Seguridad y Protección de Sistemas Informáticos

Fco. Javier Lobillo Borrero

Departamento de Álgebra, Universidad de Granada

Curso 2017/2018

Índice

Data hiding I

Data (o *information*) *hiding* es un término general que engloba a un amplio espectro de problemas que comprenden técnicas para incrustar mensajes en otro contenido.

Marcas de agua Es la práctica que consiste en alterar un trabajo de manera imperceptible para incrustar un mensaje sobre dicho trabajo.

Esteganografía Es la práctica que consiste en alterar un trabajo de manera indetectable para incrustar un mensaje secreto.

Data hiding II

Cuadro: Tipos de Data Hiding

	Mensaje dependiente	Mensaje independiente
Existencia oculta	Marcas ocultas	Esteganografía
Existencia conocida	Marcas de agua	Otros tipos

- Detección de filtraciones.
- Espíonaje.
- Contenido de museos / agencias.
- Señal horaria en señales de radio.

Data hiding III

Un esquema de ocultación de información consta de cinco elementos:

- Un conjunto $\mathcal{C}$ de posibles trabajos,
- un conjunto $\mathcal{M}$ de posibles mensajes,
- un conjunto $\mathcal{K}$ de posibles claves,
- una función $\text{inc} : \mathcal{C} \times \mathcal{M} \times \mathcal{K} \to \mathcal{C}$,
- una función $\text{rec} : \mathcal{C} \times \mathcal{C} \times \mathcal{K} \to \mathcal{M}$

satisfaciendo para cada $c \in \mathcal{C}$, $m \in \mathcal{M}$ y $k \in \mathcal{K}$,

$$\text{rec}(\text{inc}(c, m, k), c, k) = m.$$

Data hiding IV

La función de recuperación puede ser independiente del trabajo original, es decir,

$$\mathrm{rec}(d, c_1, k) = \mathrm{rec}(d, c_2, k)$$

para cualesquiera $c_1, c_2, d \in \mathcal{C}$ y $k \in \mathcal{K}$. En este caso podemos ver $\mathrm{rec} : \mathcal{C} \times \mathcal{K} \to \mathcal{M}$, satisfaciendo para cada $c \in \mathcal{C}$, $m \in \mathcal{M}$ y $k \in \mathcal{K}$,

$$\mathrm{rec}(\mathrm{inc}(c, m, k), k) = m.$$

Data hiding V

- Normalmente el uso de la clave se deja a la incorporación de técnicas criptográficas, por lo que prescindiremos habitualmente de ellas.
- En el mundo digital $\mathcal{C} = \mathcal{A}^n$ y $\mathcal{M} = \mathcal{A}^k$ para cierto alfabeto finito $\mathcal{A}$, que normalmente es $\mathcal{A} = \mathbb{Z}_q$ o $\mathcal{A} = \mathbb{F}_{2^t}$. De esta forma

$$\text{inc} : \mathcal{A}^n \times \mathcal{A}^k \to \mathcal{A}^n$$

y

$$\text{rec} : \mathcal{A}^n \times \mathcal{A}^n \to \mathcal{A}^k \quad \text{o} \quad \text{rec} : \mathcal{A}^n \to \mathcal{A}^k$$

Data hiding VI

En $\mathcal{A}^n$ consideraremos la distancia de Hamming: para cualesquiera $x = (x_0, \ldots, x_{n-1}), y = (y_0, \ldots, y_{n-1}) \in \mathcal{A}^n$,

$$\mathrm{d_H}(x, y) = \#\{0 \leq i \leq n-1 \mid x_i \neq y_i\},$$

es decir, el número de posiciones en que x e y difieren.

Si $\mathcal{A} = \mathbb{F}_q$, se define el peso de Hamming de $x = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_q^n$ como

$$\mathrm{w_H}(x) = \mathrm{d_H}(x, 0) = \#\{0 \leq i \leq n-1 \mid x_i \neq 0\}.$$

Observemos que

$$\mathrm{d_H}(x, y) = \mathrm{w_H}(x - y).$$

Watermarks: Antecedentes I

Marcas de agua

- Aclarado de papel: Fraude en emisión de monedas
- Información destacando letras de un libro.
- Código de identificación en grabaciones musicales insertando muescas a muy baja frecuencia (1 kHz).
- Marcas de agua digitales: sistemas de protección anticopia.

Watermarks: Antecedentes II

Esteganografía

- Tatuajes en la cabeza.
- Tablas de madera y cera.
- Accesorios de indumentaria (sobre todo mujeres).
- Tamaño de las letras.
- Acrósticos (esteganografía lingüística).
- Cambios en la tipografía (Francis Bacon).
- Esteganografía digital.

Watermarks: Características I

Las marcas de agua buscan asociar información sobre un trabajo al mismo. ¿Por qué no usar otras técnicas más sencillas para el mismo fin?

Porque...

- son imperceptibles,
- son inseparables,
- sufren el mismo tipo de transformaciones que el trabajo en el que están incrustadas.

Watermarks: Aplicaciones I

Seguimiento de emisiones multimedia: Identificar cuándo y dónde se han emitido los trabajos reconociéndolos por las marcas de agua incrustadas en ellos. Otras soluciones, como bases de datos de contenidos o analizadores semánticos son tremendamente costosos e ineficientes.

Identificación del propietario: Incrustación de la identidad del poseedor de los derechos del trabajo como una marca de agua. Los métodos legalmente establecidos son fácilmente eliminables voluntaria o involuntariamente.

Prueba de propiedad: Uso de marcas de agua para proporcionar evidencias en caso de disputas sobre la propiedad. Complementa a la aplicación anterior. Otros sistemas, normalmente basados en la creación de repositorios centralizados, son caros tanto para el proveedor como para el usuario.

Seguimiento de las transacciones: Uso de las marcas de agua para identificar personas que obtienen el contenido legalmente pero lo distribuyen ilegalmente. Normalmente se logra insertando marcas de agua con un número de serie propio para cada copia.

Watermarks: Aplicaciones II

Autenticación del contenido: Incrustar una firma digital o un MAC para más tarde comprobar que el contenido no ha sido alterado. Sin la incrustación pueden ser fácilmente borradas. Esto incluye, por ejemplo, vídeos de vigilancia. La aplicación de filtros a contenido multimedia puede ser más fácilmente detectable si existen marcas de agua.

Control de copia: La criptografía es la mejor herramienta para proteger el acceso a contenido registrado. Sin embargo, una vez descifrado es fácilmente duplicable. Uso de marcas de agua puede indicar al equipo grabador qué contenido no debe ser grabado.

Control de dispositivos: Uso de marcas de agua para que los dispositivos reacciones ante el contenido mostrado.

Mejoras heredadas: Uso de marcas de agua para mejorar la funcionalidad de sistemas existentes.

Watermarks: Propiedades I

La idoneidad de un sistema de marcas de agua para una aplicación concreta puede ser juzgada en términos de las siguientes propiedades.

Incrustación efectiva: Probabilidad de una incrustación satisfactoria dentro de un trabajo aleatoriamente seleccionado. Lo deseable es el 100 %, aunque el coste de garantizarla puede ser incompatible con otras propiedades. Puede ser calculada de forma analítica o mediante una aproximación estadística.

Fidelidad: La calidad en la percepción en el contenido con la marca de agua incrustada. Puede depender de la posible degradación de la señal desde que se emite hasta que llega al receptor.

Datos cargados: Cantidad de información que una marca de agua puede incluir. Se mide en bits, y depende del uso. Por ejemplo, el control de copia no requiere más de 8 bits cada 10 segundos de música o 5 minutos de vídeo. El seguimiento de emisiones requiere 24 bits en el primer segundo.

Watermarks: Propiedades II

Detección ciega o informada: Si el recuperador puede detectar una marca de agua en un trabajo sin tener información adicional o si necesita alguna información relacionada con la versión original del trabajo. La aplicación puede ser crucial a la hora de establecer el tipo de marca de agua.

Tasa de falsos positivos: Frecuencia con la debemos esperar una recuperación falsa de una marca de agua en un contenido que carece de ella. Como variable aleatoria podemos considerar tanto los trabajos como los mensajes. El diseño con mayor o menor tasa depende, como siempre, de la aplicación.

Robustez: La habilidad de la marca de agua para sobrevivir al procesado normal del contenido. Hay ocasiones en que lo interesante es la ausencia de esta propiedad.

Seguridad: Habilidad de la marca de agua para resistir ataques hostiles. Pueden ser de tres tipos: Borrados, incrustación (activos) o detección (pasivo) no autorizados.

Modificación y múltiples marcas de agua: Posibilidad de cambiar la marca de agua incrustada o incluir varias marcas.

Coste: Coste computacional del incrustador y del recuperador.

Watermarks: Observaciones I

- Las propiedades requeridas de una marca de agua dependen de la aplicación.
- Benchmarking es un medio razonable para comparar sistemas de marcas de agua. Sin embargo, ninguna referencia concreta es probable que sea relevante para todas las aplicaciones.
- Los sistemas de marcas de agua deben probarse con conjuntos grandes de datos.
- Si un sistema de marca de agua se mejora de manera que tenga un mejor rendimiento en una propiedad, a menudo produce mejoras de rendimiento en otras propiedades.

Esteganografía: Características I

- La esteganografía es una herramienta para la privacidad.
- La esteganografía se considera rota si simplemente se detecta la mera existencia del mensaje.
- La indetectabilidad suele garantizarse con mensajes suficientemente cortos.
- Los sistemas esteganográficos deben comprobarse mediante ataques ciegos y dirigidos, realizados sobre conjuntos de datos grandes y diversos.
- Algunas aplicaciones de la esteganografía pueden obtenerse con otras tecnologías. La principal ventaja radica en que la propia existencia de la comunicación se mantiene en secreto.

Esteganografía: Aplicaciones I

- Espionaje.
- Comunicaciones encubiertas entre disidentes.
- Comunicaciones encubiertas entre criminales.

Esteganografía: Propiedades I

Las propiedades comentadas sobre las marcas de agua tienen la siguiente interpretación para sistemas esteganográficos.

Incrustación efectiva: No es relevante.

Fidelidad: No necesariamente relevante.

Capacidad esteganográfica: Es el equivalente a los datos cargados. Cantidad de bits que pueden ser ocultados en un trabajo de tal manera que la probabilidad de detección por parte de un adversario sea despreciable.

Capacidad de incrustación: Máximo número de bits que pueden ser ocultados en un trabajo dado.

Eficiencia de la incrustación: Número de bits del mensaje incrustados por unidad de distorsión.

Recuperación ciega o informada: Depende de si el receptor dispone o no de una copia original del trabajo.

Estegoanálisis del sistema: Se refiere a ataques que se basan en debilidades de la implementación en lugar de en la naturaleza de la incrustación.

Estegoanálisis ciego: Métodos de detección independientes del sistema esteganográfico usado.

Esteganografía: Propiedades II

Estegoanálisis dirigido: Métodos de ataque diseñados contra sistemas esteganográficos concretos.

Indetectabilidad estadística: Probabilidad de detectar un trabajo incrustado basándose en las distribuciones de probabilidad de trabajos con y sin incrustación.

Tasa de falsa alarma: Probabilidad de que un algoritmo de análisis detecte la presencia de de un mensaje incrustado cuando éste no está.

Robustez: Normalmente este paso se obvia en la esteganografía, pues en la actualidad los sistemas digitales carecen de degradación.

Seguridad: Se suele evaluar en términos de ataques pasivos.

Modificación y múltiples mensajes: No es aplicable.

Coste: No es relevante.

Estegosistemas: Reglas de selección

Normalmente no se emplea todo el mensaje/trabajo para realizar la incrustación:

- Para marcas de agua la incrustación debe realizarse en aquellas zonas que minimicen la percepción de las mismas y a la vez garanticen la utilidad de las marcas.
- En la esteganografía, la incrustación debe realizarse en aquellos lugares en los que sea más difícil de detectar.

El caso más intuitivo es la incrustación de datos en imágenes. Pensemos en una imagen presentada como una colección de píxeles, cada uno indicando un tono de gris mediante D bits, es decir, cada píxel es un número en el rango $\{0, \ldots, 2^D - 1\}$. Para ocultar datos en la imagen debemos decidir cuántos bits vamos a cambiar en cada píxel. Dicha elección nos conducirá a decidir qué píxeles podemos cambiar y cuáles no.

El mensaje o trabajo recibe el nombre en inglés de *cover work* o *cover object*. La parte seleccionada para incrustar los datos recibe el nombre de *cover sequence* o *cover vector*. Las reglas para elegirlos reciben el nombre de *selection rules*.

Estegosistemas: Parámetros I

- Longitud del trabajo n.
- Capacidad de incrustación k.
- Radio de incrustación

$$\rho = \max\left\{ \mathrm{d_H}(c, \mathrm{inc}(c, m)) \mid c \in \mathcal{A}^n, m \in \mathcal{A}^k \right\}.$$

- Número medio de cambios en cada incrustación

$$R_a = \frac{1}{q^{kn}} \sum_{\substack{c \in \mathcal{A}^n \\ m \in \mathcal{A}^k}} \mathrm{d_H}(c, \mathrm{inc}(c, m))$$

- Carga relativa $\alpha = \frac{k}{n}$, y carga binaria relativa (o tasa de incrustación) $E = \frac{k}{n} \log_2(q)$.
- Tasa de cambio (o distorsión media) $c = \frac{R_a}{n}$.
- Eficiencia de incrustación $e = \frac{k}{R_a}$ y eficiencia de incrustación mínima $\underline{e} = \frac{k}{\rho}$.

LSB modulation

La entrada es una imagen dada como una matriz de vectores en $\mathbb{F}_2^D$, es decir, una matriz de cadenas de D bits.

La selección se realiza en dos fases:

- Seleccionamos qué píxeles vamos a emplear, lo que nos da una lista $s = (s_1, \ldots, s_n)$. Cada $s_i = (b_{i,0}, \ldots, b_{i,D-1}) \in \mathbb{F}_2^D$ equivale al número escrito en binario $s_0 = \sum_{j=0}^{D-1} b_{i,j} 2^j$.
- La *cover sequence* se obtiene concatenando los t bits menos significativos, es decir,

$$b_{1,0} \ldots b_{1,t-1} b_{2,0} \ldots b_{2,t-1} \ldots b_{n,0} \ldots b_{n,t-1}$$

Imágenes JPEG

JPEG

- La imagen se divide en bloque de 8×8 píxeles.
- Se aplica la Transformada de Coseno Discreta (DCT) a dichos bloques, lo que proporciona el espectro de frecuencia espacial.
- Los datos resultantes se comprimen con el conocido como algoritmo sin pérdida de Huffmann.

Data hiding en JPEG

- Se seleccionan algunos de los coeficientes DCT.
- El cover vector consiste en la sucesión de los bits menos significativos (LSB) de los coeficientes anteriores.

Índice

Códigos Correctores de Errores I

ECC

- Fijamos como alfabeto un cuerpo finito $\mathbb{F}_q$.
- Un $(n, M)_q$-código es un subconjunto $\mathcal{C} \subseteq \mathbb{F}_q^n$ de cardinal M. Decimos que n es la longitud del código.
- La distancia mínima de $\mathcal{C}$ se define como

$$\mathrm{d}(\mathcal{C}) = \min\{\mathrm{d_H}(x, y) \mid x, y \in \mathcal{C}, x \neq y\}$$

- Un algoritmo de decodificación es una aplicación $\mathrm{dec} : \mathbb{F}_q^n \to \mathcal{C}$ tal que para cualquier $x \in \mathbb{F}_q^n$, $\mathrm{d_H}(x, \mathcal{C}) = \mathrm{d_H}(x, \mathrm{dec}(x))$.

Códigos Correctores de Errores II

Capacidad de corrección

- Si transmitimos $c \in \mathcal{C}$ a traves de un canal con ruido, recibiremos $c + e$ con e cierto error. Si $2\,w_H(e) < d(\mathcal{C})$, entonces $\mathrm{dec}(c + e) = c$.
- $t = \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor$ es la capacidad de corrección del código $\mathcal{C}$.
- $B(c, t) = \{x \in \mathbb{F}_q^n \mid d_H(x, c) \leq t\}$. Si $c \in \mathcal{C}$ y $x \in B(c, t)$, entonces $\mathrm{dec}(x) = c$. El cardinal de estas "bolas" es fácil de calcular: $\#B(c, t) = \sum_{i=0}^{t} \binom{n}{i}(q-1)^i$.
- La cota de Hamming establece

$$M \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq q^n.$$

- $\mathcal{C}$ se dice perfecto si se alcanza la cota de Hamming. En este caso todo elemento de $\mathbb{F}_q^n$ se decodifica a un elemento de $\mathcal{C}$.

Enlazando ECC y estegosistemas I

- Sea $\mathcal{S} = (\text{inc}, \text{rec})$ un sistema estaganográfico donde $\text{inc} : \mathbb{F}_q^n \times \mathbb{F}_q^k \to \mathbb{F}_q^n$ y $\text{rec} : \mathbb{F}_q^n \to \mathbb{F}_q^k$.
- Para cada $m \in \mathbb{F}_q^k$, sea el código $\mathcal{C}_m = \{x \in \mathbb{F}_q^n \mid \text{rec}(x) = m\}$.
- La familia $\{\mathcal{C}_m \mid m \in \mathbb{F}_q^k\}$ es una partición de $\mathbb{F}_q^n$.
- Para cada $m \in \mathbb{F}_q^k$, la aplicación $\text{dec}_m : \mathbb{F}_q^n \to \mathcal{C}_m$ definida por $\text{dec}_m(x) = \text{inc}(x, m)$ es un algoritmo de decodificación.

- Sea $\{\mathcal{C}_m \mid m \in \mathbb{F}_q^k\}$ una familia de códigos que constituyen una partición de $\mathbb{F}_q^n$.
- Para cada $m \in \mathbb{F}_q^k$ denotamos $\text{dec}_m : \mathbb{F}_q^n \to \mathcal{C}_m$ al correspondiente algoritmo de decodificación.
- Sea $\text{inc} : \mathbb{F}_q^n \times \mathbb{F}_q^k \to \mathbb{F}_q^n$ la aplicación definida por $\text{inc}(x, m) = \text{dec}_m(x)$.
- Sea $\text{rec} : \mathbb{F}_q^n \to \mathbb{F}_q^k$ la aplicación definida por $\text{rec}(x) = m$ si $x \in \mathcal{C}_m$.
- La pareja $\mathcal{S} = (\text{inc}, \text{rec})$ es un estegosistema.

Enlazando ECC y estegosistemas II

En el diseño de métodos de ocultación de información debemos centrar los esfuerzos en la función de recuperación, ya que es la que determina el sistema completo.

Códigos lineales y afines I

Definiciones

- Un $[n, k]_q$–código lineal es un subespacio vectorial $\mathcal{C} \leq \mathbb{F}_q^n$ de dimensión k.
- Un $[n, k]_q$–código afín es un subespacio afín de $\mathbb{F}_q^n$ de dimensión k, es decir, un subconjunto de la forma $z + \mathcal{C}$ donde $\mathcal{C}$ es un $[n, k]_q$–código lineal.

Lema

Para cualesquiera $x, y, z \in \mathbb{F}_q^n$, $\mathrm{d_H}(x, y) = \mathrm{d_H}(x + z, y + z)$.

Proposición

Sea $\mathrm{dec} : \mathbb{F}_q^n \to \mathcal{C}$ *un algoritmo de decodificación para un código lineal* $\mathcal{C}$. *La aplicación* $x \mapsto x + \mathrm{dec}(x - z)$ *es un algoritmo de decodificación para el código afín* $z + \mathcal{C}$.

Códigos lineales y afines II

Sea $\mathcal{C}$ un $[n.k]_q$–código lineal.

- Una matrix $G \in \mathcal{M}_{k\times n}(\mathbb{F}_q)$ tal que

$$\mathcal{C} = \{mG \mid m \in \mathbb{F}_q^k\}$$

  recibe el nombre de matrix generadora o *encoder*.

- Una matrix $H \in \mathcal{M}_{(n-k)\times n}(\mathbb{F}_q)$ tal que

$$\mathcal{C} = \{x \in \mathbb{F}_q^n \mid xH^{\mathrm{T}} = 0\}$$

  recibe el nombre de matrix (verificadora) de paridad o *parity check matrix*.

Convertir matrices generadoras en matrices de paridad es el mismo proceso que convertir sistemas de generadores (bases) en ecuaciones cartesianas y viceversa.

Códigos lineales y afines III

Códigos de Hamming

Una familia de códigos lineales adecuada para esta tarea son los códigos de Hamming. Los códigos de Hamming binarios son $[2^r-1, 2^r-1-r]_2$–códigos lineales cuya matriz de paridad tiene por columnas los números $1, 2, \ldots, 2^r-1$ escritos en binario. Por ejemplo, el $[7,4]$–código de Hamming tiene por matriz de paridad

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Estos códigos tienen distancia 3 y son muy sencillos de decodificar.

Códigos lineales y afines IV

Síndrome

Sea H una matrix de paridad de un $[n,k]_q$–código lineal $\mathcal{C}$. Se define el síndrome como la aplicación

$$\begin{aligned} \operatorname{syn} : \mathbb{F}_q^n &\to \mathbb{F}_q^{n-k} \\ x &\mapsto \operatorname{syn}(x) = xH^{\mathrm{T}} \end{aligned}$$

Observemos que si transmitimos una palabra $c \in \mathcal{C}$ y recibimos $y = c + e \in \mathbb{F}_q^n$, tenemos que

$$\operatorname{syn}(y) = (c+e)H^{\mathrm{T}} = cH^{\mathrm{T}} + eH^{\mathrm{T}} = \operatorname{syn}(e).$$

Códigos lineales y afines V

Decodificación por síndrome

La decodificación por síndrome consiste en generar una lista

Cuadro: Síndromes

Síndrome	Error
s_1	e_1
s_2	e_2
$\vdots$	$\vdots$

donde la columna error contiene de el conjunto $\{x \in \mathbb{F}_q^n \mid \text{syn}(x) = s_i\}$ un elemento de peso mínimo, y para cada palabra recibida $y \in \mathbb{F}_q^n$

$$\text{dec}(y) = e_i \text{ si } \text{syn}(y) = s_i.$$

Bibliografía I


C. Adams, P. Cain, D. Pinkas, and R. Zuccherato.
Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
IETF, August 2001.


Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker.
Digital Watermarking and Steganography.
The Morgan Kaufmann Series in Multimedia Information and Systems. Elsevier, second edition edition, 2008.


D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk.
Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
IETF, May 2008.


Quynh H. Dang.
The Keyed-Hash Message Authentication Code (HMAC).
National Institute of Standards and Technology (NIST), July 2008.

Bibliografía II


Kresimir Delac and Mislav Grgic.
A survey of biometric recognition methods.
In *46th International Symposium Electronics in Marine, ELMAR-2004*, pages 184–193, 2004.


Hans Delfs and Helmut Knebl.
Introduction to Cryptography. Principles and Applications.
Information Security and Cryptography. Springer, third edition, 2015.


T. Dierks and E. Rescorla.
The Transport Layer Security (TLS) Protocol Version 1.2.
IETF, August 2008.


Educause.
7 things you should know about Federared Identity Management, September 2009.

Peter Gutmann.
Everything you Never Wanted to Know about PKI but were Forced to Find Out.
Technical report, University of Auckland.

Bibliografía III


ISO/IEC.
Information technology — Security techniques — A framework for identity management —, December 2011.


Joseph Migga Kizza.
Guide to Computer Network Security.
Computer Communications and Networks. Springer, 3rd. edition, 2015.


S. Kent and K. Seo.
Security Architecture for the Internet Protocol.
IETF, December 2005.


Andre Karamanian, Srinivas Tenneti, and Francois Dessart.
PKI Uncovered: Certificate-Based Security Solutions for Next-Generation Networks.
Cisco Press, 2011.

Bibliografía IV


Carlos Munuera.
Steganography from a Coding Theory Point of View, pages 83–128.
WORLD SCIENTIFIC, 2013.


Satoshi Nakamoto.
Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer.
Technical report, bitcoin.org.
Traducido por @breathingdog.


National Institute of Standards and Technology (NIST).
DATA ENCRYPTION STANDARD (DES), October 1999.


National Institute of Standards and Technology (NIST).
ADVANCED ENCRYPTION STANDARD (AES), November 2001.


National Institute of Standards and Technology (NIST).
SECURE HASH STANDARD, August 2002.

Bibliografía V


National Institute of Standards and Technology (NIST).
Digital Signature Standard (DSS), July 2013.


Josef Pieprzyk, Thomas Hardjono, and Jennifer Seberry.
Fundamentals of Computer Security.
Springer, 2003.