interlocutor el criptograma de 48 dígitos que hemos escrito anteriormente. ¿Cuál es el texto claro que hemos transmitido con este criptograma si además afirmamos que es un criptograma reducido o plantilla? Imposible de saber si no damos como información adicional cual ha sido concretamente la tabla de equivalencias que hemos usado. En efecto, si hemos usado una tabla de equivalencias conformada a partir de la *matriz base de residuos numéricos binaria* de la Tabla.2, habremos tenido que elegir *una* de entre las $8! \approx 23 \times 10^{129}$ posibilidades de *matrices base reordenada de residuos numéricos binarias*. Escogida una de éstas, el número de elementos de esta matriz por cada elemento de la matriz alfanumérica de 40 caracteres es de 2 y todavía sobra uno. ¿Y si hubiésemos elegido una tabla de equivalencias conformada a partir de la *matriz base de residuos numéricos ternaria* de la Tabla.3? Entonces habremos tenido que elegir *una* de entre las $729! \approx 68 \times 10^{1770}$ posibilidades de *matrices base reordenada de residuos numéricos ternarias*. Escogida una, en este caso, el número de elementos de esta matriz por cada elemento de la matriz alfanumérica de 40 caracteres es de 18 y todavía sobran nueve. ¿Y si la tabla de equivalencias se ha conformado a partir de la *matriz base de residuos numéricos cuaternaria*? En este caso habremos tenido que elegir *una* de entre las $6561! \approx 203 \times 10^{22194}$ posibilidades de *matrices base reordenada de residuos numéricos cuaternarias*. Escogida una, en este caso, el número de elementos de esta matriz por cada elemento de la matriz alfanumérica de 40 caracteres es de 164 sobrando uno. No seguimos ya. Pero esto significa que cualquiera de las frases que a continuación podemos leer, entre una cantidad ingente de textos que podríamos seguir añadiendo, es candidata a ser el texto claro que realmente hemos querido transmitir:

**EJEMPLO.1. Frases para matriz base de residuos numéricos binaria
(24 caracteres)**

FUMATE EL PURO CON PAQUI	CUI PRODEST SCELUS MARIA
ES MES UTIL CRIPTOGRAPHY	JUST ESTA CAMINO DE LUGO
FELISA Y SU MULO JOSEFIN	IRAN HOMBRES MUY HABILES
TOMASO DE FORMENT NI GRA	COMPRE LA FINCA DE RUBIO
GAT DE VINT UNGLES QUICO	BARCELONA 32 SPORTING 19
QUI SAP QUAN SORTIRE MUT	---

**EJEMPLO.2. Frases para la matriz base de residuos numéricos ternaria
(16 caracteres)**

MAÑANA NOS VEMOS	
ME DUELE LA MANO	THEORY OF MATTER
ETS UN HOME FORT	THE OTHER PAPERS
VIGILA SUS ACTOS	LES PLUS SIMPLES
ENS VEGEM DIJOUS	DANS CE CHAPITRE
CON DON FABRIZIO	ETCETERA ES ETC
PESA 16000 KILOS	---

EJEMPLO.3. Frases para la matriz base de residuos numéricos cuaternaria (12 caracteres.)

5	BEUREM AIGUA	IS A DENSITY
	VINE A LES 6	IS INVARIANT
	DONARE EUROS	DI LAMPEDUSA
	TOMALA GUAPA	ANGELICA MIA
10	PONTE COMODO	UNE EQUATION
	NOS CALLAMOS	-----
	THE UNIVERSE	

15 Sin perjuicio de mantener mayores desarrollos, todavía cabrían aquí las matrices de sexto orden (8 caracteres por frase), de octavo orden (6 caracteres), de duodécimo orden (4 caracteres), de décimo sexto orden (3 caracteres), de vigésimo cuarto orden (2 caracteres) y de cuadragésimo octavo orden (1 carácter).

20 ¿Cuál es la frase que hemos decidido transmitir? Imposible saberlo si no añadimos como información adicional de cuál ha sido la tabla de equivalencias concreta que hemos usado.

25 A partir de aquí podemos hacer uso de la doble seguridad de Criptograma Seguro de Shannon, aplicándole a la plantilla la clave de protocolo que pone en marcha el algoritmo de codificación para conseguir el que aquí hemos denominado *Criptograma final de residuos*. Obviamente, esto significa que la plantilla anterior la podemos transformar en infinidad de criptogramas finales, todos conteniendo el mismo texto claro.

30

35

Mejor manera de realizar la invención

5 En conclusión, para la mejor realización de la presente invención deben de ser empleados los siguientes elementos o medios técnicos por orden secuencial y sucesivo: 1°. *Una matriz alfanumérica*, 2°. *una matriz base de residuos numéricos*, 3°. *una clave de equivalencias*, 4°. *una tabla de equivalencias*, 5°. *un criptograma reducido de residuos o plantilla*, 6°. *cuna clave de protocolo*, 7°. *un algoritmo de codificación*, 8°. *un criptograma final de residuos* y 9°. *un algoritmo de decodificación*.

10

 Puede también, llevarse a la práctica un segundo modo de realización más simplificando suprimiendo las etapas de, *una clave de equivalencias* y *una*

15 *tabla de equivalencias*, menos operativo y más vulnerable, pero manteniendo el cumplimiento de los presupuestos de Shannon, mediante el siguiente orden secuencial y progresivo: 1°. *Una matriz alfanumérica*, 2°. *una matriz base de residuos numéricos*, 3°. *un criptograma reducido de residuos o plantilla*, 4°. *una clave de protocolo*, 5°. *un algoritmo de codificación*, 6°. *un criptograma final de*

20 *residuos* y 7°. *un algoritmo de decodificación*.

25

30

REIVINDICACIONES

5 1. - Procedimiento de doble criptograma simétrico de seguridad de Shannon por codificación de información para transmisión telemática y electrónica fiables, rápidas y seguras para aplicación industrial en los sectores privados y públicos de las telecomunicaciones, informática, Defensa nacional, programas de ordenador, transacciones de pagos electrónicos y operaciones
10 bancarias, criptografía de obras musicales y audiovisuales, y firmas y certificados digitales **caracterizado porque** comprende los siguientes elementos o medios técnicos por orden secuencial y sucesivo: 1º. Una matriz alfanumérica, 2º. una matriz base de residuos numéricos, 3º. una clave de equivalencias, 4º. una tabla de equivalencias, 5º. un criptograma reducido de
15 residuos o plantilla, 6º. una clave de protocolo, 7º. un algoritmo de codificación, 8º. un criptograma final de residuos y 9º. un algoritmo de decodificación.

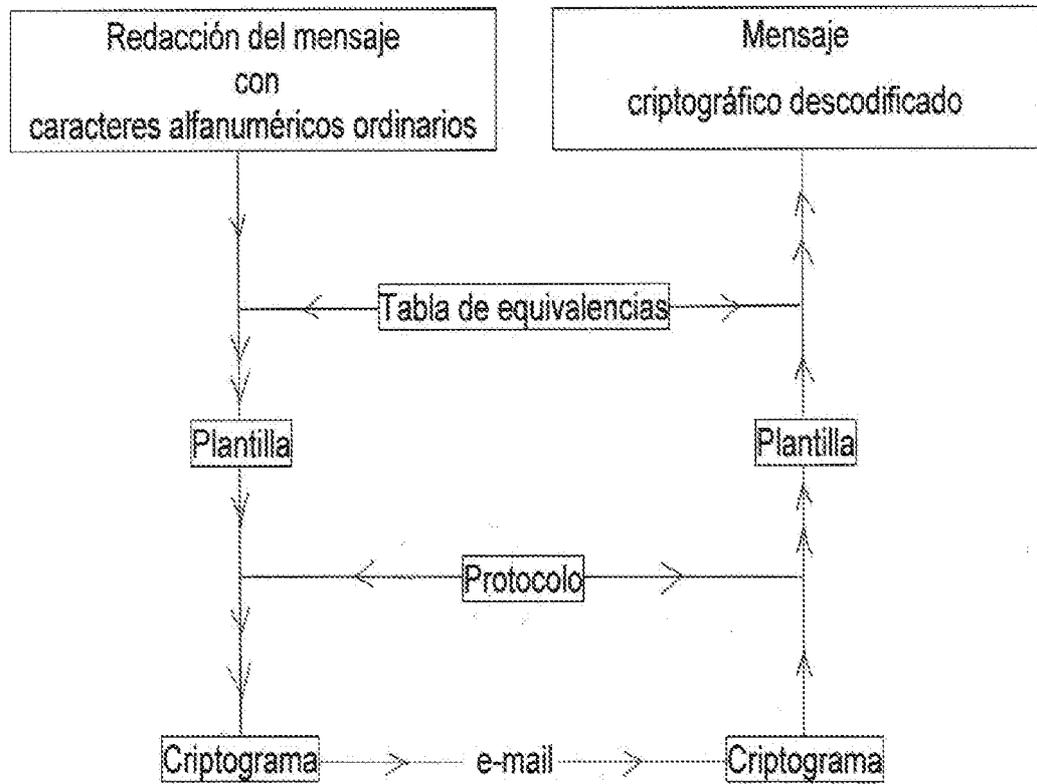
2. - Procedimiento de doble criptograma simétrico de seguridad de Shannon por codificación de información para transmisión telemática y electrónica fiables, rápidas y seguras para aplicación industrial en los sectores privados y públicos de las telecomunicaciones, informática, Defensa nacional, programas de ordenador, transacciones de pagos electrónicos y operaciones bancarias, criptografía de obras musicales y audiovisuales, y firmas y
20 certificados digitales simplificado conforme a la Reivindicación.1 **caracterizado porque** se suprimen los siguientes elementos o medios en el orden secuencial y sucesivo: 3º. una clave de equivalencias y 4º. una tabla de equivalencias,

30

DIBUJOS

EMISOR

RECEPTOR



INTERNATIONAL SEARCH REPORT

International application No.
PCT/ES2011/070331

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/06 (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC, INVENES, WPI, XPMISC, XPI3E, XPIETF, XPIEE, XPESP, NPL, COMPDX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2008076861 A2 (QUALCOMM INC; GANTMAN ALEXANDER; ROSE GREGORY GORDON; CHOI JAE-HEE ; NOERENBERG JOHN W II) 26-06-2008,	1-2
A	US 2007064933 A1 (LUCENT TECHNOLOGIES INC) 22-03-2007,	1
A	01-01-1997, Highland H J, "Data Encryption: A Non-Mathematical Approach" COMPUTERS & SECURITY, ELSEVIER SCIENCE PUBLISHERS, I, Vol. 16, Nr: 5, Págs: 369 - 386 ISSN 0167-4048, doi:10.1016/S0167-4048(97)82243-2	1

Further documents are listed in the continuation of Box C.

See patent family annex.

<p>* Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance.</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure use, exhibition, or other means.</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other documents , such combination being obvious to a person skilled in the art</p> <p>"&" document member of the same patent family</p>
--	---

Date of the actual completion of the international search
02/02/2012

Date of mailing of the international search report
(07/02/2012)

Name and mailing address of the ISA/

OFICINA ESPAÑOLA DE PATENTES Y MARCAS
Paseo de la Castellana, 75 - 28071 Madrid (España)
Facsimile No.: 91 349 53 04

Authorized officer
M. Muñoz Sanchez

Telephone No. 91 3495349

INTERNATIONAL SEARCH REPORT

International application No.

Information on patent family members

PCT/ES2011/070331

Patent document cited in the search report	Publication date	Patent family member(s)	Publication date
WO2008076861 A	26.06.2008	TW200840263 A EP2100405 A EP20070869269 KR20090100399 A CN101558598 A US2010034385 A JP2010515083 A	01.10.2008 16.09.2009 14.12.2007 23.09.2009 14.10.2009 11.02.2010 06.05.2010
-----	-----	-----	-----
US2007064933 A	22.03.2007	US7801307 B WO2007120169 A KR20080031906 A EP1927212 A EP20060851115 JP2009503580 A CN101461173 A	21.09.2010 25.10.2007 11.04.2008 04.06.2008 17.07.2006 29.01.2009 17.06.2009
-----	-----	-----	-----

INFORME DE BÚSQUEDA INTERNACIONAL

Solicitud internacional nº
PCT/ES2011/070331

A. CLASIFICACIÓN DEL OBJETO DE LA SOLICITUD
H04L9/06 (2006.01)

De acuerdo con la Clasificación Internacional de Patentes (CIP) o según la clasificación nacional y CIP.

B. SECTORES COMPRENDIDOS POR LA BÚSQUEDA

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)
H04L

Otra documentación consultada, además de la documentación mínima, en la medida en que tales documentos formen parte de los sectores comprendidos por la búsqueda

Bases de datos electrónicas consultadas durante la búsqueda internacional (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

EPODOC, INVENES, WPI, XPMISC, XPI3E, XPIETF, XPIEE, XPESP, NPL, COMPDX

C. DOCUMENTOS CONSIDERADOS RELEVANTES

Categoría*	Documentos citados, con indicación, si procede, de las partes relevantes	Relevante para las reivindicaciones nº
A	WO 2008076861 A2 (QUALCOMM INC; GANTMAN ALEXANDER; ROSE GREGORY GORDON; CHOI JAE-HEE ; NOERENBERG JOHN W II) 26-06-2008,	1-2
A	US 2007064933 A1 (LUCENT TECHNOLOGIES INC) 22-03-2007,	1
A	01-01-1997, Highland H J, "Data Encryption: A Non-Mathematical Approach" COMPUTERS & SECURITY, ELSEVIER SCIENCE PUBLISHERS, I, Vol. 16, Nr: 5, Págs: 369 - 386 ISSN 0167-4048, doi:10.1016/S0167-4048(97)82243-2	1

En la continuación del recuadro C se relacionan otros documentos Los documentos de familias de patentes se indican en el anexo

* Categorías especiales de documentos citados:	"T"	documento ulterior publicado con posterioridad a la fecha de presentación internacional o de prioridad que no pertenece al estado de la técnica pertinente pero que se cita por permitir la comprensión del principio o teoría que constituye la base de la invención.
"A" documento que define el estado general de la técnica no considerado como particularmente relevante.	"X"	documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado.
"E" solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior.	"Y"	documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.
"L" documento que puede plantear dudas sobre una reivindicación de prioridad o que se cita para determinar la fecha de publicación de otra cita o por una razón especial (como la indicada).	"&"	documento que forma parte de la misma familia de patentes.
"O" documento que se refiere a una divulgación oral, a una utilización, a una exposición o a cualquier otro medio.		
"P" documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada.		

Fecha en que se ha concluido efectivamente la búsqueda internacional.
02/02/2012

Fecha de expedición del informe de búsqueda internacional.
07-FEBRERO-2012 (07/02/2012)

Nombre y dirección postal de la Administración encargada de la búsqueda internacional
OFICINA ESPAÑOLA DE PATENTES Y MARCAS
Paseo de la Castellana, 75 - 28071 Madrid (España)
Nº de fax: 91 349 53 04

Funcionario autorizado
M. Muñoz Sanchez
Nº de teléfono 91 3495349

INFORME DE BÚSQUEDA INTERNACIONAL

Solicitud internacional nº

Informaciones relativas a los miembros de familias de patentes

PCT/ES2011/070331

Documento de patente citado en el informe de búsqueda	Fecha de Publicación	Miembro(s) de la familia de patentes	Fecha de Publicación
WO2008076861 A	26.06.2008	TW200840263 A EP2100405 A EP20070869269 KR20090100399 A CN101558598 A US2010034385 A JP2010515083 A	01.10.2008 16.09.2009 14.12.2007 23.09.2009 14.10.2009 11.02.2010 06.05.2010
----- US2007064933 A	----- 22.03.2007	----- US7801307 B WO2007120169 A KR20080031906 A EP1927212 A EP20060851115 JP2009503580 A CN101461173 A	----- 21.09.2010 25.10.2007 11.04.2008 04.06.2008 17.07.2006 29.01.2009 17.06.2009
-----	-----	-----	-----