novática
UPGRADE Revista de la Asociación de Técnicos de Informática

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática). ***Novática*** edita también ***Upgrade***, revista digital de **CEPIS** (*Council of European Professional Informatics Societies*), en lengua inglesa, y es miembro fundador de **UPENET** (*UPGRADE European NETwork*)

<http://www.ati.es/novatica/>
<http://www.upgrade-cepis.org/>

ATI es miembro fundador de **CEPIS** (*Council of European Professional Informatics Societies*) y es representante de España en **IFIP** (*International Federation for Information Processing*); tiene un acuerdo de colaboración con **ACM** (*Association for Computing Machinery*), así como acuerdos de vinculación o colaboración con **AdaSpain**, **AI2** y **ASTIC.**

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Padilla 66, 3º, dcha., 28006 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Composición, Edición y Redacción ATI Valencia
Av. del Reino de Valencia 23, 46005 Valencia
Tlfn./fax 963330392 <secreval@ati.es>
Administración y Redacción ATI Cataluña
Via Laietana 41, 1º, 1ª, 08003 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>
Redacción ATI Andalucía
Isaac, Newton, s/n, Ed. Sadiel,
Isla Cartuja 41092 Sevilla, Tlfn./fax 954460779 <secreand@ati.es>
Redacción ATI Aragón
Lagasca, 9, 3-B, 50006 Zaragoza.
Tlfn./fax 976235181 <secreara@ati.es>
Redacción ATI Asturias-Cantabria <gp-astucant@ati.es>
Redacción ATI Castilla-La Mancha <gp-clmancha@ati.es>
Redacción ATI Galicia
Recinto Ferial s/n, 36540 Silleda (Pontevedra)
Tlfn.986581413; fax 986580162 <secregal@ati.es>
Suscripción y Ventas
<http://www.ati.es/novatica/interes.html>,o en ATI Cataluña o ATI Madrid
Publicidad
Padilla 66, 3º, dcha., 28006 Madrid
Tlnf.914029391; fax.913093685 <novatica.publicidad@ati.es>
Imprenta
Derra,S.A., Juan de Austria 66, 08005 Barcelona.
Depósito legal: B.15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: Antonio Crespo Foix / © ATI 2004
Diseño: Fernando Agresta / © ATI 2004

Nº 172, noviembre-diciembre 2004, año XXX

sumario

Monografía del próximo número: "*XML*"

Una breve panorámica de la Criptografía

Arturo Ribagorda Garnacho[1], Javier Areitio Bertolín[2]
[1] Depto. de Informática, Universidad Carlos III de Madrid; [2] Universidad de Deusto (Bilbao)

<arturo@inf.uc3m.es>, <jareitio@eside.deusto.es>

Resumen: *en este artículo se describen brevemente la historia y las características de la criptografía, disciplina cuyo fin último es garantizar la confidencialidad de la información, y que se ha convertido en una herramienta decisiva para garantizar la seguridad de la información en nuestras sociedades tecnificadas.*

Palabras clave: *confianza, criptografía, seguridad, información.*

Autores

Arturo Ribagorda Garnacho es Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid y Doctor en Informática por la misma Universidad. Es Catedrático de Universidad y Director del Depto. de Informática de la Universidad Carlos III de Madrid, de cuya Escuela Politécnica Superior ha sido director. Su actividad académica se centra en la Seguridad de las Tecnologías de la Información, campo en el que participa en diversos proyectos de investigación nacionales y europeos, ha publicado más de 100 artículos en revistas nacionales e internacionales, y presentado numerosas ponencias en congresos. Asimismo es autor de cuatro libros sobre la citada materia.

Javier Areitio Bertolín es Doctor en Física Aplicada por la Universidad del País Vasco. Es Catedrático del Departamento de Telecomunicaciones de la Facultad de Ingeniería de la Universidad de Deusto (Bilbao), siendo Director del Grupo de Investigación Redes y Sistemas. Es Miembro de CORDIS (Community Research and Development Information Service, European Commission). Ha sido Coordinador Técnico del Proyecto COMMETT "Information and Computer Security" ICS/EU y Tutor para la AECI (Agencia Española de Cooperación Internacional). Su principal campo de investigación es la Seguridad-Criptografía aplicada a las Tecnologías de la Información y las Comunicaciones, un campo donde ha trabajado en numerosos proyectos de investigación nacionales e internacionales. Es ponente, moderador y evaluador habitual de Congresos, Seminarios y Symposium y es autor de numerosos artículos científicos en revistas técnicas. Es autor de varios libros técnicos sobre Seguridad en Redes de Computadoras, Criptografía y Criptoanálisis. Actualmente coordina algunos proyectos aplicados en colaboración con varias empresas españolas y universidades europeas. Es miembro de diversas asociaciones españolas e internacionales, por ejemplo ATI, donde es coordinador de la Sección Técnica "Seguridad" de su revista ***Novática***.

1. Concepto y evolución

Acciones tan cotidianas hoy en día como efectuar una llamada telefónica desde un móvil, realizar una operación con una tarjeta de crédito o débito, conectarse a un servidor seguro u otras muchas, conllevan el concurso de técnicas criptográficas, que transforman los datos para ocultar su significado e imposibilitar su alteración fraudulenta.

Ello no obstante, la criptografía (del griego *kriptos*, oculto, y *grafos* , escritura), era hasta hace bien poco --no más de treinta años-- objeto de interés sólo en reducidos círculos --aureolados de misterio-- como la inteligencia o la diplomacia. La razón de este súbito y generalizado interés se encuentra en la importancia adquirida en nuestros días por la información, que se ha convertido en el centro y motor del mundo en que vivimos. No puede por tanto extrañar que la seguridad --y su principal soporte: la criptografía-- haya devenido en un tema de capital importancia para nuestras sociedades.

En una primera aproximación, la criptografía se puede definir como la disciplina que estudia los principios, métodos y medios de transformar los datos para ocultar su significado. Así pues, según esta aproximación, es una disciplina cuyo fin último es garantizar la confidencialidad de la información. Al proceso consistente en encubrir la información (que requiere del conocimiento de una información secreta denominada clave de cifrado) se le denomina **cifrado**, conociéndose como **descifrado** al proceso inverso (que igualmente precisa del conocimiento de una clave de descifrado, igual o distinta de la anterior).

Así, los primeros ejemplos ampliamente documentados de métodos criptográficos (procedentes de la Grecia y Roma Clásicas, aunque hay esporádicos ejemplos de usos aun anteriores [1]) tenían dicho objetivo. Todavía a día de hoy solemos ilustrar los métodos criptográficos con el llamado cifrado César --nombrado así en honor de Julio César, primero en utilizarlo durante el siglo I aC--, consistente en una sustitución cíclica de cada letra del alfabeto por aquella situada tres posiciones después de ella.

Sin embargo, en nuestros días las aplicaciones de la criptografía se han ampliado notoriamente, proporcionando también pruebas de integridad, autenticación y no repudio [2]. Por ello, en el presente, se puede definir con más precisión como la materia estudia los principios, métodos y medios de transformar los datos para ocultar la información contenida en ellos, garantizar su integridad, establecer su autenticidad y prevenir su repudio.

Por otra parte, la disciplina contraria, es decir aquella que investiga los métodos de descubrir informaciones cifradas sin el conocimiento de la clave de descifrado se denomina **criptoanálisis**. Finalmente, el estudio de ambas --criptografía y criptoanálisis-- constituye el objetivo de la rama de saber denominada criptología.

2. Los sistemas criptográficos

En la actualidad, los sistemas criptográficos o criptosistemas son muy complejos y comportan, en el extremo emisor, el empleo de un dispositivo criptográfico, o cifrador, hardware o software (en esencia un algoritmo matemático extraordinariamente complejo) que, con ayuda de una clave de cifrado, k_E, transforma un texto --llamado "en claro"-- en otro ininteligible denominado texto cifrado. En el extremo receptor un descifrador, con el auxilio de una clave de descifrado, k_D, invierte el proceso anterior obteniendo nuevamente el texto en claro a partir del criptograma (**figura 1**). Eventualmente, el cifrador incorpora un generador de claves, así como el criptosistema incluye un protocolo de intercambio de éstas.

Evidentemente, la transformación de cifrado debe ser computacionalmente irreversible, a no ser que se posea una información adicional: la **clave de descifrado**.

Cabe destacar que desde tiempo inmemorial los sistemas empleados han venido usando iguales claves de cifrado que de descifrado (o bien, de ser distintas, del conocimiento de una se podía deducir la otra), por lo que su invulnerabilidad dependía, en primera instancia, del mantenimiento en secreto de di-

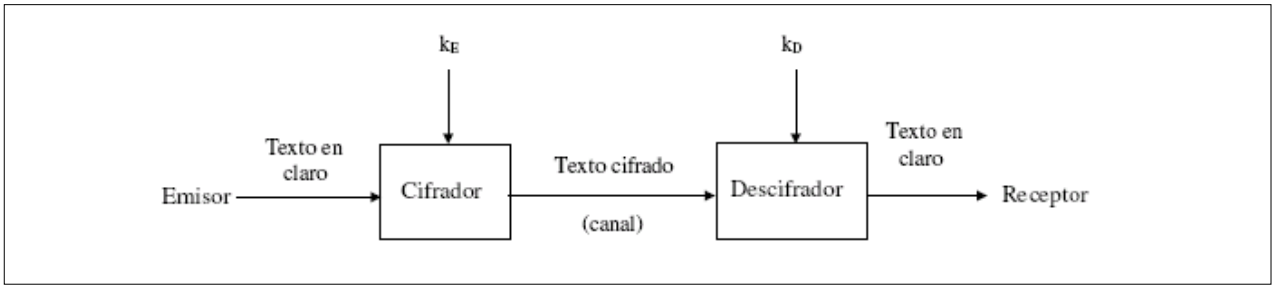

Figura 1. Esquema de un sistema de cifrado.

cha clave. Consiguientemente, ésta debía transferirse del emisor al receptor a través de un canal seguro, obviamente diferente del canal del criptosistema, que por hipótesis se suponía amenazado por posibles interceptadores. Estos criptosistemas clásicos son los conocidos como de **clave secreta** o **simétricos**.

Además de la ventaja que les reporta su simetría, que conlleva que los papeles del emisor y receptor sean fácilmente reversibles, también aportan al receptor la garantía de que el emisor es quien dice ser y no un impostor. No obstante, presentan la importante desventaja de exigir un canal seguro para distribuir las claves, canal evidentemente distinto de aquél por el que transita el texto cifrado.

Son muy numerosos los ejemplos de algoritmos de cifrado de este tipo, sobresaliendo el DEA (base del antiguo estándar federal estadounidense de cifrado DES, *Data Encryption Standard*), el IDEA (*International Data Encryption Standard*), el A-5 (empleado en la telefonía móvil celular GSM), la familia RC-X (con X= 2, 4, 5, 6) y, muy recientemente el AEA (*Advanced Encryption Algorithm*), base del estándar federal estadounidense AES (*Advanced Encryption Standard*).

Sin embargo en 1976 Diffie y Hellman [3] demostraron la posibilidad de construir criptosistemas que no precisaban transferir una clave secreta entre el emisor y el receptor, previamente al establecimiento de una transmisión cifrada. En estos criptosistemas aquél que desee recibir textos cifrados hace de general conocimiento su clave de cifrado, denominada por este motivo **pública** (en lo que sigue k_u). Por el contrario, mantiene a buen recaudo la correspondiente clave de descifrado, denominada **privada** (en adelante k_v), de modo que sólo él la conozca. Obviamente ambas claves no son independientes, pero del conocimiento de la pública no se infiere la privada, salvo que se disponga de innumerables recursos o de tiempo ilimitado.

Así, con estos criptosistemas cuando un emisor, A, necesite remitir una información cifrada a B, cifra las misma con la clave pública de este último. Cuando B recibe esta información sólo tiene que descifrarla con su clave privada. De este modo, aunque alguien intercepte la información no podrá descifrarla al no disponer de la clave privada, ni poderla obtener a partir de la pública. Naturalmente, si B desea contestar a A deberá cifrar la respuesta con la clave pública de A, descifrándola éste con su privada.

Estos criptosistemas, denominados de **clave pública** (pues la de cifrado debe ser de universal conocimiento) o **asimétricos** (por la asimetría expuesta en la manera de cifrar según que sea A el emisor o el receptor), soslayan la desventaja inherente a los simétricos --la construcción o hallazgo de un canal seguro--, pues ahora la clave de cifrado, clave pública, puede ser conocida universalmente. Empero, por ser mucho más lentos que los de clave secreta de similar robustez, se emplean exclusivamente para cifrar informaciones de exiguo volumen, como claves secretas, o bien para firmar digitalmente el resumen --de pequeño tamaño-- de un documento (lo que se denomina **firma digital** del documento).

En la práctica cotidiana, el único algoritmo de clave pública empleado para cifrar, no así para firmar, es el RSA, ideado por los criptógrafos estadounidenses Rivest, Shamir y Adlemann, y cuyas iniciales constituyen su sigla en 1997 [4].

3. Conclusión

En resumen, el milenario arte de la criptografía se ha convertido en una disciplina científica y técnica de capital importancia para el desarrollo de las sociedades, a las que suministra garantías de confidencialidad e integridad de las informaciones, proporciona pruebas de la autenticación de los intervinientes en una comunicación y evita que ninguno de ellos pueda repudiar haber participado en la misma. En resumen, nos da la seguridad y confianza que todos requerimos para adentrarnos en esta nueva era de la información.

Referencias

[1] David Kahn. *The Codebreakers*: The Story Of Secret Writing. MacMillan, 1967

[2] Gustavus J. Simmons. *Contemporary Cryptology : The Science of Information Integrity*. Wiley-IEEE Computer Society Pr, 27 January, 1999.

[3] Whitfield Diffie, Martin E. Hellman. "New Directions in Cryptography", *IEEE Transactions in Information Theory*, vol. IT-22, pp. 664-654. Noviembre de 1976

[4] R. L. Rivest, A. Shamir, L. Adleman. A Method for Obtaining Digital Signature and Public-Key cryptosystems". *Communications of the ACM*, vol. 21, nº 2, pp. 120-126. Febrero de 1978.