



CRIPTOGRAFÍA PARA INGENIER@S

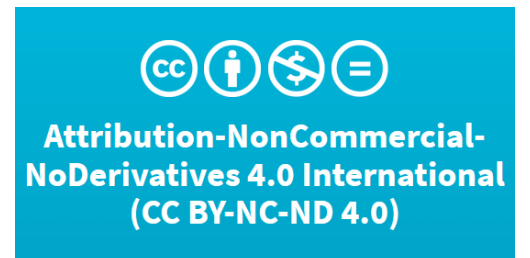
Class4crypt

© Jorgeramió 2022

Aula virtual de
criptografía
aplicada

Diapositivas
utilizadas en las
clases grabadas
de Class4crypt

Módulo 5 Fundamentos de la criptografía
Dr. Jorge Ramió Aguirre © 2022





*El ingenio es intrínseco al ser humano,
solo hay que darle una oportunidad
para que se manifieste.*

<https://www.criptored.es/cvJorge/index.html>

Tu aula virtual de criptografía aplicada

Módulo 10. Criptografía asimétrica

Class4crypt

Módulo 5. Fundamentos de la criptografía

- 5.1. Definiendo criptografía y criptoanálisis
- 5.2. Esquemas y elementos de un criptosistema
- 5.3. Principios de Kerckhoffs y fortaleza de la cifra
- 5.4. Introducción a la esteganografía
- 5.5. Mecanismos y máquinas de cifrar
- 5.6. Clasificación de los sistemas de cifra clásica
- 5.7. Introducción a la criptografía moderna
- 5.8. Comparativa entre cifra simétrica y asimétrica

Lista de reproducción del módulo 5 en el canal Class4crypt

<https://www.youtube.com/playlist?list=PLq6etZPDh0kucaDN4B4YC7T1L4t4m7t3P>

Class4crypt c4c5.1

Módulo 5. Fundamentos de la criptografía

Lección 5.1. Definiendo criptografía y criptoanálisis

5.1.1. La criptografía y el criptoanálisis como parte de la criptología

5.1.2. Definiciones de criptografía según su ámbito de estudio

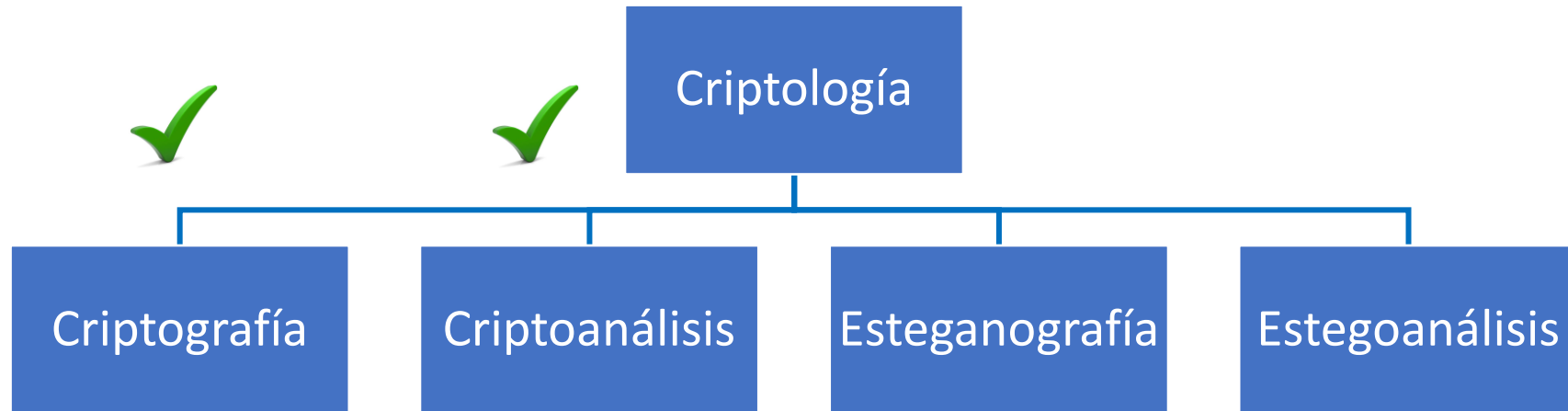
5.1.3. Diferencias entre cifrar y codificar

5.1.4. Definición de criptoanálisis

5.1.5. Entornos de cifra más o menos propensos al criptoanálisis

Class4crypt c4c5.1 Definiendo criptografía y criptoanálisis
<https://www.youtube.com/watch?v=d40xut6OHe8>

Criptografía y criptoanálisis



- La criptología es la ciencia que estudia cómo mantener un secreto cifrándolo mediante la criptografía, o bien ocultando ese secreto mediante la esteganografía. Por el contrario, el criptoanálisis y el estegoanálisis intentarán romper la seguridad y la fortaleza de las técnicas usadas para la protección del secreto o bien su ocultación

Criptografía según la RAE



REAL ACADEMIA ESPAÑOLA

- **criptografía** (de cripto y grafía)
 - Arte de escribir con clave secreta o de un modo enigmático
 - cripto (del gr. κρυπτός kryptós)
 - Significa 'oculto, encubierto'
 - grafía (del gr. γραφή graphé)
 - Modo de escribir o representar los sonidos, y, en especial, empleo de tal letra o tal signo gráfico para representar un sonido dado
- **criptología** (de cripto y logía)
 - Estudio de los sistemas, claves y lenguajes ocultos o secretos
- ¿Son correctas estas definiciones? No del todo...



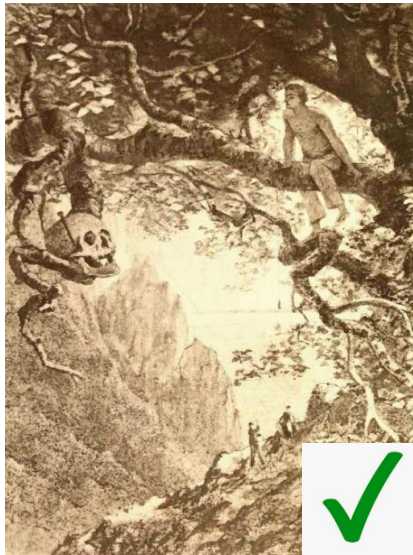
RAE: una definición muy literaria (1/2)

- La definición que nos da la RAE sobre criptografía es muy literaria
- Puede ser válida para algunos textos literarios o novelas que usan a la criptografía como fin principal o parte de su trama, pero no es una definición adecuada para nuestro perfil técnico
 - La criptografía deja de ser un arte tras los estudios de Claude Shannon que ya hemos visto en el módulo dedicado a la teoría de la información
 - Hoy en día no escribimos documentos sino que los generamos, siendo éstos de todo tipo. Por ejemplo documentos en formatos docx, pptx, xlsx, accdb, jpg, mp3, mp4, exe, jar, etc.

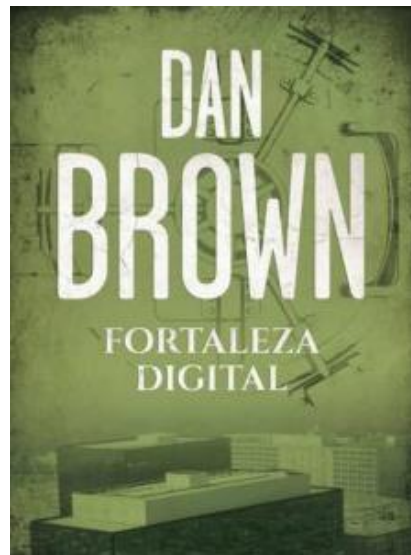
RAE: una definición muy literaria (2/2)

- Hoy en día no se usa una única clave secreta en la cifra
 - En los algoritmos de criptografía moderna simétrica en bloque se usa una clave de cifra K secreta, además de un vector inicial IV , si bien este último puede ser público
 - En los algoritmos de criptografía moderna asimétrica se usan dos claves, una pública y otra privada inversa de la anterior, según la operación de cifra que desee realizarse
- La criptografía actual opera sobre bits y bytes, por lo que los resultados de una cifra (e.g. 10110000 o bien 01100011) no pueden ser considerados como enigmáticos

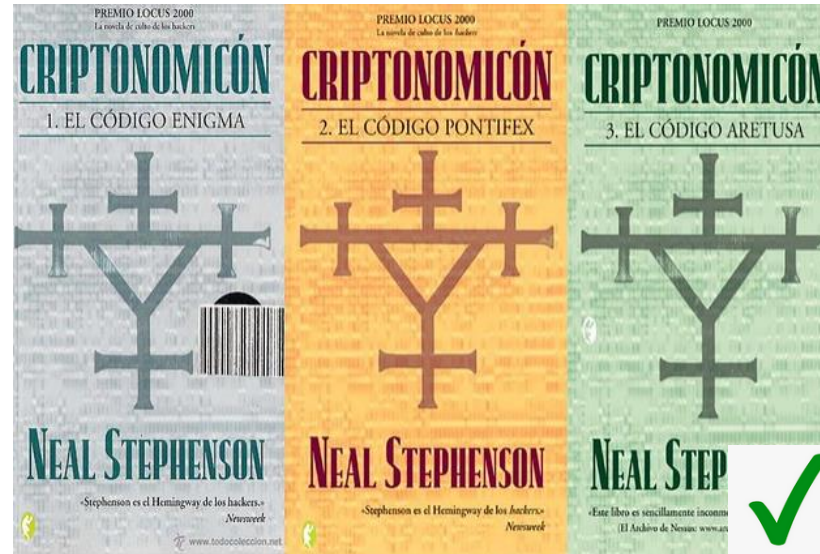
Esa criptografía literaria... “buena” y “mala”



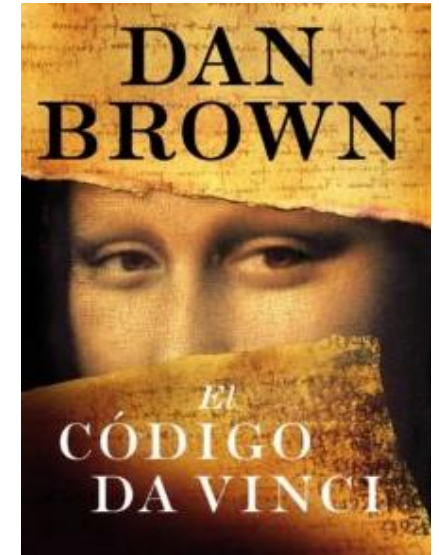
El escarabajo de oro, Edgar Allan Poe, 1843



Fortaleza digital, Dan Brown, 1998



Criptonomicrón, Neal Stephenson, 1999



El código Da Vinci, Dan Brown, 2003

Definiciones técnicas de criptografía

- Disciplina científica que se ocupa del estudio de los algoritmos, protocolos y sistemas que se utilizan para proteger la información, así como para dotar de seguridad a las comunicaciones y a las entidades que se comunican
- Se trata de un conjunto de herramientas matemáticas, técnicas y algoritmos, que con el uso de una o más claves permiten cifrar la información y, por tanto, protegerla y dotarle al menos de los principios de confidencialidad y de integridad
- Lo más importante es que hoy en día la criptografía se trata de una disciplina científica, es decir de una ciencia, no de un arte

¿Es lo mismo cifrar que codificar?

- No es lo mismo y es un error utilizarlos como sinónimos
- La cifra será una operación dinámica, ya que para cada clave distinta el criptograma será también distinto. Y lo recomendable es que se use una clave diferente en cada operación de cifra
- En cambio, la codificación será una operación estática, ya que cada elemento codificado se representará por un único símbolo, y éste nunca cambiará, ni por razones de espacio ni de tiempo
 - Por ejemplo, la letra A en ASCII es 01000001 y es así desde la invención de ese código en 1963, lo mismo en España, que en USA, Perú, China o Japón
 - Ejemplos de códigos comunes en la informática: Morse, Baudot, ASCII, ASCII extendido, UTF-8, ISO/IEC 8859, ISO 646, Unicode, Base64

Pero cifrar sí es lo mismo que encriptar

- En Latinoamérica es común el uso de encriptar en vez de cifrar
- La Real Academia Española reconoce en 2014 que ambos términos son sinónimos, pero yo prefiero utilizar la palabra en castellano cifrar porque “encriptar” podría tener otro significado...
- **Encriptar**
 - Del ingl. to encrypt; cf. gr. ἐγκρύπτειν enkrýptein 'ocultar'
 - 1. tr. cifrar (transcribir con una clave)
- **Cifrar**
 - 1. tr. Transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje o texto cuyo contenido se quiere proteger



Definiciones de criptoanálisis

- Según la RAE, criptoanálisis es el “Arte de descifrar criptogramas”
 - No acierta nuevamente la Real Academia Española en su descripción de criptoanálisis porque no se trata de un arte
- El criptoanálisis es la ciencia que se dedica al estudio de las debilidades de los sistemas criptográficos, con el fin de romper su seguridad y descubrir una clave secreta o recuperar la información original a partir de un criptograma. Para ello usará procedimientos eficientes, a diferencia de la denominada fuerza bruta, que sería intentar el descifrado con todas y cada una de las claves posibles
 - Podemos decir que el criptoanálisis es un ataque con *elegancia*

Entorno de cifra propenso a criptoanálisis

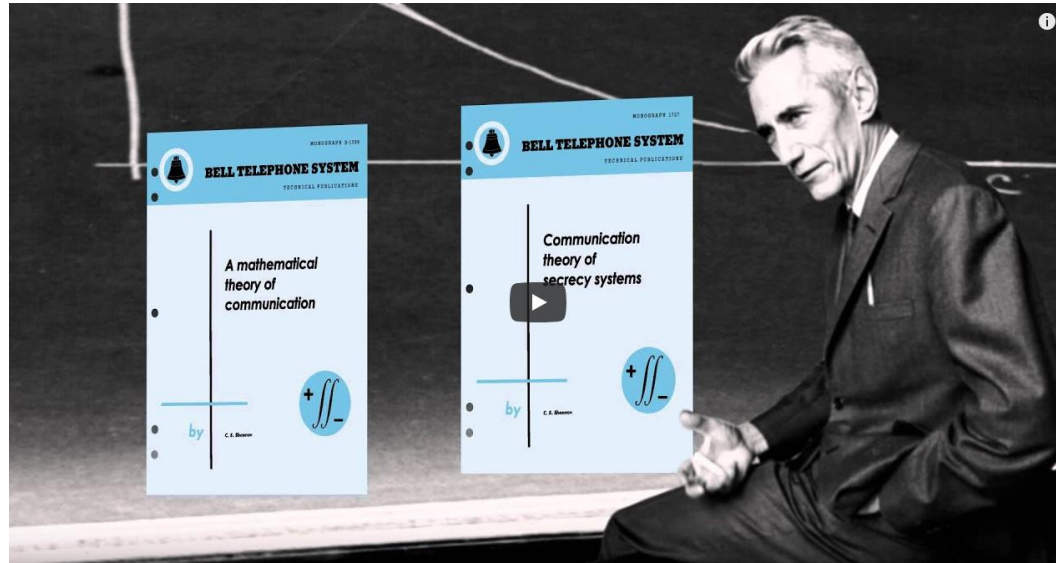
- Los sistemas de cifra denominados clásicos, es decir algoritmos, mecanismos y sistemas criptográficos de hasta mediados del siglo XX, son propensos al criptoanálisis
- Aquí la cifra es una función lineal y, aunque no se conozca la clave, muchas veces dicha cifra es fácilmente reversible por ataques
 - Aplicando estadísticas del lenguaje sobre el criptograma, para ver si la redundancia de éste en el texto en claro se manifiesta también en el criptograma (e.g. ataque de Kasiski a la cifra de Vigenère)
 - Aplicando operaciones matemáticas que permitan descubrir la clave (e.g. ataque con texto en claro de Gauss-Jordan a la cifra de Hill)
- En sistemas modernos el criptoanálisis será mucho más difícil

Más información sobre criptografía



- "Lenguajes Secretos y Códigos", programa Sacalalengua, Televisión Española TVE1, emitido el 3 de noviembre de 2009
- Participación desde el minuto 36:06 al minuto 39:48
- Enlace en Lectura recomendada

Más información en píldoras Thoth



- <https://www.youtube.com/watch?v=PDpMgx7avzA>



- <https://www.youtube.com/watch?v=77BrG2vRKss>

Conclusiones de la Lección 5.1

- Las definiciones que nos entrega la RAE sobre criptografía y criptoanálisis no son las adecuadas en un entorno técnico como el que aquí nos interesa
- En ambos casos no se trata de un arte sino de una ciencia
- Es importante recalcar que en la cifra actual puede usarse más de una clave secreta, por ejemplo en el intercambio de clave de DH, y que la apariencia del criptograma no puede calificarse de enigmática en tanto son solamente bytes
- La criptografía nos permitirá aplicar algoritmos para proteger la información y dotarle, al menos, de confidencialidad y de integridad
- Por contrapartida, el criptoanálisis tratará de romper el sistema de cifra, descubriendo la clave utilizada y recuperando el secreto, utilizando siempre procedimientos más eficientes que un simple ataque por fuerza bruta

Lectura recomendada (1/2)

- Criptografía, Real Academia de la Lengua
 - <https://dle.rae.es/criptograf%C3%ADa>
- El escarabajo de oro, Edgar Allan Poe, 1843
 - <https://ciudadseva.com/texto/el-escarabajo-de-oro/>
- Criptonomicrón, Wikipedia
 - <https://es.wikipedia.org/wiki/Criptonomic%C3%B3n>
- Criptoanálisis, Real Academia de la Lengua
 - <https://dle.rae.es/criptoan%C3%A1lisis>

Lectura recomendada (2/2)

- Lenguajes Secretos y Códigos, Programa Sacalalengua de TVE1 Televisión Española, 03/11/2009, minutos 36:06 al 39:48
 - <https://www.rtve.es/alacarta/videos/saca-la-lengua/sacalalengua-lenguajes-secretos-codigos/621025/>
- Guion píldora formativa Thoth nº 2, ¿Qué es la criptografía?, Jorge Ramió, 2014
 - <https://www.criptored.es/thoth/material/texto/pildora002.pdf>
- Guion píldora formativa Thoth nº 6, ¿Ciframos, codificamos o encriptamos ?, Jorge Ramió, 2014
 - <https://www.criptored.es/thoth/material/texto/pildora006.pdf>

Class4crypt c4c5.2

Módulo 5. Fundamentos de la criptografía

Lección 5.2. Esquema y elementos de un criptosistema

5.2.1. La necesidad de cifrar la información

5.2.2. Esquema de un sistema de cifra

5.2.3. Texto en claro y criptograma

5.2.4. Algoritmo de cifrado y de descifrado

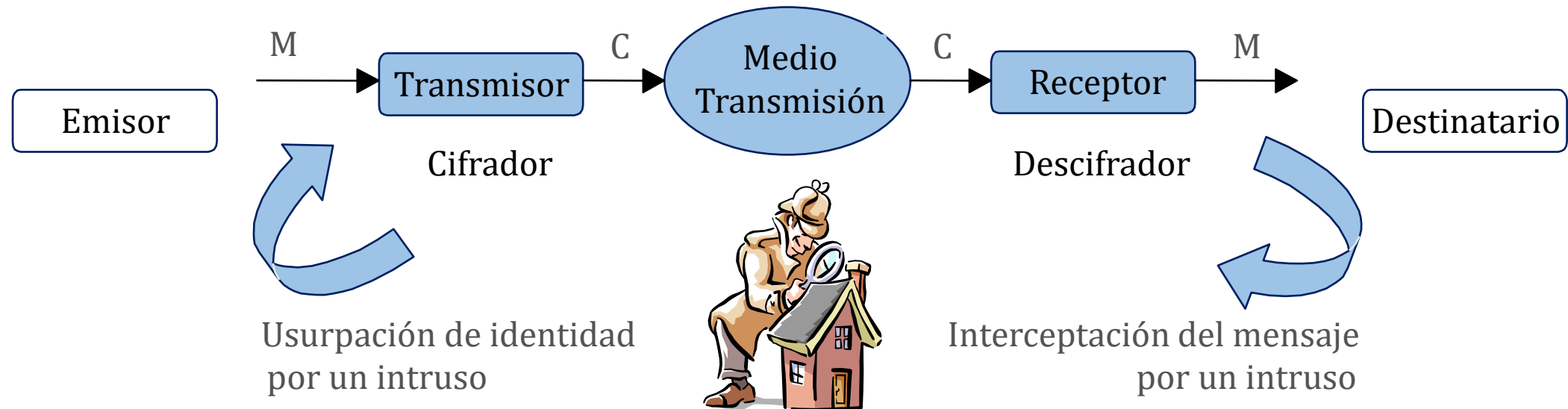
5.2.5-Clave de cifrado y de descifrado

5.2.6. Canal o medio de transmisión

5.2.7. Alfabeto de cifra

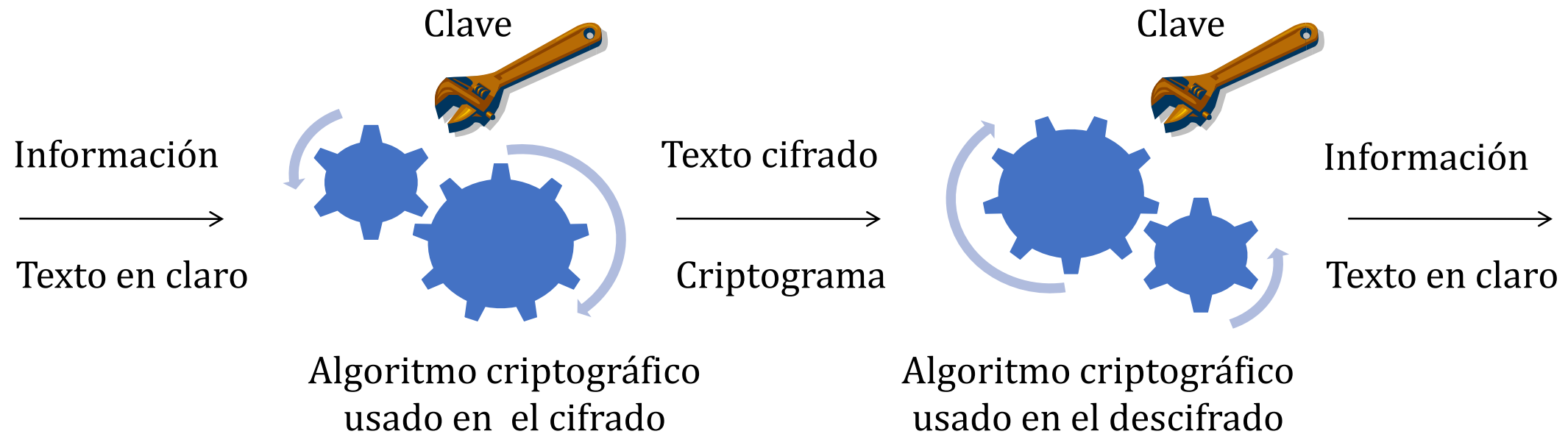
Class4crypt c4c5.2 Esquema y elementos de un criptosistema
https://www.youtube.com/watch?v=W_mbzla2pbA

¿Por qué ciframos la información?



- Como el medio de transmisión será por definición inseguro, e incluso puede serlo el medio de almacenamiento final, deberemos cifrar la información **M** para protegerla de un atacante que desee leer en el extremo receptor el texto secreto que esconde **C**, o bien que el atacante desee suplantar al emisor en el extremo transmisor con el fin de enviar un mensaje falso **M'**

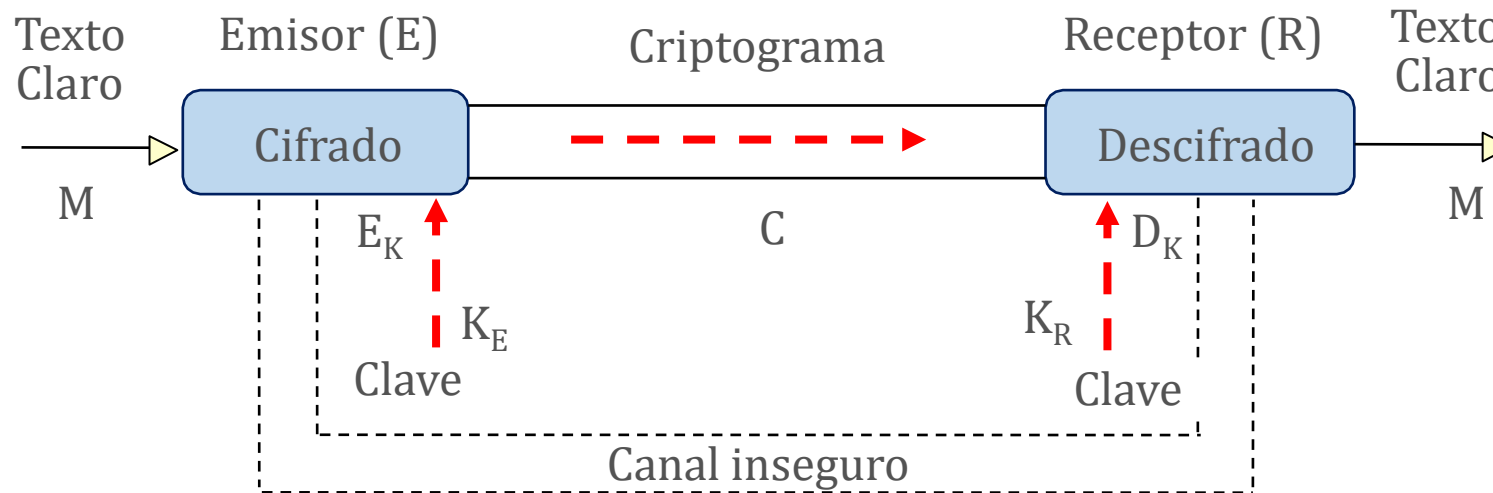
Esquema básico de un sistema de cifra



Esquema de cifra simétrica y clásica: la misma clave en ambos extremos

- El sentido de las operaciones de cifrado y de descifrado son inversas: en el cifrado primero se usa la rueda pequeña y después la rueda grande, en el descifrado primero se usa la rueda grande y después la rueda pequeña

Elementos en un esquema de cifra



- Texto en claro o texto base
- Criptograma o texto cifrado
- Canal o medio de transmisión
- Algoritmo de cifrado
- Algoritmo de descifrado
- Clave usada en emisión
- Clave usada en recepción
- Alfabeto usado en la cifra

Texto en claro y criptograma

- Texto en claro o texto base M
 - Información que resulta comprensible por sí misma por un ser humano, o un archivo sobre el que se realizan consultas como una base de datos, o programas ejecutables que realizan alguna operación. Se le asigna la letra M de Mensaje. Por ejemplo, M = EN UN LUGAR DE LA MANCHA
- Criptograma o texto cifrado C
 - Documento o texto que resulta de la cifra de cualquier información y que no es comprensible por un ser humano, salvo por el destinatario legítimo de la misma al descifrarlo. Puede ser también un archivo del que no se pueda extraer información con sentido ni tampoco ejecutarlo. Se le asigna la letra C de Criptograma. Por ejemplo C = HPXPÑ XJDUG HÑDOD PFKD, resultado de cifrar el texto M anterior con el algoritmo del César

Algoritmos de cifra y canal de transmisión

- Algoritmos de cifrado E_K (encrypt) y de descifrado D_K (decrypt)
 - Procesos que permiten transformar un texto en claro en un criptograma y viceversa. Como es lógico, debería poder descifrar el criptograma sólo quien tenga la clave secreta K y sea el destinatario legítimo de ese secreto. En emisión y en recepción se usará el mismo algoritmo, de forma tal que lo que se cifre en emisión luego pueda descifrarse en recepción
- Canal o medio de transmisión
 - Puede ser un canal de comunicación en Internet, una red local, un PC al guardar información desde la RAM al disco duro, el propio dispositivo de almacenamiento final, etc. Todos son inseguros por definición, dado que dependiendo del valor que tenga esa información, el atacante podrá invertir más o menos dinero y recursos para hacerse con el secreto

Claves de cifrado y de descifrado

- Claves de cifrado K_E y de descifrado K_D
 - Dependiendo del tipo de algoritmo que se use, las claves de emisión K_E (cifrado) y de recepción K_D (descifrado) pueden ser
 - Iguales $K_E = K_D = K$ (cifra simétrica)
 - Ambos interlocutores deberán compartir previamente la clave K
 - Diferentes $K_E \neq K_D$ (cifra asimétrica)
 - Ambos interlocutores usarán claves diferentes, sin necesidad de compartir previamente una clave
 - El descifrado se alcanza porque el algoritmo en destino **a)** realiza las mismas operaciones que en emisión pero en sentido contrario, **b)** usa las mismas operaciones que en emisión pero con claves inversas dentro de un módulo, o bien **c)** utiliza funciones inversas a las usadas en emisión

El alfabeto en la cifra clásica

- En la mayoría de los cifradores clásicos se utiliza como alfabeto de cifrado el mismo alfabeto que el del texto en claro
- Para poder aplicar las operaciones modulares de transformación, se asocia a cada letra del alfabeto un número, de forma que a la letra A le corresponde el 0, a la letra B el 1, etc.
 - Módulo 27: letras mayúsculas en castellano
 - Módulo 37: letras mayúsculas y dígitos
 - Módulo 54: letras mayúsculas y minúsculas
 - Módulo 59: letras mayúsculas, minúsculas y minúsculas acentuadas
 - Módulo 191: subconjunto de caracteres imprimibles del ASCII extendido
 - Módulo 224: caracteres imprimibles del ASCII extendido

Codificación del alfabeto mod 27

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

- Una pregunta muy frecuente es si es seguro asignar siempre a la letra A el código 0, a la B el código 1, etc. En otras palabras, ¿le entrega esto pistas al atacante?
- Sí es seguro. La redundancia del lenguaje se manifiesta en el texto en claro, independientemente del código que se le asigne a la letra
- Por lo tanto, el conocimiento por parte del atacante de un código fijo del alfabeto no le aporta ningún beneficio extra en el ataque

El alfabeto en la cifra moderna

- Una gran mayoría de los cifradores modernos, tanto en la cifra simétrica como en la cifra asimétrica, realizan operaciones de cifra modulares dentro de un grupo o de un cuerpo
- Esas operaciones se realizan sobre bytes (ASCII) o sobre números
- A diferencia de la cifra clásica, en la que el tamaño del alfabeto nos indicaba el valor del módulo en las operaciones de la cifra, en la criptografía moderna esto no tiene por qué estar relacionado
- Por ejemplo, en DH y RSA se opera actualmente con módulos de 2.048 bits y en IDEA las operaciones modulares de suma se hacen en módulo de 16 bits y las de multiplicación en módulo de 17 bits

Conclusiones de la Lección 5.2

- Debemos cifrar la información porque el canal de transmisión o el dispositivo de almacenamiento final son inseguros por definición
- Los elementos que forman un criptosistema son
 - El texto en claro M
 - El criptograma C
 - Los algoritmos de cifrado E_K y de descifrado D_K
 - Las claves de cifrado K_E y de descifrado K_D
 - El canal o medio de transmisión
 - El alfabeto o código con el que se codifica el documento a cifrar
- Las claves de cifrado K_E y de descifrado K_D operarán de forma diferente si se trata de una cifra simétrica o de una cifra asimétrica
- En la cifra clásica los elementos del alfabeto fuerzan el tamaño del módulo

Class4crypt c4c5.3

Módulo 5. Fundamentos de la criptografía

Lección 5.3. Principios de Kerckhoffs y fortaleza de la cifra

5.3.1. La figura de Auguste Kerckhoffs

5.3.2. Los principios, postulados o lemas de Kerckhoffs

5.3.3. Ataques por fuerza bruta y criptoanálisis

5.3.4. Tipos de ataque a los algoritmos de cifra

5.3.5. Fortaleza de un algoritmo de cifra

Class4crypt c4c5.3 Principios de Kerckhoffs y fortaleza de la cifra
<https://www.youtube.com/watch?v=Isg2-XHa0hY>

Auguste Kerckhoffs

- Auguste Kerckhoffs (1835 – 1903) fue un lingüista y criptógrafo holandés, profesor de alemán en París
- En febrero de 1883 publica en el Journal des Sciences Militaires “La cryptographie militaire”, un importante tratado sobre la criptografía en el que establece lo que conocemos como principios, postulados o lemas de Kerckhoffs
- Por el tipo de publicación y año, estos principios están orientados al uso de la criptografía en un ambiente militar o bélico
- Se trata de 6 principios básicos, que 138 años después la mayoría de ellos siguen siendo muy válidos para la criptografía actual

Principios de Kerckhoffs (1/2)

1. El sistema debe ser en la práctica indescifrable, en caso de que no lo sea matemáticamente
 - Si el sistema no es teóricamente irrompible, en la práctica sí debe serlo. Hoy se interpreta como que el sistema de cifra sea computacionalmente seguro. Es decir, que debido a las limitaciones en la capacidad de cómputo de los actuales ordenadores, el sistema de cifra resista todo tipo de ataques, en tanto el tiempo necesario como el esfuerzo económico para realizar dichos ataques sería inmenso, y por lo tanto en la práctica inviable
2. El sistema no debe ser secreto y no debe ser un problema que éste caiga en manos del enemigo
 - Es la aportación más interesante de Kerckhoffs. Hoy se interpreta como que la seguridad debe residir solamente en el secreto de la clave y no en el desconocimiento del algoritmo de cifrado. Más aún, el algoritmo debe ser público para que éste pueda ser analizado por la comunidad científica en búsqueda de posibles vulnerabilidades o de un mal diseño
 - Casos notables en la criptografía moderna en que esto no se ha cumplido (oscurantismo)

Principios de Kerckhoffs (2/2)

3. La clave del sistema debe ser fácil de memorizar y comunicar a otros, sin necesidad de tener que escribirla; será cambiable y modificable por los interlocutores válidos
 - El intercambio de DH aparece en 1976. Generar claves seguras, con una aleatoriedad adecuada, máxima entropía, etc., sigue siendo un problema en la actualidad
4. El sistema debe poder aplicarse a la correspondencia telegráfica
 - Lógicamente esto hoy no aplica, habría que actualizarlo a las comunicaciones digitales
5. El sistema debe ser portable y su uso no deberá requerir la intervención de varias personas
 - Este principio y el próximo (orientación militar) pueden adaptarse a los tiempos actuales
6. El sistema debe ser fácil de usar, no requerirá conocimientos especiales ni tendrá una larga serie de reglas

Clasificación de los ataques a la cifra

- Ataques por fuerza bruta
 - Como en la cifra se usa una clave secreta y el algoritmo deberá ser público, el atacante siempre tiene la posibilidad de descifrar el criptograma con todas y cada una de las claves posibles, hasta dar con la verdadera
 - Este tipo de ataque es elemental (y burdo) pues sólo requerirá que el atacante tenga una cierta capacidad de cómputo y tiempo suficiente
- Ataques mediante criptoanálisis
 - Aplicaremos al criptograma análisis estadísticos y ciertos procedimientos matemáticos para romper el sistema y descubrir la clave secreta, con un esfuerzo mucho menor que si se aplicase la fuerza bruta
 - Se trata ahora de un ataque elegante, técnico, que tiene un nivel científico

Tipos comunes de ataque a una cifra (1/3)

- Ataque con sólo con texto cifrado
 - De fuerza bruta, probando todas las claves posibles hasta que obtenemos un mensaje o documento con sentido
 - Basados en diccionario, probando únicamente con un subconjunto de las claves posibles, por ejemplo si las claves son palabras o textos comunes
 - Mediante un análisis de frecuencia. Se debe disponer de suficiente texto cifrado para poder aplicar estadísticas del lenguaje (sólo cifra clásica)
- Ataque con texto en claro conocido
 - Se dispone de un texto en claro y su correspondiente criptograma, lo que permite reducir el espacio de búsqueda de claves u obtener estadísticas que puedan usarse para hacer deducciones en otros textos cifrados

Tipos comunes de ataque a una cifra (2/3)

- Ataque con texto en claro elegido o texto cifrado elegido
 - Al elegir el tipo de texto en claro, se puede observar qué se obtiene como salida y esto puede reducir el espacio de búsqueda de la clave
 - El hecho de elegir trozos de uno o más criptogramas, por ejemplo cadenas repetidas, puede permitir que el ataque prospere más rápidamente
- Ataque meet-in-the-middle
 - Ataque con texto en claro conocido, que en algunos algoritmos permite demostrar que la fortaleza real de la clave es menor a la que se supone
- Ataque man-in-the-middle
 - El atacante se posiciona en medio de los interlocutores, crea sus propios datos, altera el sistema engañando a ambos y es dueño de la comunicación

Tipos comunes de ataque a una cifra (3/3)

- Ataque por la paradoja del cumpleaños
 - Se generan varios documentos (o cifrados) y se comparan los resultados entre sí en búsqueda de colisiones, haciendo que el esfuerzo del ataque se reduzca de un hipotético 2^n a $2^{n/2}$ intentos, siendo n los bits de la clave
- Ataque por cifrado cíclico
 - El atacante usa los datos públicos de la víctima realizando cifrados de forma cíclica o repetitiva, hasta que encuentra el secreto que se ha cifrado
- Ataque por canal lateral
 - El atacante observa y mide las manifestaciones físicas que los algoritmos de cifra producen cuando se ejecutan (radiaciones electromagnéticas, consumo de energía, sonidos, etc.) y es capaz de encontrar la clave secreta

Fortaleza de los algoritmos de cifra

Para que un sistema criptográfico sea considerado fuerte...



Debe disponer de un número elevado de claves posibles, con alta entropía, de modo que no sea razonable intentar descifrar un mensaje por el método de la fuerza bruta, probando todas las claves



Debe estar correctamente diseñado, de tal manera que la cifra produzca un criptograma que tenga una apariencia y una distribución aleatoria de todos los elementos (hoy bits) en ese texto cifrado



Debe resistir todo tipo de ataques. Es decir, además de ser imposible descifrar el criptograma por fuerza bruta, que sea resistente a ataques por criptoanálisis, en especial por texto en claro conocido

Más información en píldoras Thoth



<https://www.youtube.com/watch?v=gBedgwej5WU>

Grados de seguridad en algoritmos de cifra

- Algoritmo computacionalmente seguro
 - Con suficiente poder de cálculo, tiempo y lógicamente dinero, el sistema de cifra podría ser roto, pero a un coste tan elevado que no es práctico realizarlo. En la gran mayoría de casos reales, hoy resulta imposible
 - Hay que tener en cuenta que el coste computacional para considerar que un algoritmo es seguro ha ido cambiando con el paso del tiempo
- Algoritmo incondicionalmente seguro
 - Son aquellos en los que incluso disponiendo de grandes recursos y con el criptograma y texto en claro conocidos, no es posible romper la clave
 - Los únicos sistemas incondicionalmente o matemáticamente seguros son los denominados one-time pad OTP (libreta o clave de un solo uso)

Conclusiones de la Lección 5.3

- El segundo principio, postulado o lema de Kerckhoffs asegura que “el sistema no debe ser secreto y no debe ser un problema que éste caiga en manos del enemigo”
- Hoy se interpreta como que la seguridad del criptosistema debe recaer sólo en la clave y sigue siendo una máxima de la seguridad criptográfica actual
- Los ataques criptográficos pueden realizarse por fuerza bruta o mediante el uso de técnicas de criptoanálisis que explotan posibles vulnerabilidades
- Los ataques pueden realizarse directamente al algoritmo de cifra, a las propiedades matemáticas donde reside su seguridad o bien al entorno donde se aplica la criptografía, siendo esto último lo más común
- Porque, por lo general, la criptografía no se ataca, se esquiva (Dr. A. Muñoz)

Lectura recomendada (1/2)

- Guion píldora formativa Thoth nº 7 ¿Qué son los principios de Kerckhoffs?, Jorge Ramió, 2014
 - <https://www.criptored.es/thoth/material/texto/pildora007.pdf>
- La cryptographie militaire, Journal des sciences militaires, vol. IX, pp. 5–38, Janvier 1883, pp. 161–191, Auguste Kerckhoffs, Février 1883
 - https://www.petitcolas.net/kerckhoffs/crypto_militaire_1.pdf
- Ataques a la criptografía, Guía de seguridad CCN-STIC-401, Glosario y Abreviaturas, Centro Criptológico Nacional, José Antonio Mañas, 2015
 - https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=94.html
- One-time pad, Wikipedia
 - https://en.wikipedia.org/wiki/One-time_pad

Lectura recomendada (2/2)

- Cryptographic attacks
 - https://en.wikipedia.org/wiki/Category:Cryptographic_attacks
- Cryptographic Attacks: A Guide for the Perplexed, Ben Herzog, Check Point Research, July 2019
 - <https://research.checkpoint.com/2019/cryptographic-attacks-a-guide-for-the-perplexed/>
- “La criptografía no se ataca, se esquiva”, entrevista al Dr. Alfonso Muñoz, Security by Default, 2014
 - <http://www.securitybydefault.com/2014/11/entrevista-alfonso-munoz-mindcrypt.html>

Class4crypt c4c5.4

Módulo 5. Fundamentos de la criptografía

Lección 5.4. Introducción a la esteganografía

5.4.1. Definición de esteganografía y estegoanálisis

5.4.2. El problema de los prisioneros

5.4.3. Casos históricos del uso de la esteganografía

5.4.4. Usos actuales de la esteganografía

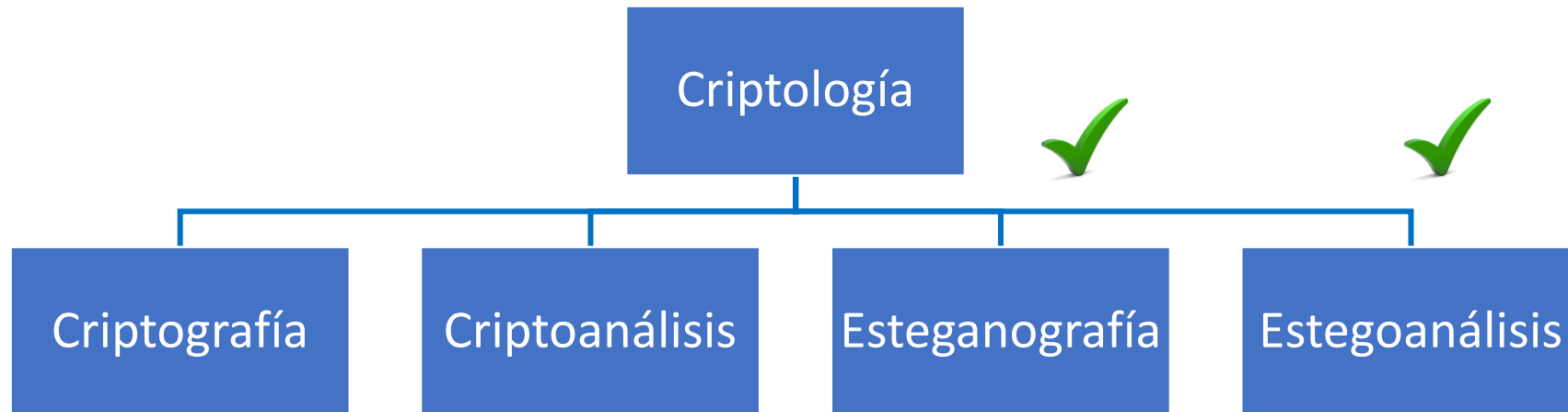
5.4.5. Introducción a la esteganografía usando imágenes

5.4.6. La esteganografía mediante el uso de acrósticos

5.4.7. Ocultación de texto dentro de una imagen desde símbolo del sistema


Class4crypt c4c5.4 Introducción a la esteganografía
<https://www.youtube.com/watch?v=5pwzv-0w5k>

Criptología y criptoanálisis




- La criptología es la ciencia que estudia cómo mantener un secreto cifrándolo mediante la criptografía, o bien ocultando ese secreto mediante la esteganografía. Por el contrario, el criptoanálisis y el estegoanálisis intentarán romper la seguridad y la fortaleza de las técnicas usadas para la protección del secreto o bien su ocultación

¿Recoge la RAE la palabra esteganografía?



REAL ACADEMIA ESPAÑOLA



Diccionario de la lengua española Edición del Tricentenario Actualización 2020

Consulta posible gracias al compromiso con la cultura de la

por palabras Consultar

Aviso: La palabra **esteganografía** no está en el Diccionario.

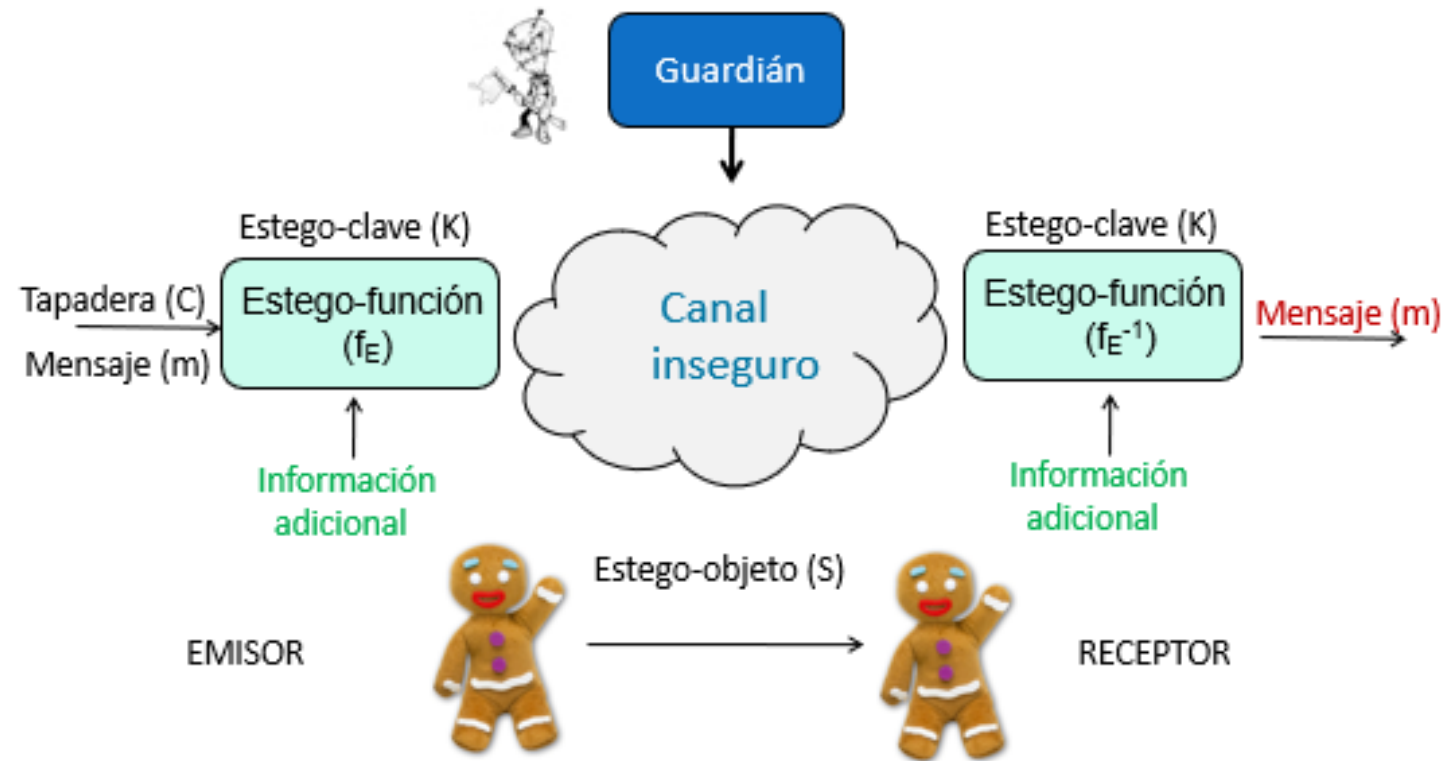
- Al contrario que con criptografía y criptoanálisis, no tendremos ninguna entrada en el diccionario de la Real Academia para esteganografía y estegoanálisis. No confundir esteganografía con estenografía, sinónimo de taquigrafía o escritura rápida con signos

Definición esteganografía y estegoanálisis

- La esteganografía es la ciencia que permite ocultar información dentro de algún archivo, que hace las funciones de tapadera, cubierta o portadora, con la intención de que no se perciba ni siquiera la existencia de dicha información
- Esa tapadera o medio en el cual se oculta la información se conoce como estegomedio y se comporta como un canal subliminal
- La información oculta puede estar como texto en claro o cifrado
- El estegoanálisis (o esteganálisis) es la ciencia que permite la detección y posterior revelación de información oculta en una portadora (stegomedio), utilizando técnicas esteganográficas

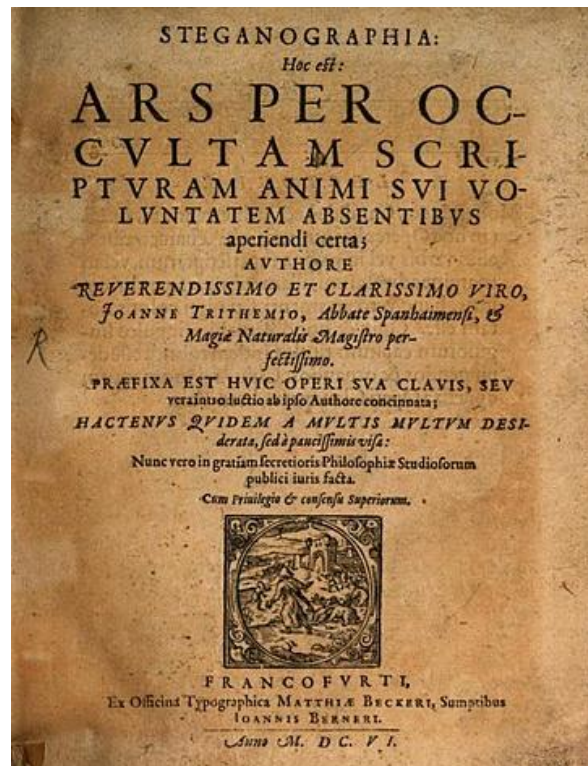
Canales subliminales y esteganografía

- Como ejemplo de canal subliminal tenemos el “Problema de los prisioneros”, que fue propuesto en 1983 por Gustavus Simmons
- Para poder huir, deben comunicarse a través del carcelero mediante misivas, sin que éste sospeche sobre cuál es el objetivo real de esos mensajes inocentes



Ref. Documentación esteganografía de Alfonso Muñoz @mindcrypt

La esteganografía en la historia antigua



- Primer libro de esteganografía, Johannes Trithemius (1499)

- Heródoto en su libro Las historias (430 a. C.) cuenta cómo Histieo afeitó la cabeza de un esclavo mensajero, tatuó un mensaje en su cuero cabelludo y esperó a que le volviera a crecer el pelo para así enviar ese secreto



- Giovanni della Porta, mensaje secreto en un huevo, siglo XV

La esteganografía en la 2ª Guerra Mundial



- La tecnología de los micropuntos fue utilizada por los alemanes durante la Segunda Guerra Mundial y durante la guerra fría
- Se reducen fotográficamente textos o fotografías hasta tamaños menores que un punto en un documento (1 mm de diámetro)

La esteganografía y el terrorismo

MailOnline

British Muslim 'had Al Qaeda contacts book with terrorists' numbers written in invisible ink'

By DAILY MAIL REPORTER
UPDATED: 16:34 GMT, 24 September 2008



A British Muslim owned a contacts book for Al Qaeda terrorists with their phone numbers written in invisible ink, a court heard today.

- En septiembre de 2008 en Reino Unido se detiene a dos personas sospechosas de pertenecer a la banda Al Qaeda
- Tenían tres libretas en las que con tinta invisible había instrucciones para sus bases sobre cómo cifrar sus correos

ars TECHNICA

[BIZ & IT](#) [TECH](#) [SCIENCE](#) [POLICY](#) [CARS](#) [GAMING & CULTURE](#)

BIZ & IT —

Steganography: how al-Qaeda hid secret documents in a porn video

Digital steganography hides files in plain sight, concealed in image and media files.

SEAN GALLAGHER - 5/2/2012, 2:02 PM

Escenarios actuales de la esteganografía

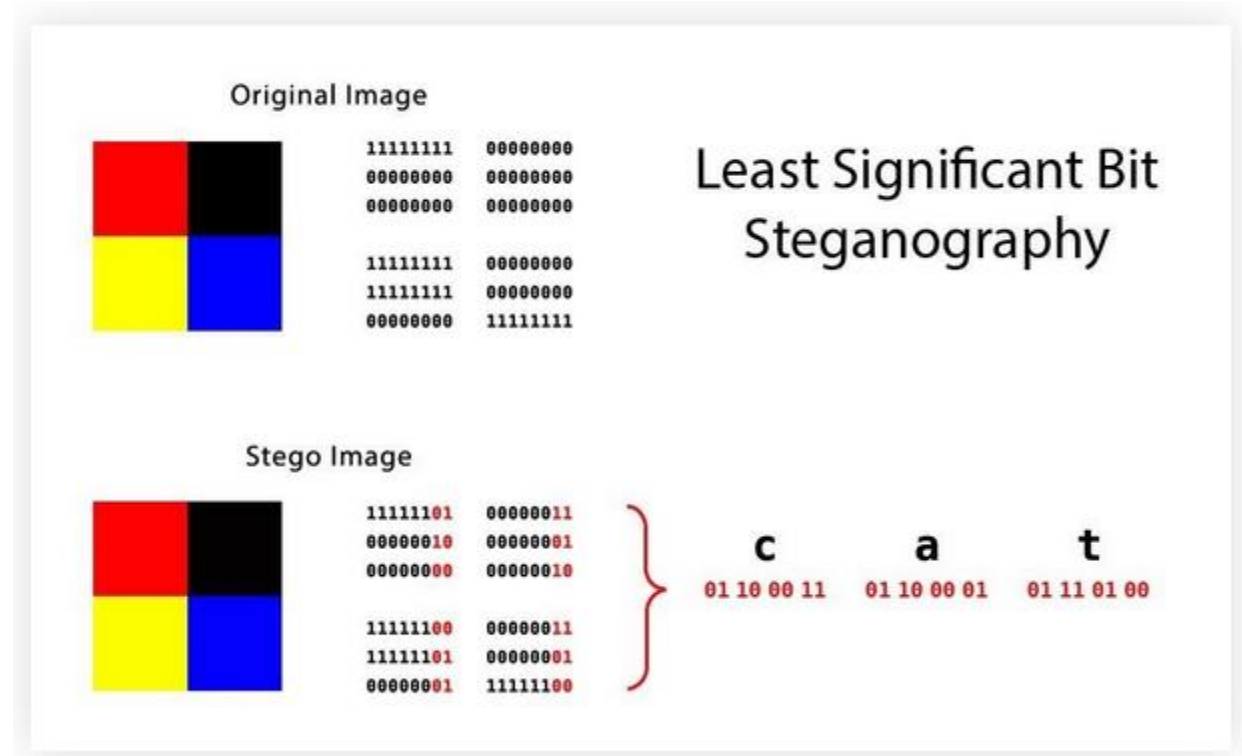
- Canales encubiertos (campos sin uso)
 - IPv4, IPv6, IPSEC, UDP, ICMP, HTTP, WiFi
- Esteganografía en ficheros y sistemas operativos
 - Fragmentación, sectores defectuosos del disco
- Esteganografía en tecnología web
 - Caracteres invisibles en HTML, etiquetas, atributos
- Esteganografía textual y lingüística
 - Acrósticos, arte ASCII, modificación léxica, semántica, errores tipográficos
- Esteganografía multimedia
 - Imágenes, audio, vídeos



Ocultación en imágenes, la más conocida

Ocultando texto en imágenes con LSB

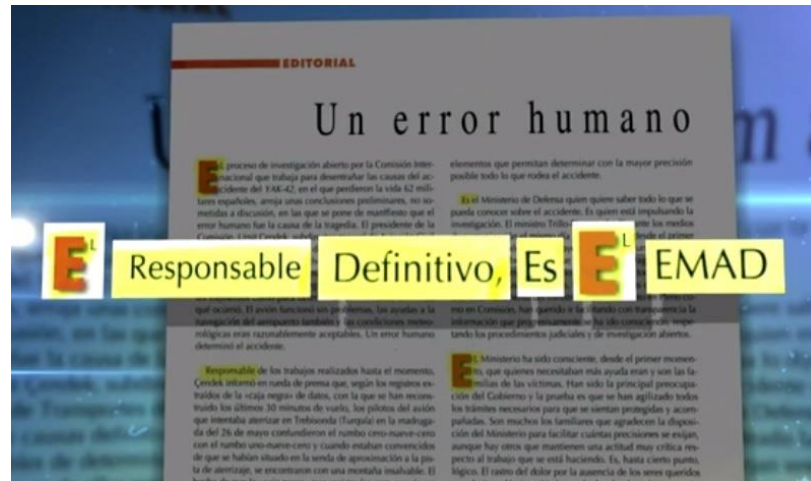
- En cada pixel RGB (Red, Green, Blue) de 24 bits pueden reemplazarse los últimos bit de cada byte, sin que sea perceptible al ojo humano
- Esta técnica conocida es como Least Significant Bit LSB. En el ejemplo de la figura, se usan los dos últimos bits de cada byte



Ref.: How to Hide Secret Data Inside an Image or Audio File in Seconds, Black Slash, 2017

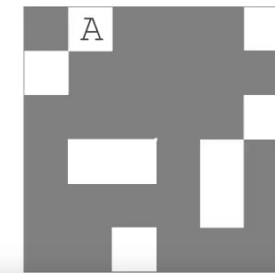
Esteganografía textual y acrósticos

Mayo 2003. Accidente avión Yakolev 42, Turquía



plain text

ATTACKATMORNINGALLUNITSAREPREPARED
N



1550, rejilla de Cardano. Aunque en realidad se trata de un sistema de cifra por permutación

The following message was actually sent by a German Spy in WWII:

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.

Taking the second letter in each word produces the following message:

Pershing sails from NY June 1 (Kahn 67).



La Celestina
(1499)
Reto 1
Clase 5.1

Ocultando texto en imagen desde sistema

- En carpeta Ejemplo, la imagen superior playa.jpg de 84 KB
- Y el archivo secreto.txt de 1 KB, con este texto secreto
 - El prisionero se entrega a las 05:30 horas
- Unimos ambos archivos en nueva imagen MiPlaya.jpg
 - `C:\Ejemplo>copy /b playa.jpg+secreto.txt MiPlaya.jpg`
- Figura de abajo archivo MiPlaya.jpg. Con doble clic o con un editor de imágenes, se verá la misma fotografía
- Si MiPlaya.jpg se abre con un editor Hexa o bloc de notas, al final del archivo se verá el texto secreto oculto



{f>°ø-ÿ "ã}[]õ®ÖÏÿ doéE[]x6115oøù?î~õ®"ßpB÷_Sýhç¶[[]çp5ÿ Öÿ z,+iù \ÿ À[-[]S[]Êµ[]ù[]n?P«p[]ÿ 'É?
ë™pbŠ([µ¹ÿ 'ÿOús½"ÿ ÈFãê(ç€)7ú@çP-ëçøñÿ ëE[]ÿÜEl prisionero se entrega a las 05:30 horas

Más información en píldoras Thoth



Píldora 47: ¿Qué es la esteganografía?

<https://www.youtube.com/watch?v=6KVrsKG5CVg>



Píldora 48: ¿Cómo se oculta información con esteganografía?

<https://www.youtube.com/watch?v=h5K-xNTmTcM>

Conclusiones de la Lección 5.4

- La esteganografía es la ciencia que permite ocultar información en un medio conocido como stegomedio para que ésta pase desapercibida, y se diferencia de la criptografía en que esta última busca cifrar la información
- La técnica de ataque a la esteganografía se conoce como estegoanálisis
- Existen muchos ejemplos en la historia del uso de la esteganografía
- Los escenarios actuales de la esteganografía son los canales encubiertos, en los sistemas operativos, en los sistemas de ficheros, en la tecnología web, en formato textual, en modo lingüístico y en los entornos multimedia
- Una técnica muy habitual y simple de esteganografía en multimedia es el reemplazo del último o de los últimos bits de cada pixel en imágenes, conocido como LSB

Lectura recomendada (1/2)

- Guion píldora formativa Thoth nº 47, ¿Qué es la esteganografía?, Alfonso Muñoz, 2017
 - <https://www.criptored.es/thoth/material/texto/pildora047.pdf>
- Guion píldora formativa Thoth 48, ¿Cómo se oculta información con esteganografía?, Alfonso Muñoz, 2017
 - <https://www.criptored.es/thoth/material/texto/pildora048.pdf>
- Esteganografía, Guía de seguridad CCN-STIC-401, Glosario y Abreviaturas, Centro Criptológico Nacional, José Antonio Mañas, 2015
 - https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=428.html
- ¿Qué es la esteganografía digital?, Blog Kaspersky, 2019
 - <https://www.kaspersky.es/blog/digital-steganography/18791/>
- Steganography tools, Wikipedia
 - https://en.wikipedia.org/wiki/Steganography_tools

Lectura recomendada (2/2)

- Steganography: A New Age of Terrorism - GIAC Certifications, SANS Institute, Stephanie R. Betancourt, 2004
 - <https://www.giac.org/paper/gsec/3494/steganography-age-terrorism/102620>
- How to Hide Secret Data Inside an Image or Audio File in Seconds, Black Slash, 2017
 - <https://null-byte.wonderhowto.com/how-to/steganography-hide-secret-data-inside-image-audio-file-seconds-0180936/>
- Secrets Hidden in Images (Steganography) - Computerphile, 2015
 - <https://www.youtube.com/watch?v=TWEXCYQKyDc>
- Privacidad y Ocultación de Información Digital Esteganografía. Protegiendo y Atacando Redes Informáticas, Alfonso Muñoz, Ra-Ma, 2016
 - https://www.ra-ma.es/libro/privacidad-y-ocultacion-de-informacion-digital-esteganografia_47926/

Class4crypt c4c5.5

Módulo 5. Fundamentos de la criptografía

Lección 5.5. Mecanismos y máquinas de cifra

5.5.1. Viaje histórico por los mecanismos, las máquinas y los personajes de la criptografía clásica

5.5.2. Cifradores de los siglos V, II y I antes de Cristo

5.5.3. Algunos cifradores a partir del siglo XV: Alberti, Vigenère, Jefferson, Playfair, Wheatstone, Bazeries y Hill

5.5.4. El telegrama de Zimmermann (WWI) y la máquina Enigma (WWII)

5.5.5. Personajes destacados: Allan Poe, Alan Turing y Claude Shannon

Class4crypt c4c5.5 Mecanismos y máquinas de cifra
<https://www.youtube.com/watch?v=89aLm5gPiVE>

Viaje histórico por los mecanismos de cifra

- Como la historia de la criptografía clásica es muy extensa, en las próximas diapositivas haremos un breve paseo histórico por las máquinas, mecanismos y artilugios de cifra más significativos, así como algunos personajes que han marcado ese tipo de criptografía
 - Escítala (s V a.C.)
 - Polibios (s II a.C.)
 - César (s I a.C.)
 - Alberti (1466)
 - Vigenère (1586)
 - Jefferson (1795)
 - Poe (1843)
 - Playfair (1854)
 - Wheatstone (1860)
 - Bazeries (1901)
 - Zimmermann (1917)
 - Enigma (1923)
 - Hill (1929)
 - Turing (1943)
 - Shannon (1949)

Cifrador escítala (siglo V antes de Cristo)

- Siglo V antes de Cristo: cifrador escítala
- Primer sistema de cifra conocido, usado por espartanos en la antigua Grecia
- Se trata de una cifra por permutación



- ¿Cómo funciona?
- Se escribe el texto longitudinalmente en una cinta enrollada en un bastón y éste se gira cuando se termina la fila
- Al desenrollar la cinta se obtiene un criptograma con letras desordenadas
- La clave es el diámetro del bastón

Cifrador de Polibio (siglo II antes Cristo)

- Siglo II antes de Cristo: cifrador de Polibio
- El historiador griego Polibio usaba como cifra una matriz de 5x5
- Es una cifra por sustitución
- Cada letra del texto en claro se lee como la intersección de una fila y una columna, dando lugar a un criptograma de dos letras
- Por ejemplo, la letras S se cifrará como como el digrama DC

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

- M = UN SALUDO
- C = DECCD CAACA DEADC D

Cifrador del César (siglo I antes de Cristo)

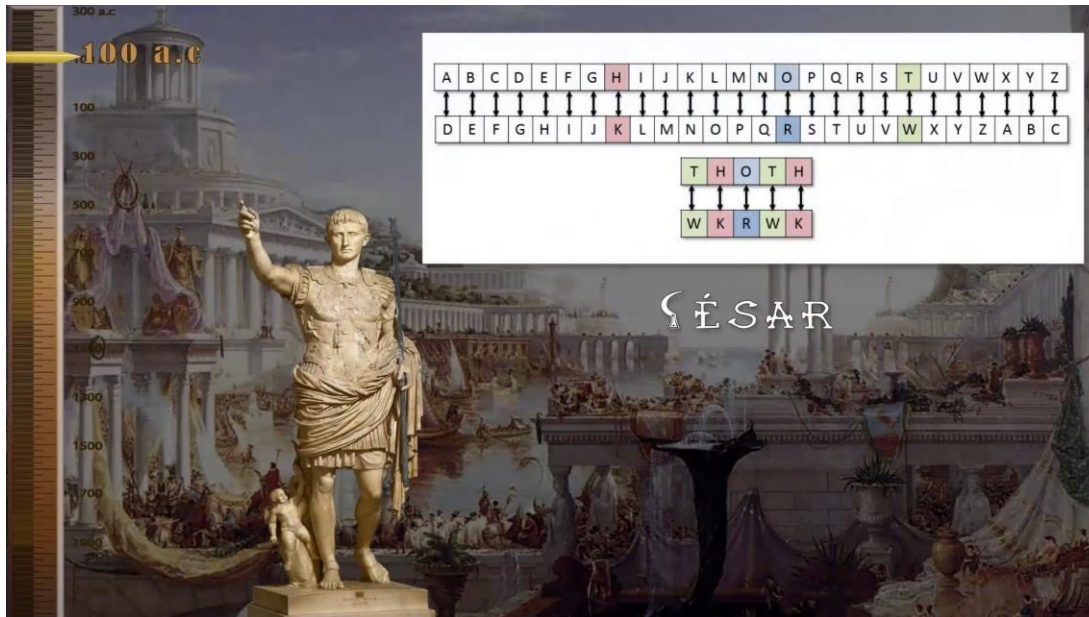
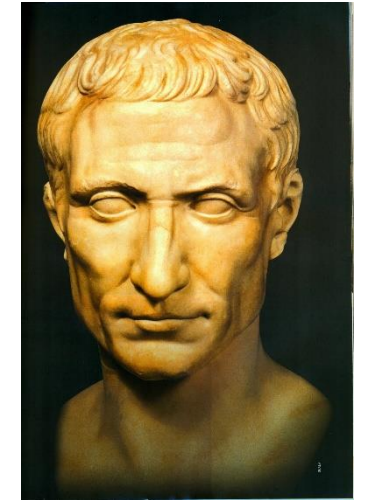
A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Cifrado: $C_i = M_i + 3 \bmod 27$

Descifrado: $M_i = C_i - 3 \bmod 27$

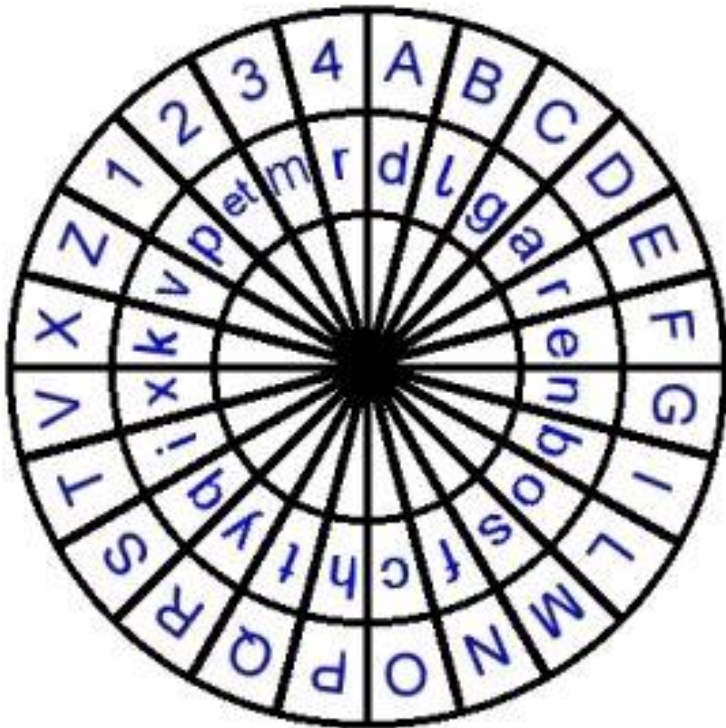
Alfabeto español

Se trata de una cifra por sustitución monoalfabética



- ¿Cómo funciona?
- Texto en claro M = AVE CESAR
- Criptograma C = DYH FHVDU
- Es demasiado elemental y se ataca fácilmente mediante fuerza bruta

Disco de Alberti (1466)



- Leon Battista Alberti da comienzo a la cifra polialfabética, puesto que puede moverse el disco interno durante la cifra según una clave y número de letras cifradas
- ¿Cómo funciona?
- En el disco exterior, letras en latín (no aparecen H, J, Ñ, K, U, W e Y) y los números 1, 2, 3, 4. En el disco interior en vez de números están & (et), h, k, y
- Si el texto en claro es M = EL SECRETO
- Se obtiene el criptograma C = roqrg yric

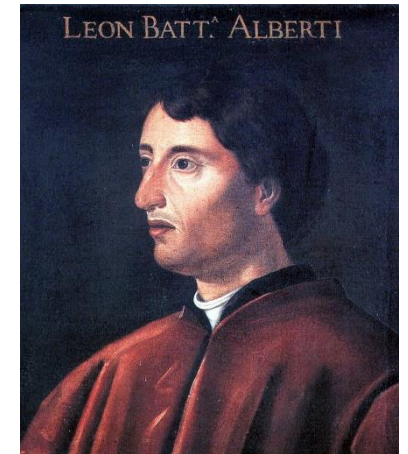


Tabla de Vigenère (1586)

- Cifrador polialfabético de Blaise de Vigenère
- Al usar más de un alfabeto, hacía muy difícil el ataque por simples estadísticas del lenguaje
- Durante más de 275 años fue indescifrable
- Se cifraba mediante la tabla que se muestra usando una clave



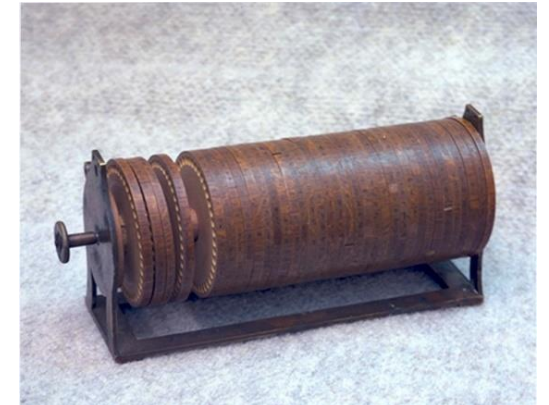
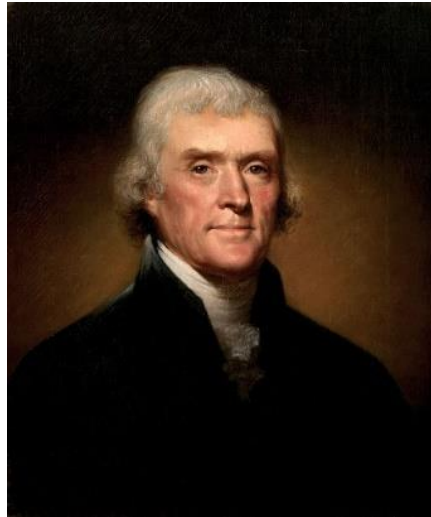
- ¿Cómo funciona?
- M = AMIGA
- CLAVE = UNO
- C = UYWAN
- $M + N \bmod 27 = Y$

TEXT O

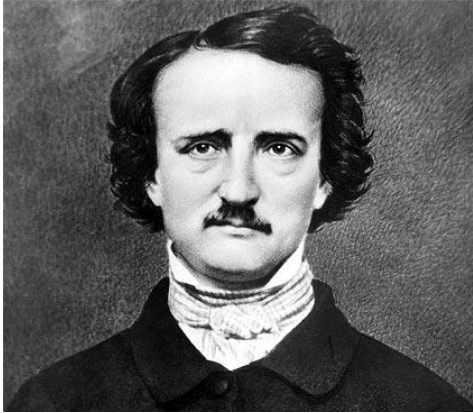
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	
C	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
L	1	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
A	2	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
V	3	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	4	E	F	G	H	I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

Cilindro de Jefferson (1795)

- Thomas Jefferson, conocido como padre de la criptografía americana, inventa en 1795 un sistema de cifra basado en un conjunto de discos con las 26 letras del alfabeto inglés
- ¿Cómo funciona?
- Emisor y receptor ponen los discos en el orden que indique la clave, por ejemplo, para 7 discos la clave puede ser 6, 3, 2, 4, 1, 7, 5. Para cifrar, el emisor rota cada disco hasta que se forme el mensaje deseado y pueda leerse en una fila. Para crear el criptograma, el emisor seleccionará cualquier otra fila, que lógicamente será un texto sin sentido

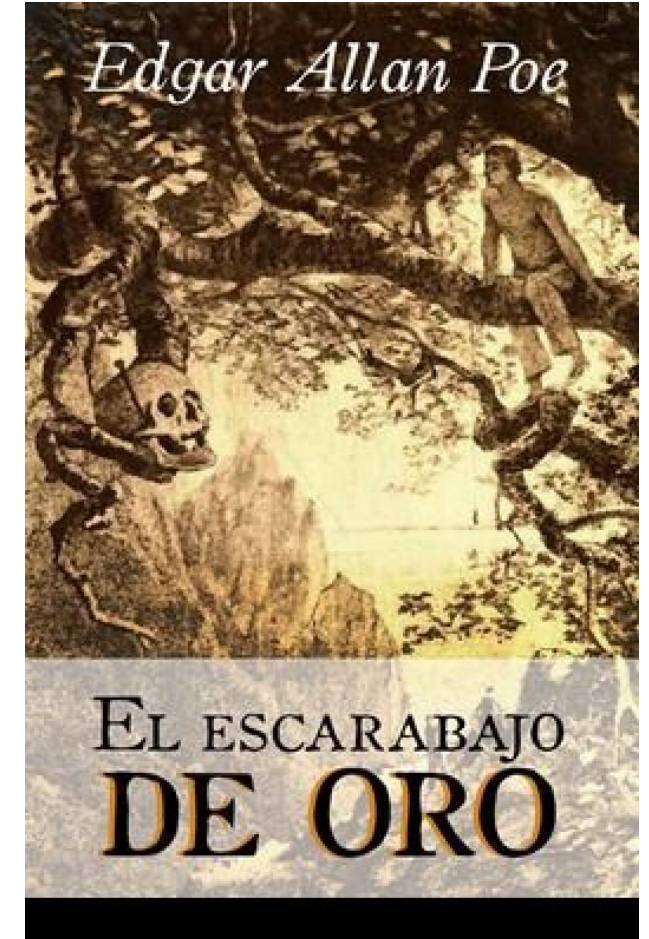


Edgar Allan Poe (1843)



- Publica en el Philadelphia Dollar Newspaper el primer cuento donde el criptoanálisis de un misterioso criptograma de cifra por sustitución monoalfabética, oculto mediante esteganografía, es la trama central

“Hace muchos años trabé íntima amistad con un caballero llamado William Legrand. Descendía de una antigua familia protestante y en un tiempo había disfrutado de gran fortuna, hasta que una serie de desgracias lo redujeron a la pobreza. Para evitar el bochorno que sigue a tales desastres, abandonó Nueva Orleans, la ciudad de sus abuelos, y se instaló en la isla de Sullivan, cerca de Charleston, en la Carolina del Sur.” ...



Cifrado de Playfair (1854)



Wheatstone



Playfair

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

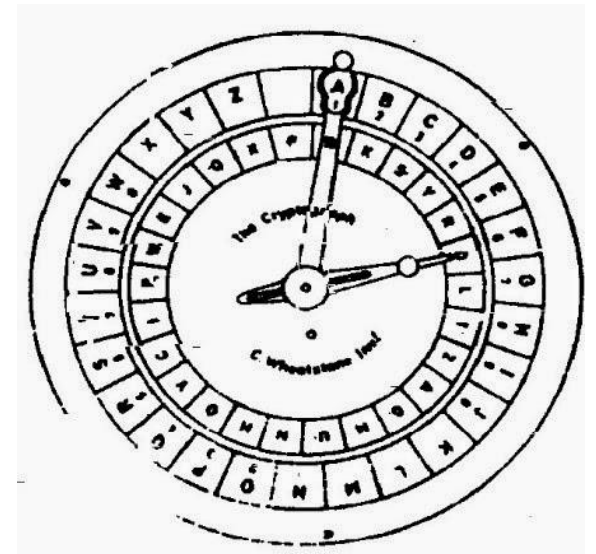
Clave: BEATLES

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

- Inventado por Charles Wheatstone, fue en realidad Lyon Playfair quien promueve su uso militar
- ¿Cómo funciona?
- Si M_1M_2 están en la misma fila, C_1C_2 son las dos letras de la derecha mod 5
- Si M_1M_2 están en la misma columna, C_1C_2 son las dos letras de abajo mod 5
- Si M_1M_2 están en filas y columnas distintas, C_1C_2 son las letras de la diagonal opuesta desde M_1
- $M = \text{YESTERDAY}$ se escribe en digramas y se usa relleno si fuese necesario $M = \text{YE ST ER DA YX}$
- $C = \text{WT FB TP KD ZY}$

Disco de Wheatstone (1860)

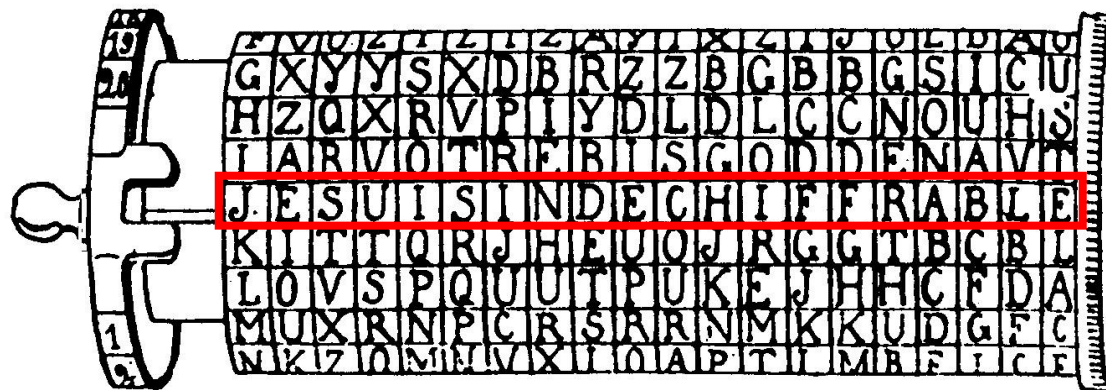
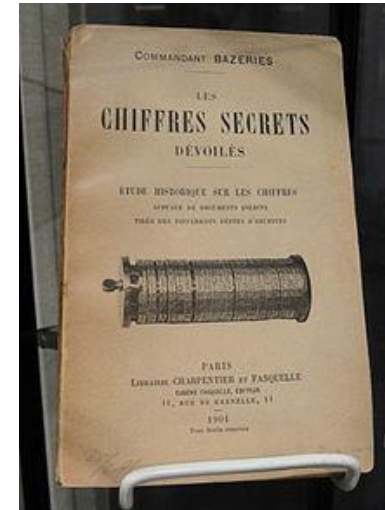
- El sistema de disco de *Wheatstone* (un invento de *Decius Wadsworth* en 1817) sigue básicamente el mismo principio de cifra que el disco de Alberti
- Pero, en este caso se utiliza el alfabeto inglés de 26 letras más el espacio en blanco para el texto en claro, representado de forma ordenada en el disco exterior
- El disco interior contiene solamente los 26 caracteres del lenguaje y se encuentran distribuidos aleatoriamente
- Muy importante: las agujas están engranadas de forma que cuando la externa gira 27 posiciones, la interna lo hace 26
- Esto hace que dos letras iguales seguidas en el texto en claro se cifren de forma diferente y que cada vez que se pase por un espacio en blanco, por una nueva palabra, se cambie la cifra



Cilindro de Bazeries (1901)



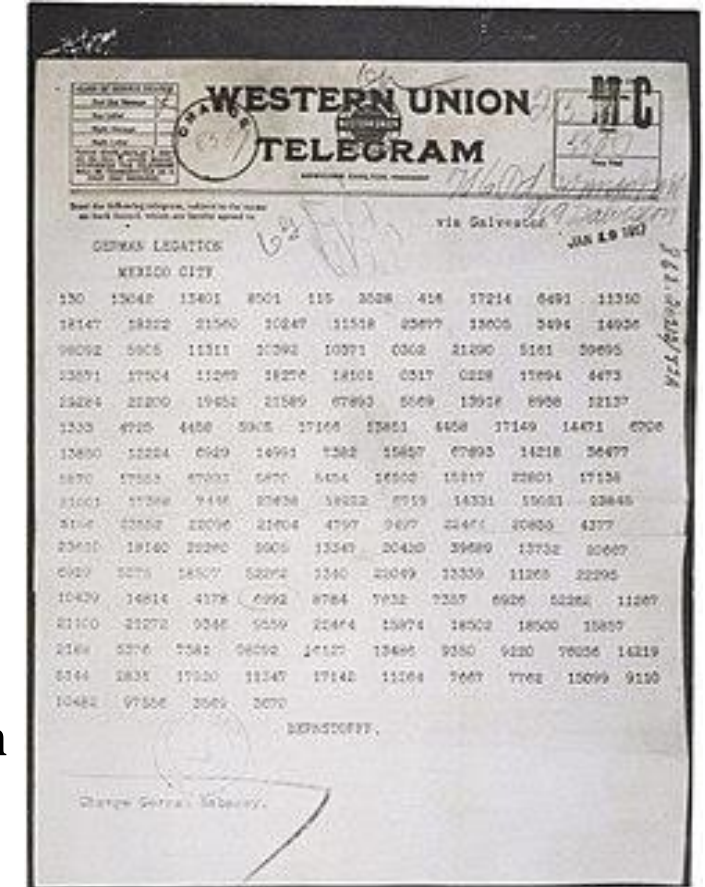
- El cifrador de Étienne Bazeries está basado en el cilindro de Jefferson, inventado 100 años antes por Thomas Jefferson



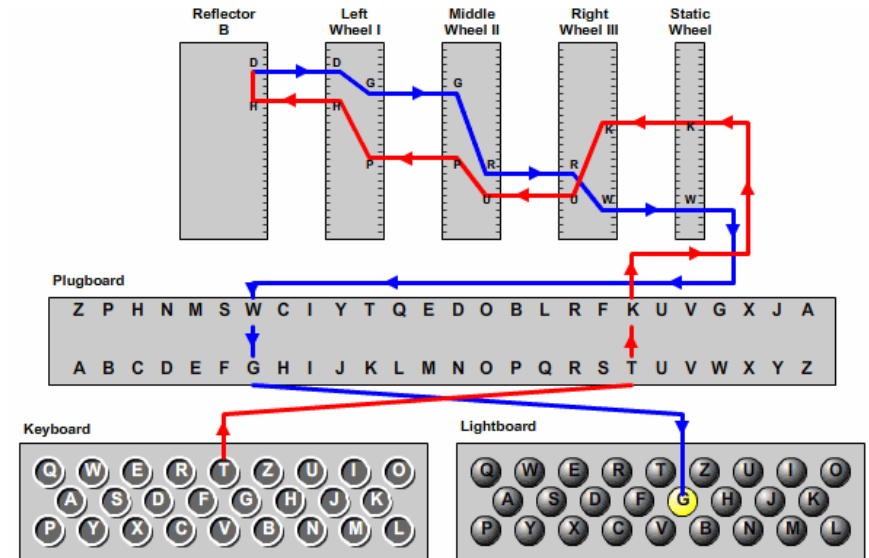
Zimmermann (1917)



- El 17 de enero de 1917 William Montgomery, criptoanalista de la sección diplomática de la Habitación 40 del Almirantazgo de la Marina Británica en Londres, intercepta un telegrama cifrado que el Ministro de Relaciones Exteriores alemán, Arthur Zimmermann, envía a su embajador en México
- Tras romper la cifra, descubren que el mensaje anunciaba una alianza con México para atacar a los Estados Unidos, a cambio de recuperar territorios de Texas, Nuevo México y Arizona
- Esto precipita que los EEUU entrasen en la primera confrontación bélica mundial, declarando la guerra a Alemania
- David Khan (1967): *"Nunca un único criptoanálisis ha tenido tan enormes consecuencias"*



Enigma (1923)



- Patentada en 1918 por Scherbius & Ritter, se puso a la venta en 1923 para su uso comercial
- En 1926 la Armada alemana la adopta para uso militar y poco después se extiende a las demás fuerzas armadas alemanas
- Tuvo un gran protagonismo antes y durante la Segunda Guerra Mundial

Matrices de Hill (1929)



- Se cifran bloques de dos o más letras con una matriz clave, que debe tener inversa en el módulo de cifra
- Pueden alcanzarse espacios de clave inmensos. Si n es primo y el bloque b letras: espacio $\approx n^{b^2}$ ($n = 37$, $b = 8$, espacio = $37^{64} \approx 2^{333}$)
- No obstante, este sistema poligrámico inventado por Lester Hill será vulnerable a ataques por texto en claro conocido

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \text{ mod } 26$$

- $P = P_1 P_2 P_3 = \text{SOL}$
- $C = C_1 C_2 C_3 = \text{XEY}$



- Si $M = \text{SOLEDAD}$, $P_1 P_2 P_3 = \text{SOL} = 18 \ 14 \ 11 \Rightarrow \text{mod } 26$
- Sea $K = K_{11} K_{12} K_{13} = 13 \ 22 \ 19$, $K_{21} K_{22} K_{23} = 14 \ 01 \ 14$, $K_{31} K_{32} K_{33} = 01 \ 09 \ 08$ (con inversa $K^{-1} \text{ mod } 26$)
- $C_1 = K_{11} * P_1 + K_{12} * P_2 + K_{13} * P_3 \text{ mod } 26$
- $C_1 = 13 * 18 + 22 * 14 + 19 * 11 \text{ mod } 26 = 234 + 308 + 209$
- $C_1 = 751 \text{ mod } 26 = 23 = X \dots \text{etc.}$

Turing (1943)



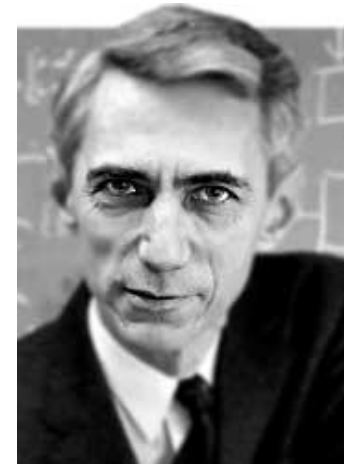
- Alan Turing es tal vez uno de los personajes más influyentes en la historia de la criptografía de los últimos 100 años
- Es el precursor de la informática y de muchos inventos (máquina de Turing, CAPTCHA, etc.)



- Basado en el trabajo previo del matemático polaco Marian Rejewski, en Bletchley Park, en las afueras de Londres, Turing descifra los mensajes dirigidos a las tropas nazis cifrados con la máquina Enigma
- En 1943 se rompían 85.000 mensajes al mes

Shannon (1949)

- Claude Elwood Shannon, sienta las bases de la teoría de la información, aplicada a la criptografía y al secreto de los sistemas
- En 1948 y 1949 publica dos artículos muy importantes
- Además de entropía, ratio y redundancia del lenguaje, etc., define los sistemas con y sin secreto perfecto
- Class4crypt
 - 4.1. Cantidad de información e incertidumbre
 - 4.2. Entropía de la información y codificador óptimo
 - 4.3. Ratio y redundancia del lenguaje
 - 4.4. Secreto perfecto y distancia de unicidad
 - 4.5. Métodos de difusión y confusión en la criptografía



Pionero de la IA (1956)

Más información en píldoras Thoth



Píldora 3: ¿Desde cuándo existe la criptografía?

<https://www.youtube.com/watch?v=jmvO3VoJeKg>



Píldora 8: ¿Qué relación existe entre Alan Turing y la criptografía?

<https://www.youtube.com/watch?v=Qwpm5ttnnbs>

Conclusiones de la Lección 5.5

- La historia de la criptografía clásica data desde el siglo V antes de Cristo y podemos situarla hasta mediados del siglo XX
- Los sistemas de cifra eran maquinarias o simples artilugios, algunos de ellos muy ingeniosos y seguros para su época, sin la ayuda de los ordenadores
- Hay un gran número de investigadores, científicos e incluso escritores, que han aportado su grano de arena en el desarrollo de la criptografía
- Todo este desarrollo ha permitido que la criptografía actual sea una ciencia muy sólida, incluso teniendo hoy el gran desafío de la computación cuántica
- En este breve paseo histórico solo hemos podido mostrar a algunos de ellos
- En la bibliografía anexa encontrarás una gran cantidad de información

Lectura recomendada (1/3)

- Guion píldora formativa Thoth nº 3, ¿Desde cuándo existe la criptografía?, Jorge Ramió, 2014
 - <https://www.criptored.es/thoth/material/texto/pildora003.pdf>
- Guion píldora formativa Thoth nº 8, ¿Qué relación existe entre Alan Turing y la criptografía?, Jorge Ramió, 2014
 - <https://www.criptored.es/thoth/material/texto/pildora008.pdf>
- Los doce césares, Cayo Suetonio Tranquilo, Edición eBooket
 - <https://uhphistoria.files.wordpress.com/2011/02/gaio-suetonio-los-doce-cesares.pdf>
- El escarabajo de Oro, Edgar Allan Poe, 1843
 - <https://ciudadseva.com/texto/el-escarabajo-de-oro/>

Lectura recomendada (2/3)

- El telegrama a México que definió la suerte de la Primera Guerra Mundial, BBC, Noviembre 2018
 - <https://www.bbc.com/mundo/noticias-46126084>
- The Enigma encryption machine, Khan Academy
 - <https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/case-study-ww2-encryption-machines>
- Alan Turing: El descifrado de la máquina Enigma, El País, Josep María Miret, Universitat de Lleida, 2013
 - <https://blogs.elpais.com/turing/2013/06/alan-turing-el-descifrado-de-la-maquina-enigma.html>
- The Codebreakers, David Khan, 1967, nueva edición 1996, microsiervos
 - <https://www.microsiervos.com/archivo/libros/the-codebreakers.html>

Lectura recomendada (3/3)

- A mathematical theory of communication, Claude Shannon, Bell System Technical Journal 27 (1948)
 - <http://www.essrl.wustl.edu/~jao/itrg/shannon.pdf>
- Communication theory of secrecy systems, Claude Shannon, Bell System Technical Journal 28 (1949)
 - <https://pages.cs.wisc.edu/~rist/642-spring-2014/shannon-secrecy.pdf>
- Códigos Ocultos, Pierre Berloquin, 2020
 - <https://www.amazon.es/CODIGOS-OCULTOS-ENCRIPACION-MENSAJES-HISTORIA/dp/9463593284>

Class4crypt c4c5.6

Módulo 5. Fundamentos de la criptografía

Lección 5.6. Clasificación de los sistemas de cifra clásica

5.6.1. ¿Qué se entiende por cifra clásica?

5.6.2. Frontera entre la criptografía clásica y la criptografía moderna

5.6.3. Clasificación histórica de los sistemas de cifra

5.6.4. Algunos sistemas de cifra clásica representativos

5.6.5. Clasificación de los criptosistemas de cifra clásica

5.6.6. Debilidades de los criptosistemas de cifra clásica

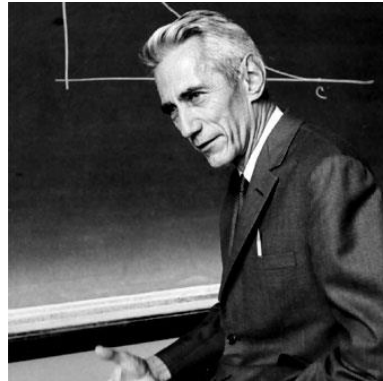
Class4crypt c4c5.6 Clasificación de los sistemas de cifra clásica
https://www.youtube.com/watch?v=pq8weLd7a_Y

¿Qué entendemos por cifra clásica?

- Aunque puede haber más interpretaciones, la cifra clásica incluye a aquellos sistemas criptográficos utilizados hasta de la mitad del siglo XX
 - Desde el siglo V antes de Cristo (Escítala)
 - Hasta la Segunda Guerra Mundial (Enigma y similares)
 - En todo caso, una criptografía en la que los algoritmos de cifra no se ejecutaban en computadores digitales (ENIAC se inventa en 1944)
- Una gran cantidad de estos sistemas fueron artilugios mecánicos o máquinas de cifra, como por ejemplo la famosa máquina Enigma
- Aquí y en las siguientes clases de este módulo, nos centraremos en algoritmos de cifra cuyas operaciones de cifrado y de descifrado puedan representarse por una ecuación de matemática discreta (aritmética modular) sencilla

Frontera entre cifra clásica y moderna

- Tendremos en cuenta los hitos importantes de la criptografía moderna
- Ya que esto nos permitirá encontrar la frontera entre la cifra clásica y la cifra moderna



Claude Shannon: 1948 - 1949



Hertz Feistel: 1974

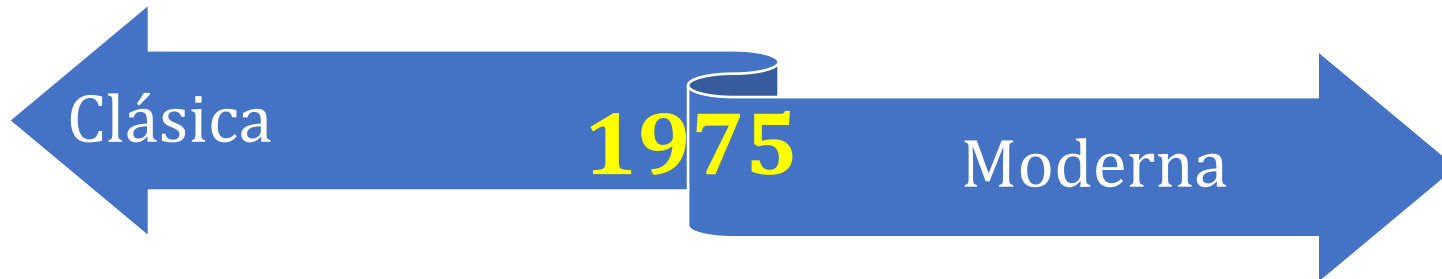


Whitfield Diffie y Martin Hellman: 1976

¿Si nos pidieran un año que represente a la cifra moderna?

1975: uso civil

Clasificación histórica de criptosistemas



- Esta no es la mejor clasificación desde el punto de vista de la ingeniería y de la informática
 - Pero permitirá comprobar el desarrollo de estas técnicas de cifra, hoy en día rudimentarias y simples, desde una perspectiva histórica y además resulta culturalmente interesante para un ingeniero
- La criptografía clásica nos permitirá criptoanalizar con cierta facilidad prácticamente todos estos sistemas de cifra
 - Y entre otras cosas comprobar también las teorías de Claude Shannon sobre las características y redundancia del lenguaje

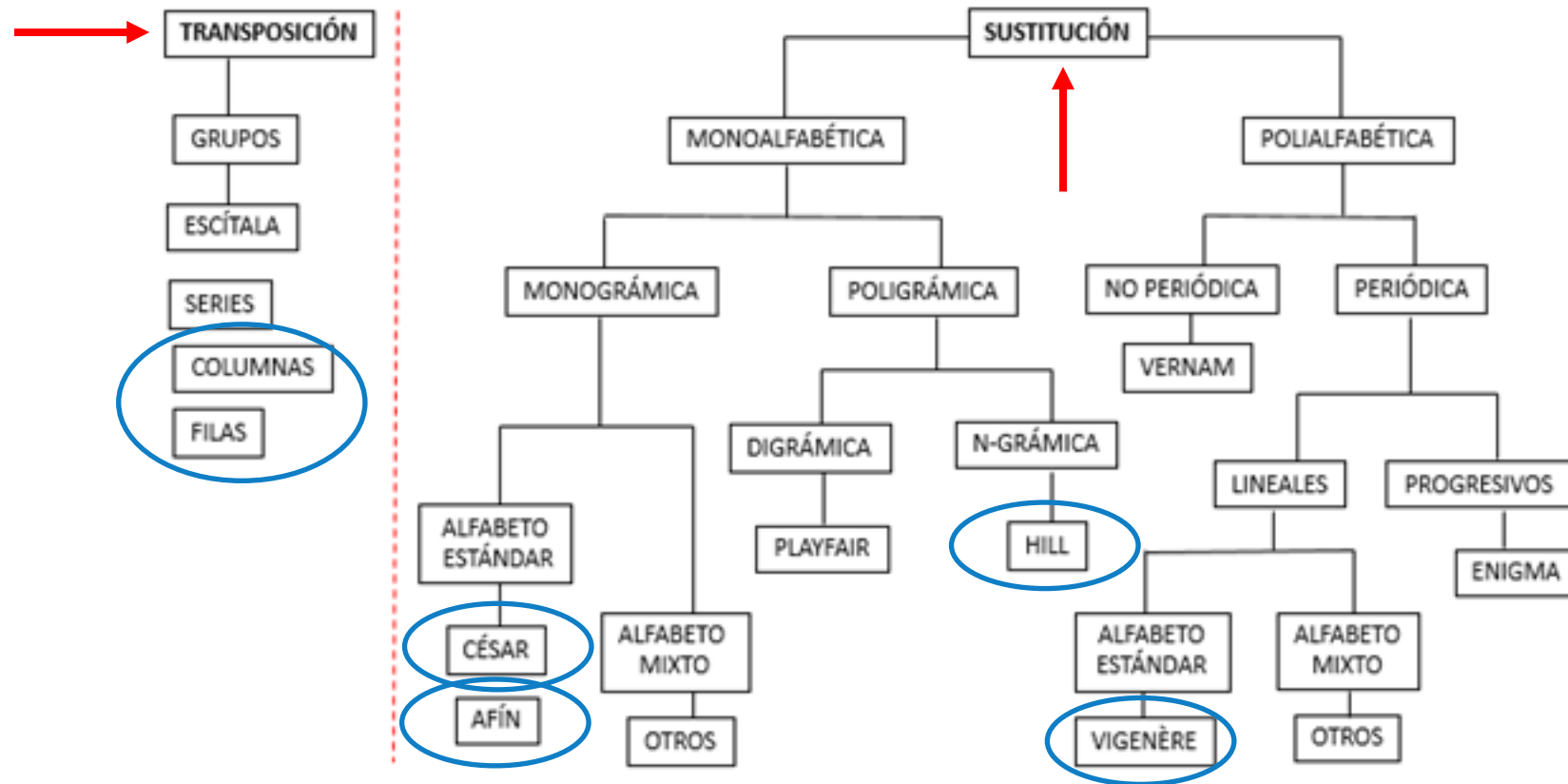
Detalles cronológicos de la cifra clásica (1)

- En la edad antigua (Desde el año 4.000 a.C hasta el siglo IV)
 - Los espartanos cifran mensajes utilizando la escítala
 - El historiador griego Polybius describe el cifrado de Polybius
 - Julio César usa un método para cifrar sus mensajes
- En la edad media (desde el siglo V hasta el siglo XV)
 - Leon Battista Alberti publica "Modus scribendi in ziferas" en donde habla por primera vez del disco de Alberti, el primer sistema polialfabético
 - El diplomático francés Blaise de Vigenère publica "Tractié de Chiffre" en donde presenta el primer sistema polialfabético con autoclave, conocido como "Le chiffre indéchiffrable" aunque más adelante se le cambiará el nombre por el de cifrado de Vigenère (es del siglo XVI)

Detalles cronológicos de la cifra clásica (2)

- En la edad contemporánea (Desde finales siglo XVIII hasta hoy)
 - Friedrich Kasiski desarrolla métodos estadísticos de criptoanálisis que fueron capaces de romper el cifrado de Vigenère
 - "La Cryptographie militaire" de Auguste Kerckhoff von Nieuwendhoff contiene el "principio de Kerckhoff" que exige basar la seguridad de un método de cifrado únicamente al secreto de la clave y no en el algoritmo
 - Lester S. Hill publica el artículo "Cryptography in an Algebraic Alphabet" y el cifrado de Hill que aplica álgebra, multiplicación modular de matrices
 - Máquinas de cifrado mecánicas y electromecánicas, como la máquina Enigma que Alan Turing rompe usando la idea de la bomba de Turing, que concibió basándose en el trabajo previo de Marian Rejewski

Clasificación de los sistemas de cifra clásica



Debilidades de la cifra clásica

- Los algoritmos de cifra clásica que estudiaremos en las próximas clases son fácilmente criptoanalizables
- Por el análisis estadístico de las letras en el criptograma
 - Permutación por filas y columnas
 - Sustitución monoalfabética monográfica del César, Decimación y Afín
 - Sustitución polialfabética monográfica de Vigenére
- Por las propiedades lineales de las operaciones matemáticas realizadas en la cifra
 - Sustitución poligrámica matricial de Hill

Más información en píldoras Thoth



<https://www.youtube.com/watch?v=IyKa2iE31tU>

Conclusiones de la Lección 5.6

- Diferenciamos entre cifra clásica y cifra moderna al aplicar una clasificación histórica o cronológica de los criptosistemas
- Los hechos que producen el cambio entre cifra clásica y moderna son la irrupción de los computadores en los algoritmos de cifra y 3 hitos muy importantes en la criptografía acaecidos en los años 1948, 1974 y 1976
 - Claude Shannon, Horst Feistel, Diffie y Hellman
- La cifra clásica se clasifica entre sistemas de cifra por permutación y sistemas de cifra por sustitución
- La cifra por sustitución ha tenido un mayor recorrido temporal que la cifra por permutación
- Los algoritmos de cifra clásica son todos criptoanalizables

Lectura recomendada

- Introducción a la seguridad informática y criptografía clásica, Lección 6 Sistemas de cifra clásica, MOOC Crypt4you, Jorge Ramió, 2016
 - <https://www.criptored.es/crypt4you/temas/criptografiaclasica/leccion6.html>
- Breve Historia de la Criptografía Clásica, José Luis Tábara
 - <https://docplayer.es/10148368-Breve-historia-de-la-criptografia-clasica.html>
- Guion píldora formativa Thoth nº 10, ¿Cómo se clasifican los sistemas de cifra clásica?, Jorge Ramió, 2014
 - <https://www.criptored.es/thoth/material/texto/pildora010.pdf>
- Criptografía Clásica, Libro Electrónico de Seguridad Informática y Criptografía Versión 4.1, Jorge Ramió, 2006
 - https://www.criptored.es/guiateoria/gt_m001a.htm

Class4crypt c4c5.7

Módulo 5. Fundamentos de la criptografía clásica y moderna

Lección 5.7. Introducción a la criptografía moderna

- 5.7.1. Objetivos, definiciones y diferencias entre la criptografía clásica y la moderna
- 5.7.2. Hitos que marcan el cambio de la criptografía clásica a la criptografía moderna
- 5.7.3. Clasificación de la cifra moderna según el tipo de claves utilizadas
- 5.7.4. Clasificación de la cifra moderna según el tratamiento de la información
- 5.7.5. Introducción a los métodos y algoritmos de cifra modernos
- 5.7.6. Introducción a la cifra en flujo y a la cifra en bloque
- 5.7.7. Introducción a la cifra simétrica y a la cifra asimétrica

Class4crypt c4c5.7 Introducción a la criptografía moderna
<https://www.youtube.com/watch?v=7sBDKQbluNk>

Criptografía clásica: orígenes y objetivos

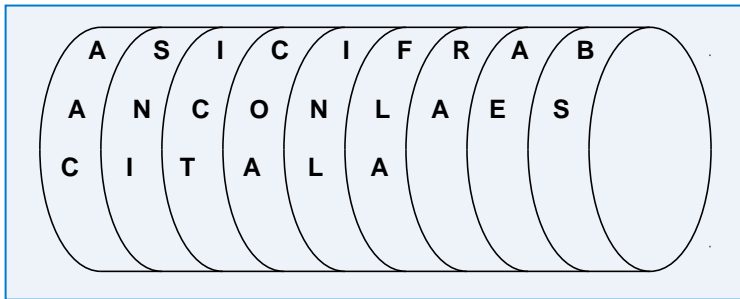
- Los orígenes de la criptografía se remontan al siglo V a.d.C. con el artilugio conocido como escítala, que usaba un pueblo griego para proteger su información
- Y se extiende hasta después de la Segunda Guerra Mundial, con el surgimiento de la computación y los sistemas informáticos a mediados del siglo XX
- El objetivo básico de la criptografía clásica era encontrar sistemas que permitiesen hacer llegar a alguien determinada información considerada secreta, desde un lugar de origen a otro de destino, de forma tan segura que si esa información fuese interceptada por un tercero, no se pudiese reconocer el mensaje original
- Otro tanto podríamos decir en cuanto a almacenar dicha información secreta para un uso posterior, solamente por parte de quien o quienes posean una clave secreta para descifrarla

Criptografía moderna: orígenes y objetivos

- La criptografía moderna puede considerarse como tal después de la Segunda Guerra Mundial, a mediados del siglo XX, hasta nuestros días. Con el nacimiento de la computación, comienzan a aparecer algoritmos criptográficos cuyo código es un programa binario que se ejecuta en una máquina digital o computadora
- El objetivo de la criptografía moderna sigue siendo -como en la clásica- dotar a la información de confidencialidad o secreto, pero además se preocupa de la integridad de dicha información y de la autenticidad del emisor
- Plantea nuevas formas de protección, válidas cuando la información está digitalizada (almacenada o transmitida) y no sólo cuando se transcribe a un papel para su envío, como en la cifra clásica
- ¿Se seguirá denominando criptografía moderna cuando la computación cuántica con centenas o miles de cúbits sea una realidad y usemos ya algoritmos postcuánticos?

Representación gráfica de las dos épocas

- Escítala siglo V a.d.C.



- Máquina Enigma (2ª Guerra Mundial)



Información de la página - https://www.amazon.es/

General Medios Permisos Seguridad

Identidad del sitio web

Sitio web: www.amazon.es

Propietario: Este sitio web no proporciona información sobre su dueño.

Verificado por: DigiCert Inc [Ver certificado](#)

Expira el: sábado, 12 de septiembre de 2020

Privacidad e historial

¿Se ha visitado este sitio web anteriormente? Sí, 70 veces

¿Este sitio web almacena información en mi ordenador? Sí, cookies y 48,0 KB de datos del sitio [Limpiar cookies y datos del sitio](#)

¿Se han guardado contraseñas de este sitio web? No [Ver contraseñas guardadas](#)

Detalles técnicos

Conexión cifrada (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, claves de 128 bits, TLS 1.2)

La página que está viendo fue cifrada antes de transmitirse por Internet.

El cifrado dificulta que personas no autorizadas vean la información que viaja entre sistemas. Es, por tanto, improbable que nadie lea esta página mientras viajó por la red.

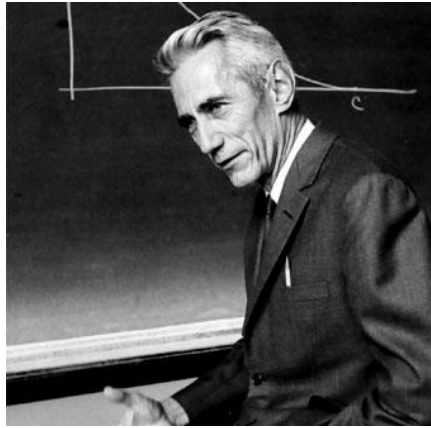
[Ayuda](#)

- Certificado digital X.509
Amazon (27/04/2020)

Algunos hitos que marcan el cambio



Gráficamente...



1948 - 1949

Claude Shannon



1974

Hertz Feistel



1976

Whitfield Diffie y Martin Hellman

¿Cómo se clasifica la criptografía moderna?

- **Según el tipo de claves**

1. Simétricos o de clave secreta. Existirá una única clave (secreta) que deben compartir emisor y receptor. Con la misma clave se cifra y se descifra. Por usar la misma clave, se denominan “simétricos”
2. Asimétricos o de clave pública. Cada usuario crea un par de claves, una privada y otra pública, inversas dentro de un módulo. Lo que se cifra en emisión con una clave, se descifra en recepción solamente con la clave inversa. Por usar claves diferentes, se denominan “asimétricos”

- **Según el tratamiento del mensaje o texto en claro**

1. Cifrado en flujo. El mensaje en claro se cifra bit a bit (o byte) con la clave
2. Cifrado en bloque. El mensaje en claro se divide en bloques de algunos bytes, aplicando a continuación la cifra a cada uno de ellos con la clave

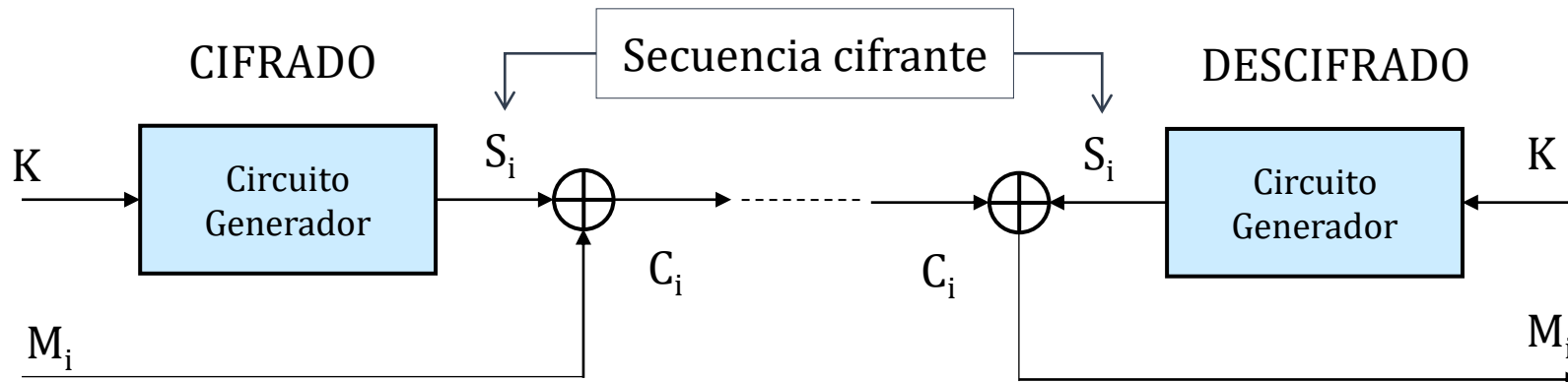
Métodos y algoritmos de cifra moderna



Introducción al cifrado en flujo

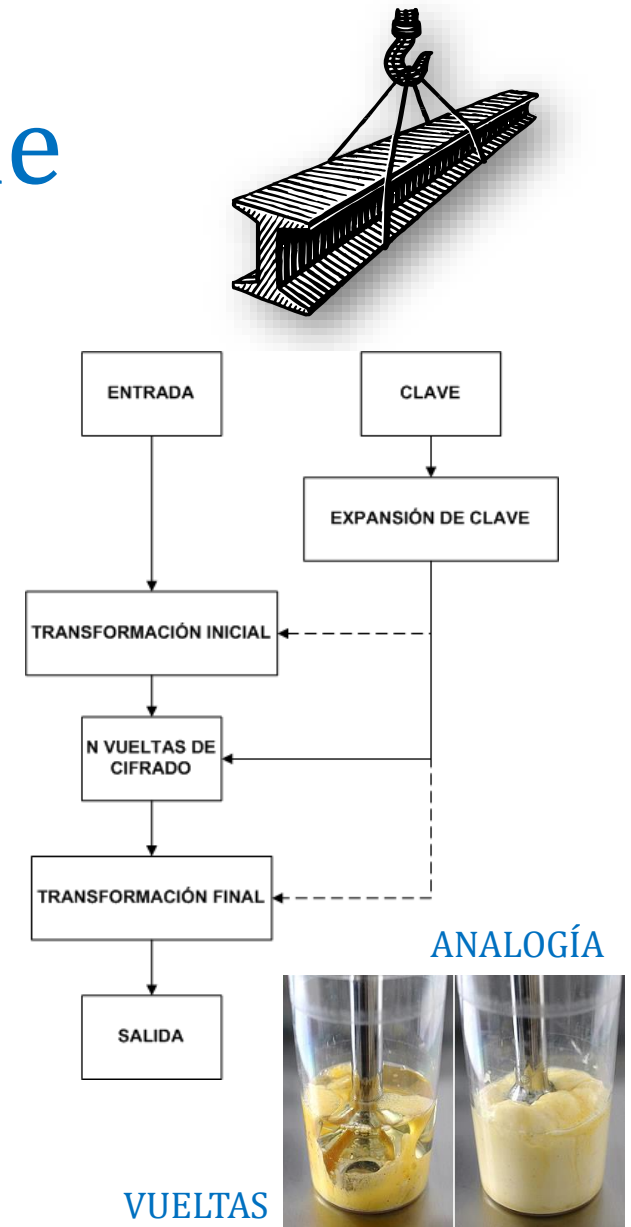
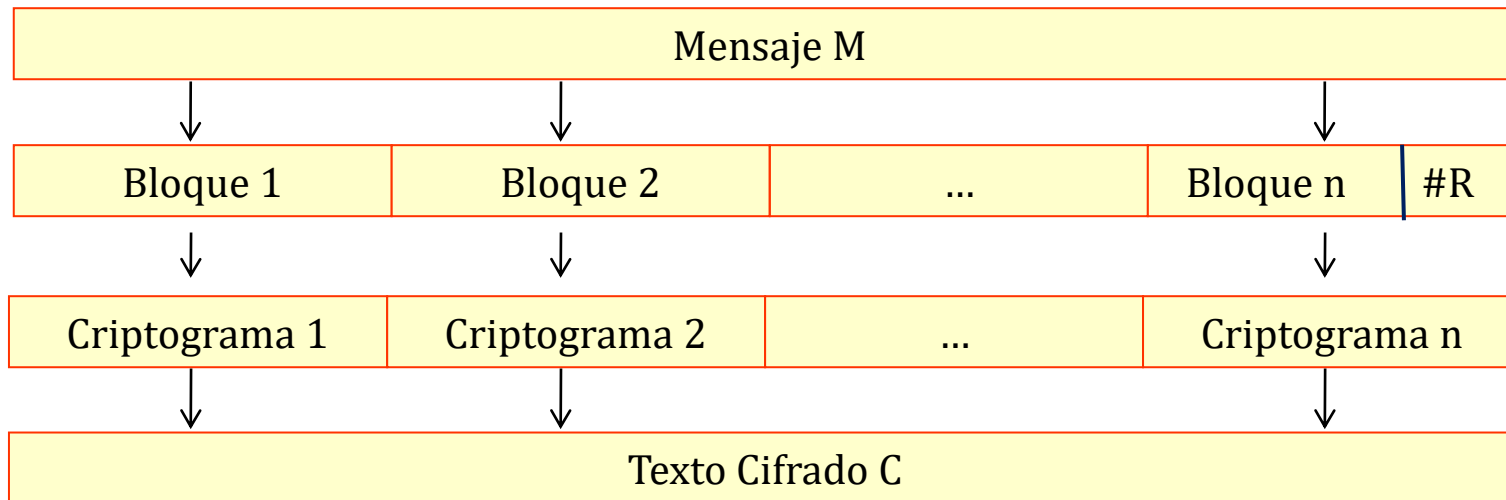


- El mensaje en claro se cifra bit a bit o byte a byte
- Dicha operación de cifra consiste en una operación XOR del texto en claro con una **secuencia cifrante** de bits S_i que debe cumplir ciertas condiciones para que tenga una apariencia aleatoria y sea segura
- Para descifrar, se vuelve a realizar un XOR del criptograma con la misma secuencia S_i pues esta función XOR es involutiva (función matemática que es su propia inversa)



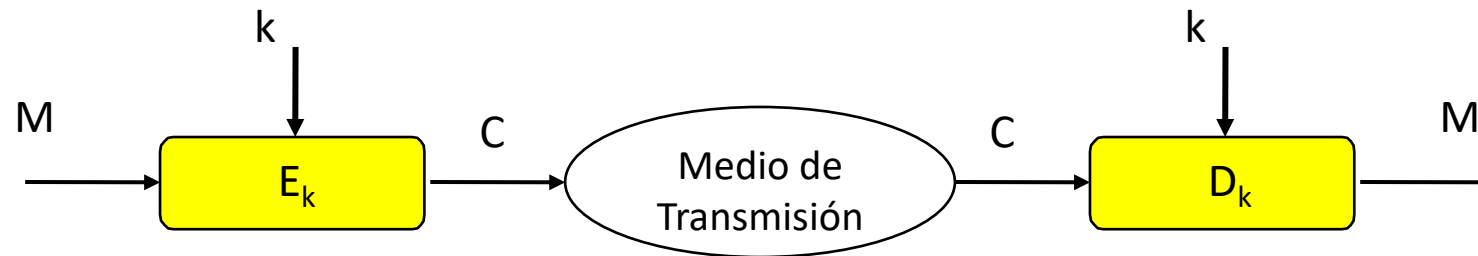
Introducción al cifrado en bloque

- Se denomina cifrado en bloque a aquella cifra en la que el mensaje original se agrupa en bloques de X bytes antes de proceder a la cifra
- Un bloque pequeño (1 byte) facilitaría un ataque por estadísticas del lenguaje. Un bloque grande (miles de bytes) supondría un tratamiento no adecuado del texto en claro

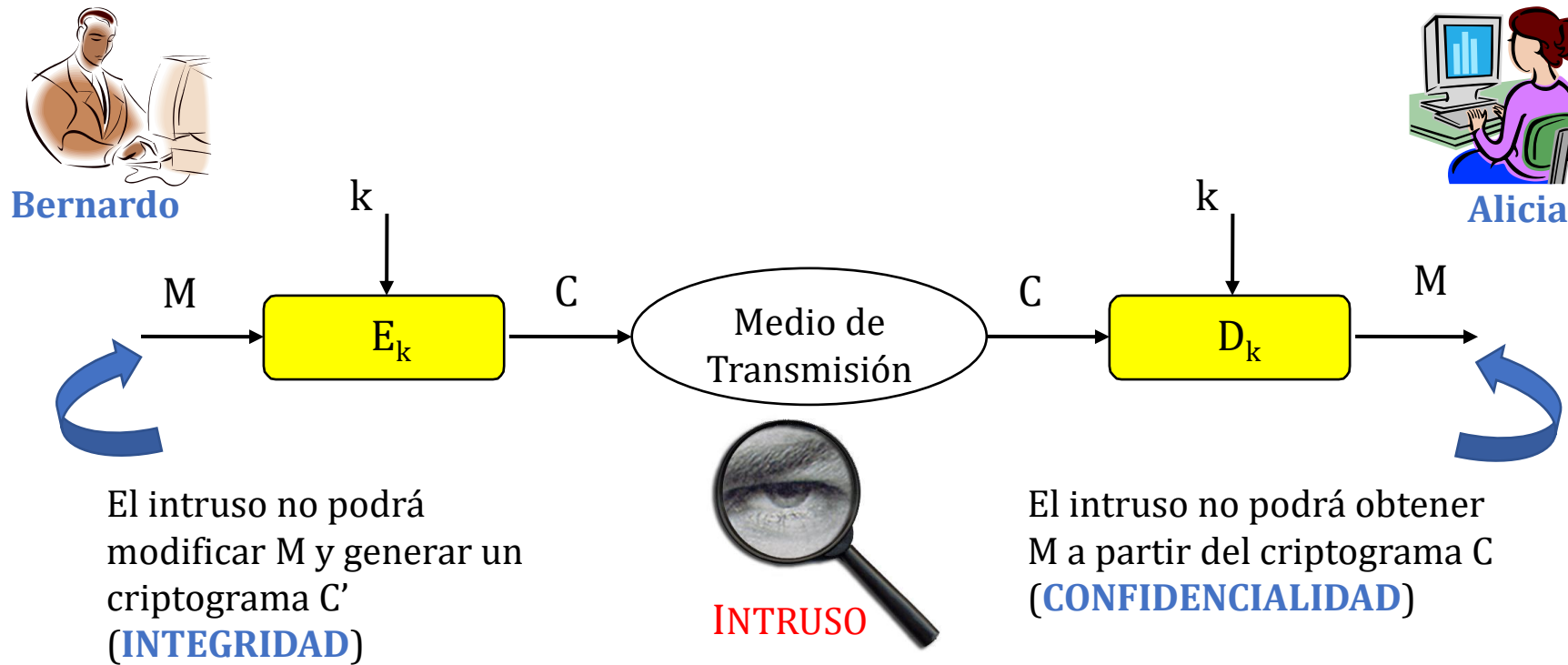


Introducción a la cifra simétrica CS

- El emisor toma el mensaje en claro M que transforma mediante un algoritmo E_k utilizando la clave k secreta para obtener el mensaje cifrado C . Posteriormente, el mensaje cifrado se transmite al receptor, que recibe el criptograma C
- El receptor para la operación de descifrado, toma como entrada el criptograma C y le aplica el algoritmo D_k igual que el de emisión E_k pero en modo descifrado, utilizando la misma clave k , para obtener el mensaje en claro M . D_k es el proceso inverso a E_k



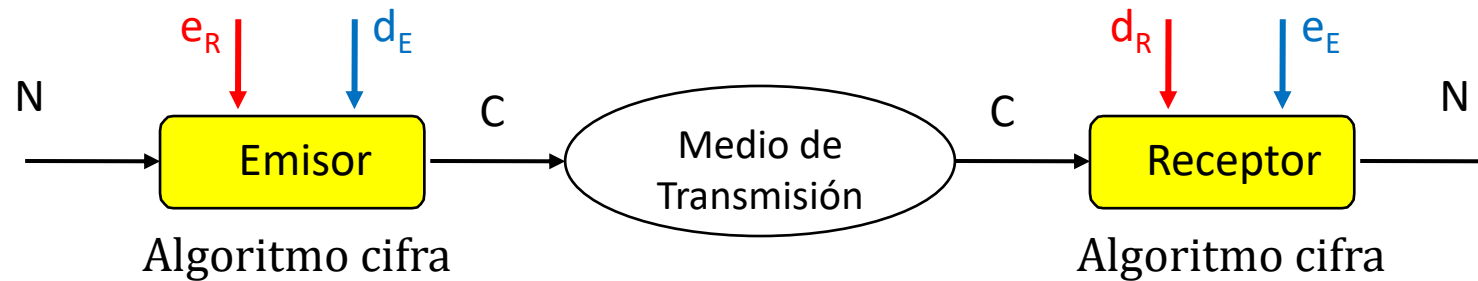
Confidencialidad e integridad en CS



La confidencialidad y la integridad se lograrán si se protegen las claves en el cifrado y en el descifrado, es decir, ambas se obtienen simultáneamente si se protege k , la clave secreta compartida.

Introducción a la cifra asimétrica CA

- Emisor y receptor poseen dos claves, una pública e por todos conocida y otra privada d solo conocida por su dueño. El conocimiento de la clave pública no pone en peligro la privada
- En emisión se cifra con la clave pública del Receptor e_R para lograr la **confidencialidad**. En recepción se descifra con la clave privada del Receptor d_R (**módulo receptor**)
- En emisión se cifra con la clave privada del Emisor d_E para lograr la **integridad** y además la **autenticidad**. En recepción se descifra con la clave pública del Emisor e_E (**módulo emisor**)



Confidencialidad en CA



Bernardo

$e_B \rightarrow$ Clave pública
 $d_B \rightarrow$ Clave privada



Alicia

$e_A \rightarrow$ Clave pública
 $d_A \rightarrow$ Clave privada

Cifrado con clave pública del receptor: Alicia



INTRUSO

No puede obtener M: Existe **CONFIDENCIALIDAD**

PROBLEMA: Puede introducir C' y no hay integridad

La **confidencialidad** se consigue ya que el destinatario podrá descifrar el criptograma C con su clave privada, que sólo él debería conocer. Ninguna otra clave servirá para descifrar C

Integridad (autenticidad) en CA



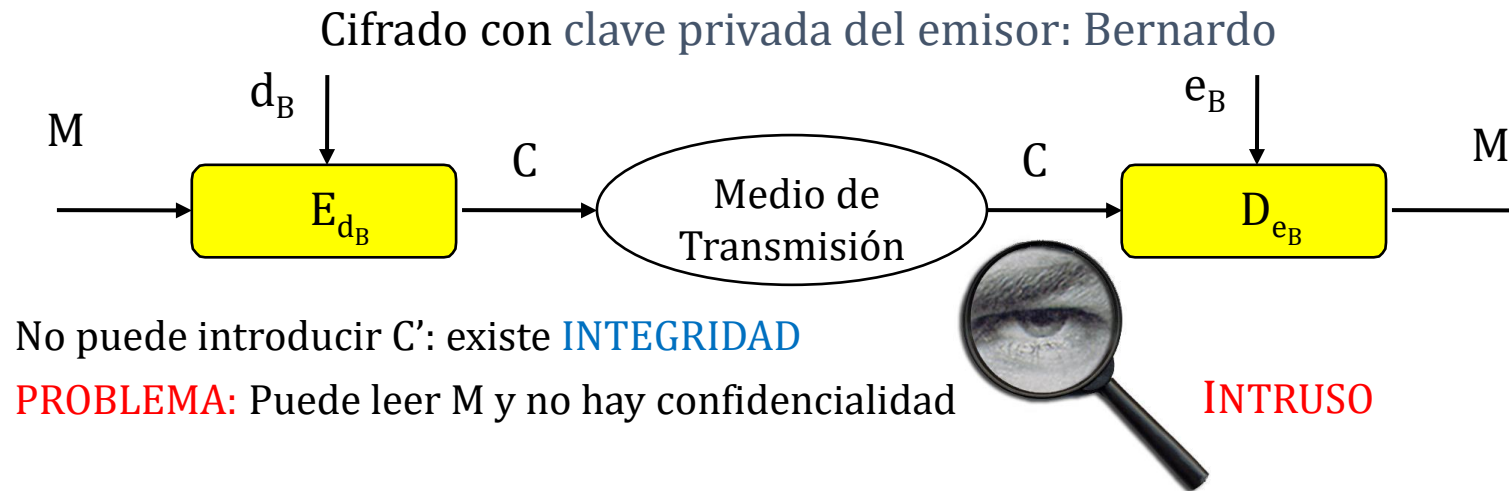
Bernardo

$e_B \rightarrow$ Clave pública
 $d_B \rightarrow$ Clave privada



Alicia

$e_A \rightarrow$ Clave pública
 $d_A \rightarrow$ Clave privada



Para conseguir la integridad del mensaje, el emisor debe utilizar su clave privada para cifrar y cualquiera puede descifrarlo utilizando su clave pública. Permite asegurar que sólo pudo haber sido el emisor quien empleó su clave privada (fundamento de la firma electrónica).

Confidencialidad e integridad en CA



Bernardo

$e_B \rightarrow$ Clave pública
 $d_B \rightarrow$ Clave privada

$e_A \rightarrow$ Clave pública
 $d_A \rightarrow$ Clave privada



Alicia

- En un sistema asimétrico, la confidencialidad y la integridad se obtienen por separado
- Una comunicación puede ser: secreta o confidencial para el receptor, ir firmada con autenticidad del emisor e integridad de la información, o ambas cosas, ser confidencial y, además, auténtica e íntegra
- Cuando se usa (cifra con) la clave pública del destinatario lo que se busca es la confidencialidad. Se utiliza para realizar de forma segura un intercambio de clave
- Cuando se usa (cifra con) la clave privada del emisor lo que se busca es la integridad; autenticar que el emisor es quien dice ser y que el mensaje es íntegro

Más información en píldoras Thoth



<https://www.youtube.com/watch?v=2ssaCyXRJIU>

Conclusiones de la lección 5.7

- La criptografía moderna no sólo se preocupa por dotar a la información de confidencialidad si ésta lo requiere, sino también de integridad y autenticidad
- Según el tipo de clave utilizada, la criptografía moderna se divide entre sistemas de cifra con clave secreta o simétricos y sistema de cifra con clave pública o asimétricos
- Según el tratamiento que hacemos de la información para su cifrado, en criptografía moderna se habla de cifrado en flujo y de cifrado en bloque
- Con la criptografía simétrica se obtiene confidencialidad e integridad de forma simultánea. En cambio, con la criptografía asimétrica la integridad y la confidencialidad se consiguen de forma separada
- Esto permite hablar con propiedad de intercambio de clave y de firma digital

Lectura recomendada

- A Mathematical Theory of Communication, The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, Claude E. Shannon, 1948
 - <http://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf>
- Communication Theory of Secrecy Systems, The Bell System Technical Journal, Vol. 28, pp. 656–715, Claude E. Shannon, 1949
 - <http://pages.cs.wisc.edu/~rist/642-spring-2014/shannon-secrecy.pdf>
- Guion píldora formativa Thoth nº 26, ¿Cómo se clasifican los sistemas de cifra moderna?, Jorge Ramió, 2012
 - <https://www.criptored.es/thoth/material/texto/pildora026.pdf>
- Curso de Criptografía Aplicada, capítulo 2.7 Características de los sistemas de cifra modernos, páginas 37 a 42, Jorge Ramió, 2018
 - <https://www.criptored.es/descarga/CursoCriptografiaAplicada2018.pdf>

Class4crypt c4c5.8

Módulo 5. Fundamentos de la criptografía clásica y moderna

Lección 5.8. Comparativa entre cifra simétrica y cifra asimétrica

5.8.1. Recordando las diferencias entre la cifra simétrica y la cifra asimétrica

5.8.2. Comparativa entre sistemas de cifra simétrica versus sistemas de cifra asimétrica

5.8.2.1. Ante la seguridad del sistema

5.8.2.5. Ante el intercambio de clave

5.8.2.2. Ante la gestión de las claves

5.8.2.6. Ante la firma digital

5.8.2.3. Ante el espacio de las claves

5.8.2.7. Ante la velocidad de cifra

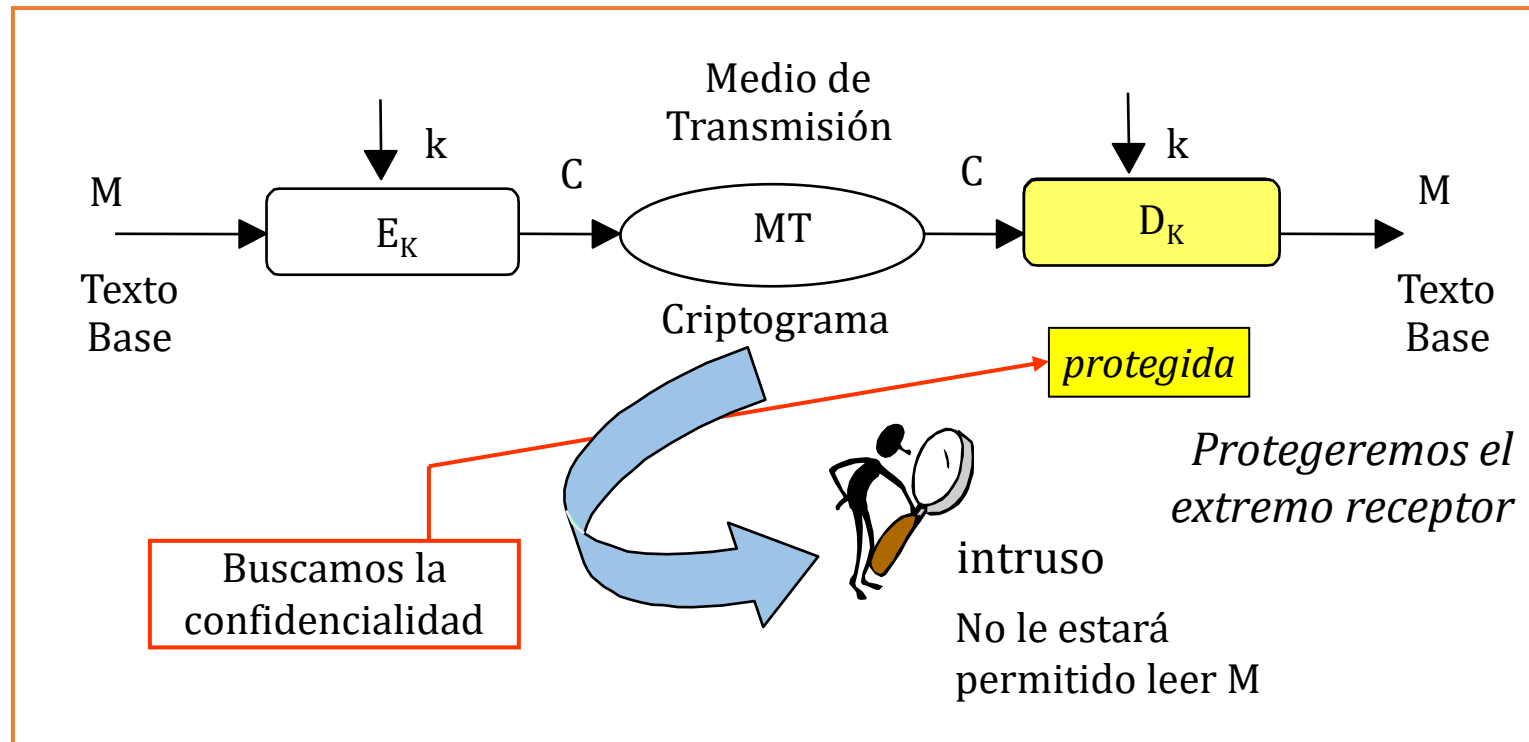
5.8.2.4. Ante la vida de las claves

5.8.3. Entornos de cifra híbrida

Class4crypt c4c5.8 Comparativa entre cifra simétrica y cifra asimétrica

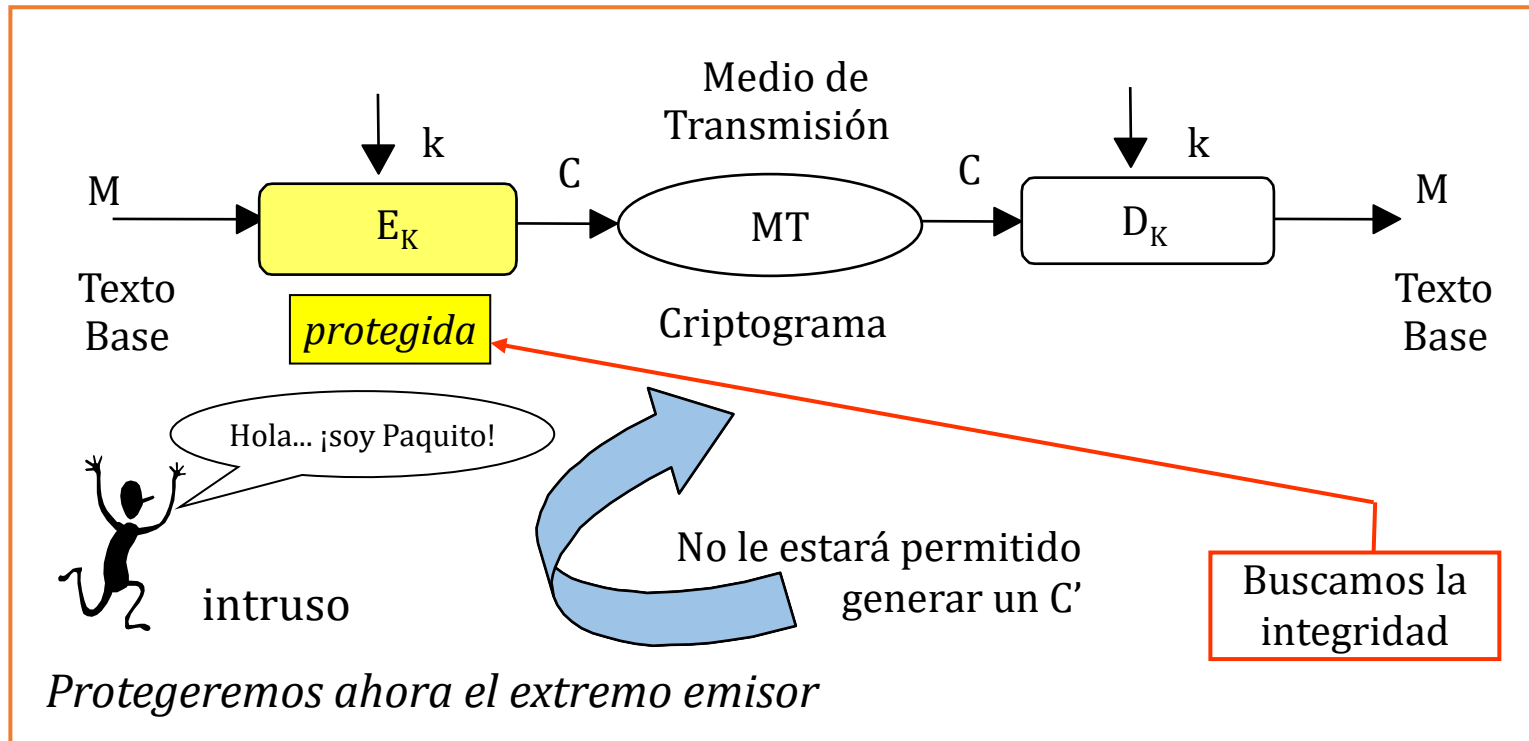
<https://www.youtube.com/watch?v=KGRm94P1qRI>

Confidencialidad en cifra simétrica



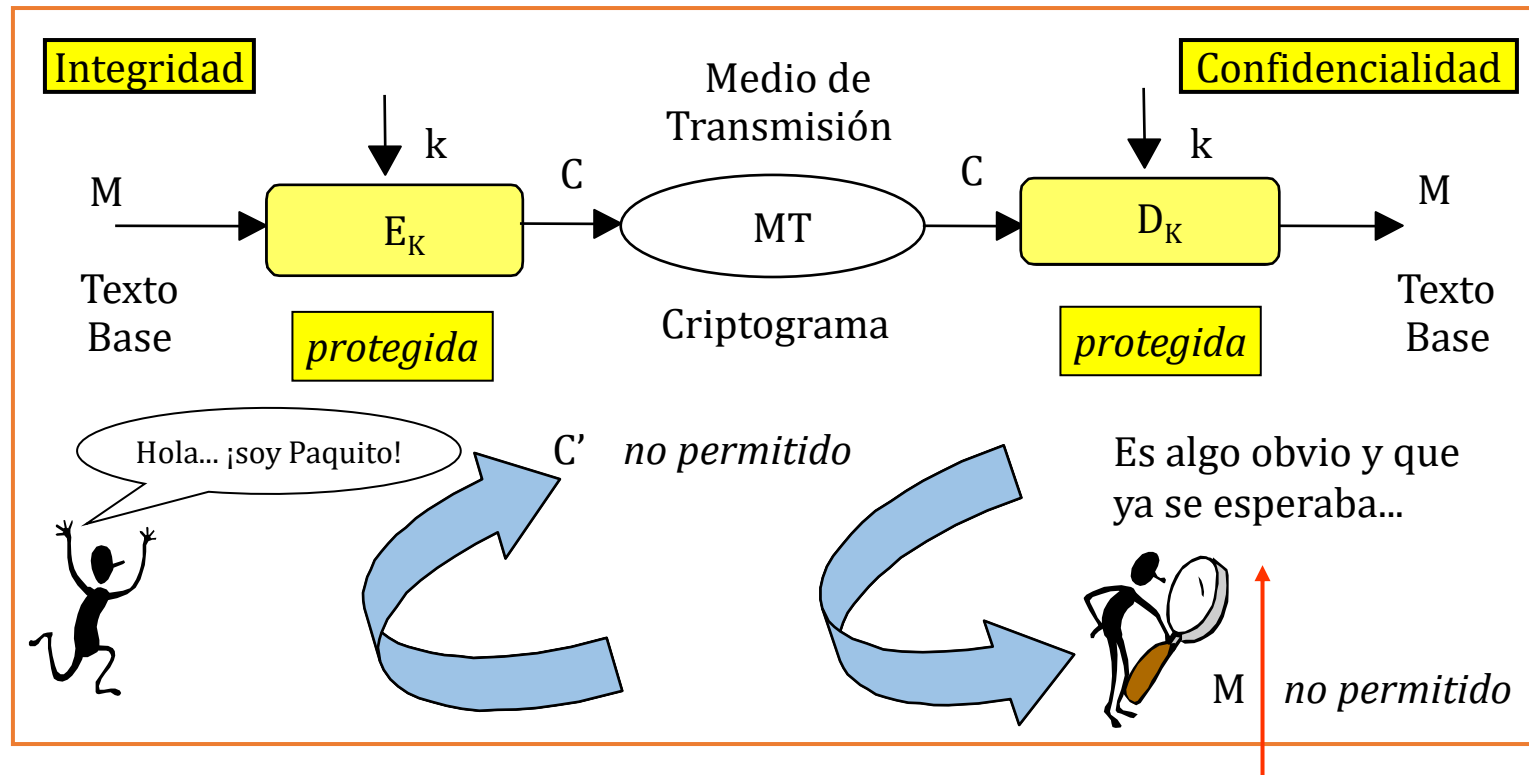
El criptoanalista no podrá descifrar el criptograma C o cualquier otro texto cifrado bajo la transformación D_K

Integridad en cifra simétrica



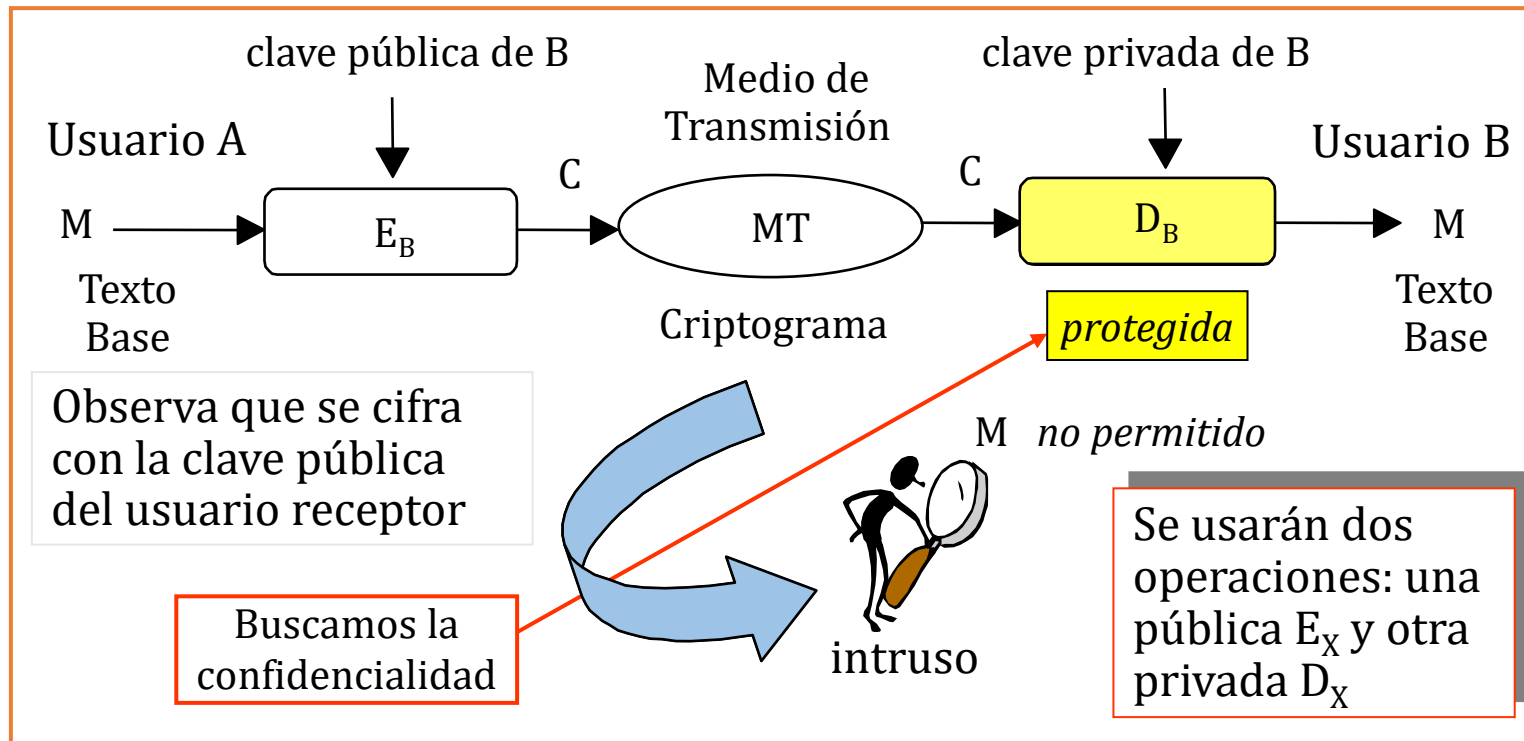
El criptoanalista no podrá cifrar un texto en claro M' y enviarlo al destinatario como $C' = E_K(M')$

Resumen en cifra simétrica



La confidencialidad y la integridad se lograrán simultáneamente si se protege la clave secreta.

Confidencialidad en cifra asimétrica

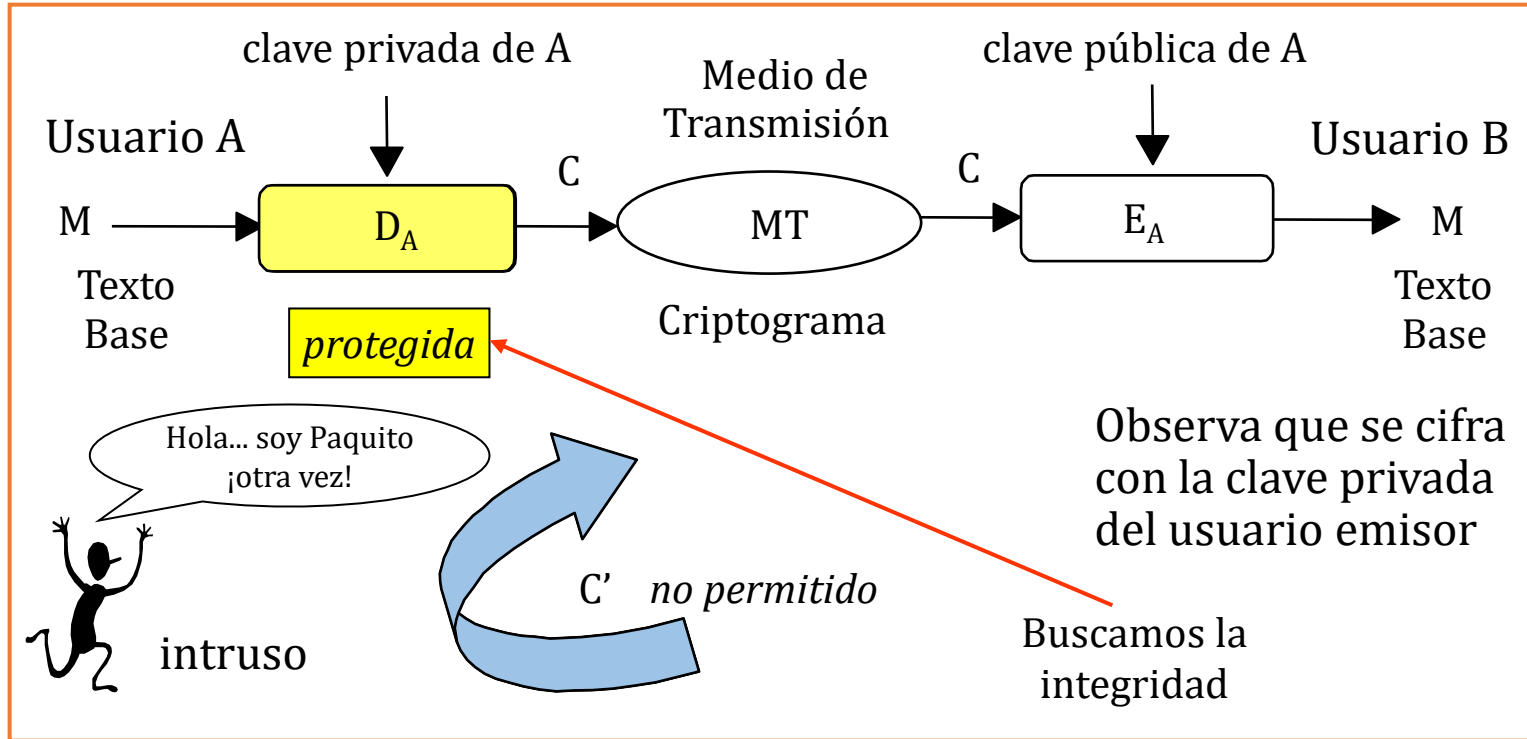


$$C = E_B(M)$$

$$M = D_B(C) = D_B(E_B(M))$$

E_B y D_B son operaciones con inversos dentro del módulo de cifra del usuario B

Integridad en cifra asimétrica

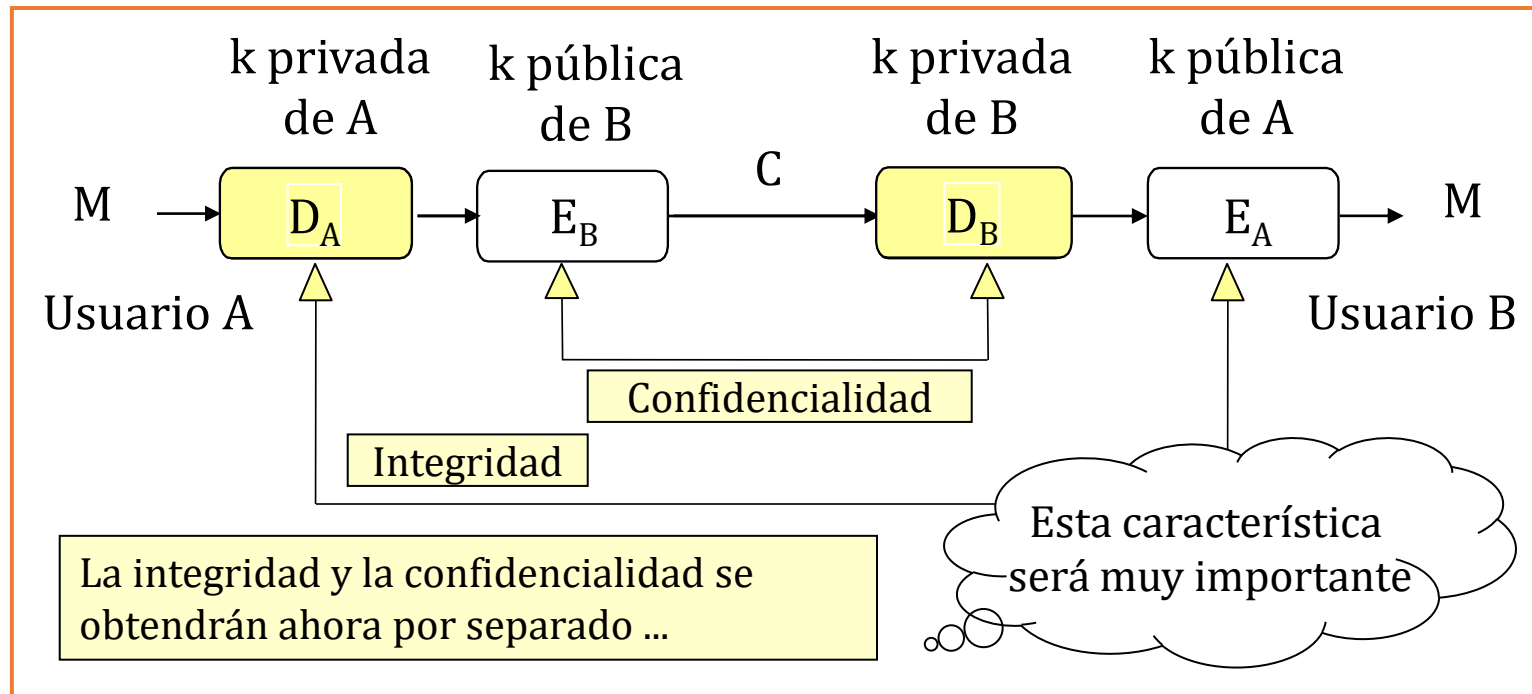


$$C = D_A(M)$$

$$M = E_A(C) = E_A(D_A(M))$$

D_A y E_A son operaciones con inversos dentro del módulo de cifra del usuario A

Resumen en cifra asimétrica



$C = E_B(D_A(M))$ Firma del mensaje con posterior cifrado para secreto

$M = E_A(D_B(C))$ Descifrado del criptograma y comprobación de firma

Estudio cifra simétrica versus asimétrica

- Vamos a comparar las características de la cifra simétrica con las de la cifra asimétrica en 7 aspectos fundamentales dentro de la criptografía:
 1. En qué basan su seguridad
 2. Cómo es la gestión de las claves
 3. Qué tamaño debe tener el espacio de claves
 - 4.Cuál es la duración (caducidad) o vida de la clave
 5. Si permite el intercambio de clave seguro
 6. Si permite la autenticación de usuarios y la firma digital
 - 7.Cuál es la velocidad o tasa de cifra

CS vs CA 1: la seguridad del sistema

- Un sistema de cifrado que se precie basa toda su seguridad en el secreto de una clave y ninguna en el algoritmo en sí, excepto su correcto diseño y código
- Se trata del segundo principio de la criptografía de Auguste Kerckhoffs (1883)

En la criptografía simétrica CS

- Se usa una única clave para cifrar en emisión y la misma para descifrar en recepción
- La seguridad en la cifra simétrica reside en cuán fuerte sea la clave (tamaño de la misma) y en cómo protegemos esa clave (procedimientos, métodos)

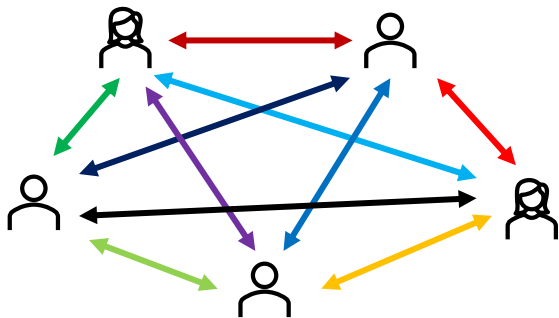
En la criptografía asimétrica CA

- Cada usuario se crea un par de claves llamadas pública y privada, inversas entre sí dentro de un módulo
- La seguridad de la cifra reside en la dificultad computacional de encontrar la clave privada a partir del conocimiento de la clave pública

CS vs CA 2: la gestión de claves

En la criptografía simétrica CS

- El sistema debe memorizar y trabajar con un número muy alto de claves. Para n usuarios, existirán $n(n-1)/2$ claves y cada usuario deberá recordar $n-1$ claves
- Además, no será posible la distribución de estas claves por canales seguros

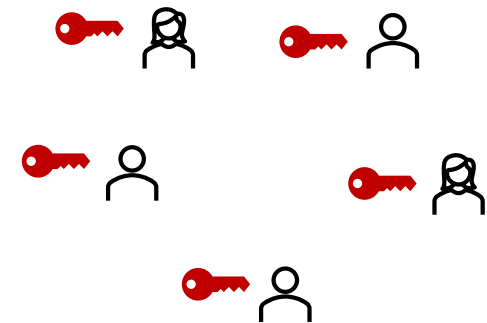


La gestión de claves será más eficiente la cifra asimétrica pues sólo es necesario memorizar la frase o palabra de paso para acceder a la clave privada. En la cifra simétrica el número de claves crece exponencialmente

En la criptografía asimétrica CA



- Sólo es necesario memorizar una clave privada, la de cada usuario
- Las claves públicas con las que nos comunicamos con los demás usuarios, las conocen todos



CS vs CA 3: el espacio de claves

En la criptografía simétrica CS

- Debido al tipo de algoritmo usado, en el que normalmente el único ataque viable es por fuerza bruta, la clave tendrá un tamaño de unas centenas de bits
- Actualmente (2020) se recomienda usar claves con valores entre 128 y 256 bits



Centenas
de bits

En cuanto al espacio de claves, no son comparables los sistemas simétricos con los asimétricos. Para atacar un sistema asimétrico no se buscará en todo el espacio de claves como debería hacerse en los sistemas simétricos, por ese motivo existe esa relación aproximada de 1/10

En la criptografía asimétrica CA

- Por el algoritmo usado en la cifra, basado en un problema matemático de difícil solución para números grandes, la clave tendrá un tamaño de miles de bits
- Actualmente (2020) RSA y DH se usan 2.048 bits y en ECC 256 bits. Pero la NSA en 2016 recomienda usar ya 3.072 y 384



Miles de bits,
excepto ECC

CS vs CA 4: la vida de las claves

En la criptografía simétrica CS

- La vida o duración de la clave es muy corta pues normalmente estamos hablando de una clave de sesión en SSL/TLS
- Lo normal es que esté en el rango de los segundos, minutos u horas
- Si se trata de una clave de cifrado simétrico convencional (cifrado archivo en un disco duro), el tiempo puede ser mucho mayor

minutos



En cuanto a la vida de una clave, en la cifra simétrica de conexión segura esta vida es mucho menor que en la cifra asimétrica. Una clave de sesión simétrica K será aleatoria. Las claves asimétricas pública y privada seguirán un protocolo propio de generación

En la criptografía asimétrica CA

- La duración de la clave pública, y por consiguiente su clave privada asociada, que la entrega y gestiona una tercera parte de confianza denominada AC, Autoridad de Certificación, suele ser bastante larga
- Lo normal es que tenga uno o dos años de validez

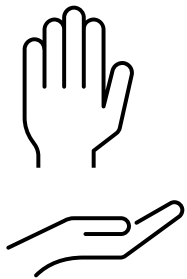
años



CS vs CA 5: el intercambio de claves

En la criptografía simétrica CS

- No existe el intercambio de claves en el sentido de que no es posible enviar una clave de sesión, conociendo que el canal es por definición inseguro



En cuanto al intercambio de una clave, los sistemas simétricos no tienen esta característica y los asimétricos sí

En la criptografía asimétrica CA



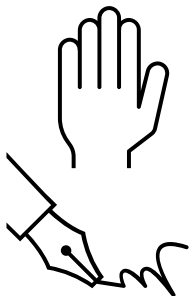
- Existe el intercambio de claves al poder enviar ésta (K) cifrada con la clave pública del destinatario, consiguiendo confidencialidad.
- Es seguridad computacional por la dificultad temporal y económica para romperla



CS vs CA 6: la autenticación y firma

En la criptografía simétrica CS

- Sólo se puede comprobar la integridad del mensaje mediante funciones MAC, Message Authentication Code
- Pero no se puede autenticar al emisor de forma sencilla y eficiente
- Carece de firma digital



En cuanto a la autenticación y firma, los sistemas simétricos tienen una autenticación pesada y requieren de una tercera parte de confianza activa. Los sistemas asimétricos permiten una firma digital verdadera, eficiente y sencilla, con una tercera parte de confianza sólo testimonial

En la criptografía asimétrica CA



- Al haber una clave pública y otra privada, se podrá autenticar al emisor y verificar la integridad del mensaje
- Si el emisor usa su clave privada, cualquiera que tenga su clave pública puede deshacer el cifrado y comprobar que es quien dice ser
- Permite la firma digital



CS vs CA 7: la velocidad de la cifra

En la criptografía simétrica CS



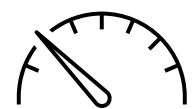
- La velocidad de cifra es muy alta
- Cientos de MegaBytes/segundo
- Es el algoritmo para la cifra del mensaje, la cifra de datos e información

En la criptografía asimétrica CA

- La velocidad de cifra es muy baja
- Cientos de KiloBytes/segundo
- Es el algoritmo para el intercambio de clave y la firma digital

En cuanto a la velocidad de cifra, los sistemas simétricos son de 100 a 1.000 veces más rápidos que los asimétricos

Por ello los sistemas de cifra asimétricos se usan para el intercambio de claves de sesión y firma digital (números de sólo pocas centenas de bits) y la cifra de los datos se hace con sistemas simétricos, con la clave de sesión antes intercambiada mediante criptografía asimétrica



¿Qué cifra es la mejor?

TIPO DE CIFRA	VENTAJAS	DESVENTAJAS
SIMÉTRICA	<ul style="list-style-type: none">• Alta velocidad o tasa de cifra MB/s• Eficiente para su uso grupos reducidos (redes pequeñas) al necesitar una sola clave• Posee una infraestructura sencilla• Las claves pueden ser pequeñas, de tan solo unas centenas de bits	<ul style="list-style-type: none">• Es necesario compartir una clave por medios que pueden ser no seguros pues no permite un intercambio de clave• Si se compromete la clave, se compromete toda la comunicación• No permite autenticar a los usuarios pues una clave la pueden usar varios usuarios• Elevado número de claves a recordar
ASIMÉTRICA	<ul style="list-style-type: none">• Número de claves reducido, dos claves por usuario y sólo una secreta a recordar• Seguridad computacional de la clave privada• No es necesario transmitir la clave privada entre emisor y receptor• Permite un intercambio de valor secreto de forma computacionalmente segura• Permite autenticar a los usuarios	<ul style="list-style-type: none">• Baja velocidad o tasa de cifra KB/s• La generación de claves requiere de un proceso diferente para cada algoritmo• Las claves deben ser muy grandes• Necesidad de una gran infraestructura de clave pública• Necesidad de una tercera parte de confianza o Autoridad de Certificación

Usos de la cifra simétrica y asimétrica

TIPO DE CIFRA	USOS Y CARACTERÍSTICAS	ALGORITMOS MÁS CONOCIDOS
SIMÉTRICA	<ul style="list-style-type: none">• Confidencialidad• Integridad• Cifrado de mensajes• Cifrado de la información	<ul style="list-style-type: none">• DES con tamaño de clave 56 bits (ya no se usa)• RC4 con tamaño de clave de 128 bits (ya no se usa)• 3DES EDE con tamaño de clave de 168 bits (uso en cifrado local o convencional)• AES con tamaños de clave 128, 192 y 256 bits• ChaCha20 con tamaños de clave de 128 y 256 bits
ASIMÉTRICA	<ul style="list-style-type: none">• Confidencialidad• Integridad• Autenticación de origen y de destino• No repudio de origen y de destino	<ul style="list-style-type: none">• Intercambio de clave• RSA con tamaño de clave de 2.048 bits (no se usa)• DH con tamaño de clave de 2.048 bits• ECDHE con tamaños de clave de 256 bits o mayor• Firma digital• RSA con claves de 2.048 bits• DSA con claves de 2.048 bits• ECDSA con claves de 256 bits o mayor

Entornos de criptografía híbrida

Uno tiene firma e intercambio de clave y el otro no, uno es rápido y el otro no ...



- Intercambio de clave, firma digital y gestión de claves
 - Son mejores los sistemas asimétricos con dos claves: pública y privada
- Cifrado de la información
 - Son mejores los sistemas simétricos con una sola clave: secreta



Sistemas de cifra híbridos

El protocolo SSL/TLS (*Secure Sockets Layer, Transport Layer Security*) utilizará ambos tipos de cifra, simétrica y asimétrica. A través de un cifrado con clave pública, cliente y servidor se autentican e intercambian una clave de sesión cuyo valor es aleatorio (*handshake*). A partir de este momento, se utiliza esta clave de sesión como clave secreta del cifrado simétrico para cifrar la información entre cliente y servidor solamente durante esa sesión

Más información en píldoras Thoth



<https://www.youtube.com/watch?v=0qfOVm-dtcQ>

Conclusiones de la lección 5.8

- En cuanto a la seguridad de las claves, la vida de las claves y la longitud de éstas, la criptografía simétrica y asimétrica no son comparables
- En cuanto a la gestión de las claves, la criptografía asimétrica es más eficiente que la criptografía simétrica, pero su infraestructura es más compleja
- En cuanto al intercambio de clave y la firma digital, la criptografía asimétrica lo permite pero la criptografía simétrica no
- En cuanto a la velocidad o tasas de cifra, la criptografía simétrica es mucho más rápida (una mil veces) que la criptografía asimétrica
- Por lo tanto, en ciertos entornos como SSL/TLS, se usa la criptografía híbrida: el intercambio de clave y la firma digital se hacen con criptografía asimétrica y el cifrado de la información se hace con criptografía simétrica

Lectura recomendada

- Guion píldora formativa Thoth nº 27, ¿Qué es mejor la cifra simétrica o la asimétrica?, Jorge Ramió, 2012
 - <https://www.criptored.es/thoth/material/texto/pildora027.pdf>
- Key size, Wikipedia
 - https://en.wikipedia.org/wiki/Key_size
- Commercial National Security Algorithm Suite (NSA)
 - https://en.wikipedia.org/wiki/Commercial_National_Security_Algorithm_Suite