1- Introducción criptografía y seguridad informática

Definiciones básicas

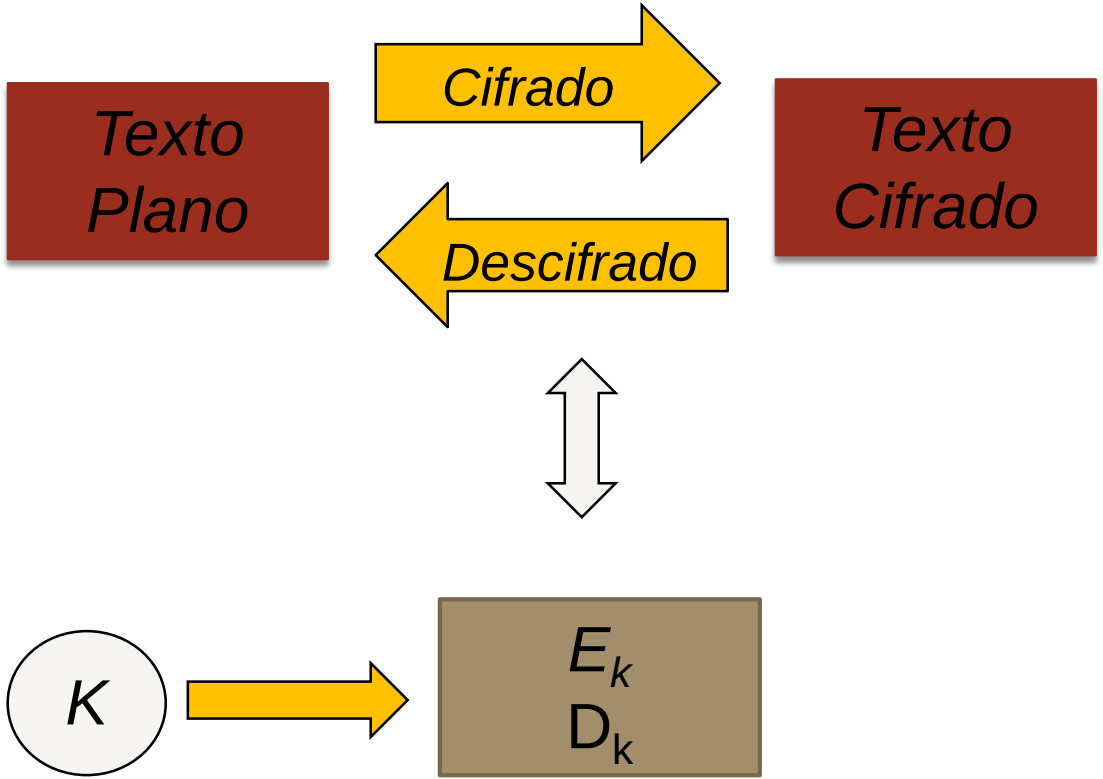
- Semántica: Según la RAE la palabra “criptografía” proviene del griego “cripto” que significa oculto, y “grafía” que significa escritura: es el arte de escribir con clave secreta y de un modo enigmático.
- Ya dejo de ser un arte, ahora es la ciencia se ocupa del estudio de los métodos para la protección y ocultamiento de la información frente a observadores no autorizados.

Definiciones básicas

- Texto Plano.
- Texto cifrado.
- Cifrado o encriptación.
- Descifrar o descifrado.
- Criptoanálisis.
- Criptología = Criptografía + Criptoanálisis.
- Esteganografía:
  - Técnica para esconder mensajes dentro de otro mensaje.
- Seguridad Perfecta.
- Algoritmos y claves.

- Protagonistas del proceso de cifrado:
  - Encriptador: A.
  - Descifrador: B.
  - Atacante: M.
- Datos y útiles:
  - Texto inicial.
  - Texto cifrado.
  - Algoritmo de cifrado.
  - Algoritmo de descifrado. (depende del de cifrado).

Definiciones básicas



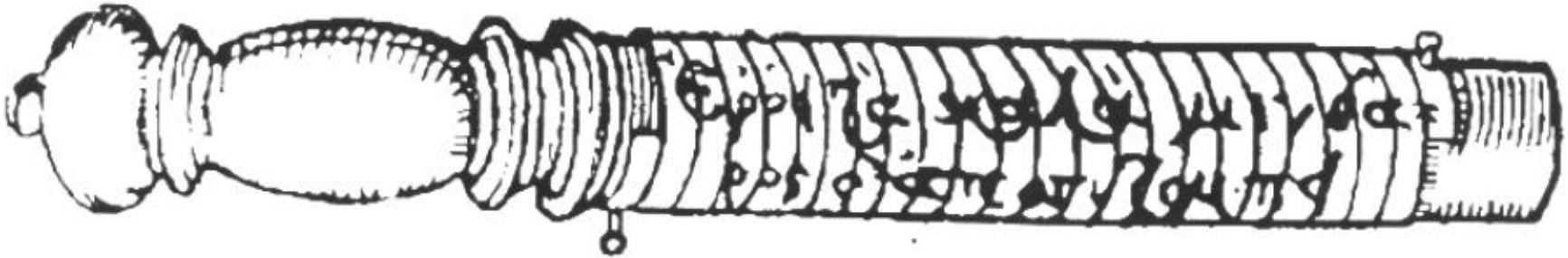
Contexto histórico de la criptografía

- Principales motores de la criptografía:
  - Político.
  - Bélico.
  - Económico (quizás el más importante hoy en día).
- Algunos datos históricos:
  - Quizás los primeros métodos criptográficos: los jeroglíficos egipcios (escritura eminentemente pictórica, siglo V a.C.): No pudieron ser descifrados hasta principios del siglo XIX (por el hallazgo de la Piedra de Rosetta).
  - El primer método criptográfico propiamente dicho el Escítalo de los Lacedemonios (siglo V a.C., Antigua Grecia).

- Algunos libros con los que se puede ampliar la historia de la criptografía:
  - José Pastor Franco, Miguel Ángel Sarasa López, José Luis Salazar. Riaño,Criptografía digital: fundamentos y aplicaciones.
  - Simon Singh, Los códigos secretos.
  - Simon Singh, The Code Book.

Contexto histórico de la criptografía

Escítalo de los Lacedemonios: transposición de caracteres.



Contexto histórico de la criptografía

Cifradores de Polybios (siglo II a.C., Grecia): Sustitución de caracteres.

- **Problema propuesto:** Estudiar con más detalle en casa el método de cifrado de Polybios y su fortaleza.

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

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

FIGURA 2. Cifradores de *Polybios*

Así, el cifrado de la máxima: EX ABUNDANTIA CORDIS OS LOQUITUR con el tablero de la parte izquierda viene dado por:

1553 11124533141133442411 133442142443 3443 3134414524444542

Contexto histórico de la criptografía: Criptografía Clásica

- Métodos de transposición: cambian la posición de los caracteres del mensaje.
- Ejemplo: *Escítalo de los Lacedemonios.*
- Métodos de sustitución: sustituyen cada carácter del mensaje por otro diferente.
  - Monoalfabético: utilizan un solo alfabeto.
    - Monográmicos: efectúan el cifrado carácter a carácter.
      - Alfabeto estándar: César.
      - Alfabetos mixtos: discos de Alberti y De la Porta.
    - Poligrámicos: efectúan el cifrado por grupos de caracteres.
      - Digrámicos: cifrados en grupos de dos caracteres.
      - Trigrámicos: cifrado en grupos de tres caracteres.
      - ……
      - Poligrámicos: libros de códigos.
  - Polialfabéticos: utilizan varios alfabetos.
    - No periódicos: claves de cifrado no periódicas: El cifrado de Vernam.
    - Periódicos: claves de cifrado periódicas.
      - Alfabetos lineales: estándar, Vigenère, mixto.
      - Alfabetos progresivos: ENIGMA.

Contexto histórico de la criptografía: Criptografía Moderna

- 1976 empieza la criptografía moderna.
  - 1976 nacimiento de la criptografía pública.
  - 1977 Data Encription Standard (DES).
  - 1978 RSA (Rivest, Shamir y Adleman).
  - 2000 Advanced Encryption Standard (AES, Rijndael).

La evolución de los métodos clásicos de cifrado

- Escítalo de los Lacedemonios (siglo V a.C., Antigua Grecia).
- El emperador César propuso un método sustitución carácter a carácter:
  - Julio César, siglo I a.C.:
    - **Sustitución** de caracteres latinos por griegos
    - Utilización sistemática de cifrados, en particular por **desplazamiento** de las letras
- El único secreto era el desplazamiento, n=3

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	0	1	2
D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A	B	C

A modo de ejemplo, el cifrado de *César* de la conocida sentencia: ALEA IACTA EST viene dado por: DOHD NDFAD HXA. Con todo lo anterior, es sencillo darse cuenta de que el cifrado de *César* podía obtenerse de forma sencilla mediante dos regletas, una fija y otra deslizante, con el mensaje en la fija y el alfabeto en la deslizante.

La evolución de los métodos clásicos de cifrado

- Además de la aportación de los griegos y romanos a la criptografía los árabes contribuyeron también de forma significativa:
  - Alrededor de 1300 esta comunidad utilizaba al menos siete métodos de cifrado:
    - Reemplazar una letras por otras.
    - Escribir palabras al revés.
    - Invertir letras alternadas en el texto de un mensaje.
    - Dar a las letras valores numéricos y escribir dichos valores con símbolos.
    - Reemplazar cada letra con otras dos de tal forma que la suma de los valores numéricos fuese igual al valor de la letra sustituida.
    - Sustituir cada letra con el nombre una persona u objeto (libro de códigos).
    - Sustituir la letras por signos lunares, pájaros, flores, u otros signos inventados.
    - ……

La evolución de los métodos clásicos de cifrado

- Además los árabes fueron los primeros en escribir un tratado sobre criptoanálisis (Yusuf Yaqub ibn Ishaq al-Sabbah Al-Kindi, siglo IX, D.C.):
  - Este matemático árabe, trabajó en la *Casa de la Sabiduría* de Bagdad, y escribió el libro: *Manuscrito sobre el desciframiento de mensajes criptográficos:*
    - En este libro se describe un método, basado en *el análisis de frecuencias*, que permite criptoanalizar todos los cifrados monoalfabéticos.

La evolución de los métodos clásicos de cifrado

- En 1466 L. B. Alberti adapto el sistema del César en discos giratorios, utilizando alfabetos mixtos:

Imagen extraída de https://it.wikipedia.org/wiki/Disco_cifrante

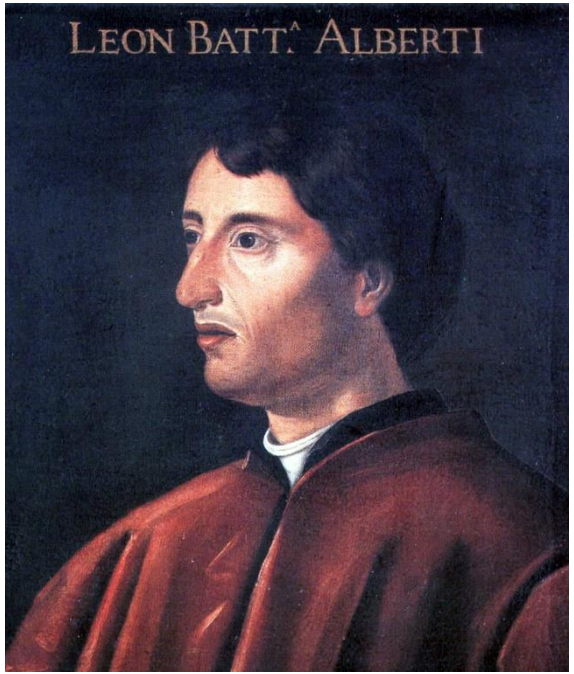


Imagen extraída de https://it.wikipedia.org/wiki/Leon_Battista_Alberti

La evolución de los métodos clásicos de cifrado

- En 1593 el cifrador de L. B. Alberti fue modificado por Giovanni Battista della Porta:

Imagen extraída de https://es.wikipedia.org/wiki/Giovanni_Battista_della_Porta

La evolución de los métodos clásicos de cifrado

```
mensaje:      P A R I S  V A U T  B I E N  U N E  M E S S E
clave:        L O U P L  O U P L  O U P L  O U P  L O U P L
criptograma:  A O M X D  K U K E  P C T X  J H T  W S N I O
```

- En 1595 el francés Blaise de Vigenère sustituyó los discos del cifrador de L. B. Alberti y de Giovanni Battista della Porta por una palabra:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	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
	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
	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
	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	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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

- En este cuadro de Vigenère por ejemplo la columna P con la fila L da la A. Es una forma fácil de cifrar mediante este cifrado.

Imagen extraída de https://es.wikipedia.org/wiki/Cifrado_de_Vigen%C3%A8re

La evolución de los métodos clásicos de cifrado

- Para aumentar la fortaleza del cifra B. Vigenère propuso un doble cifrado: cifrar el resultado del primer cifrado con otra clave diferente a la utilizada en el primer cifrado.
- Se puede demostrar que este cifrado resultante tiene por clave la suma de las otras dos claves (ejercicio).
- Este cifrado se creía un cifrado perfecto, hasta que prusiano Friedrich Kasiski descubrió un método eficiente de criptoanalizar dicho cifrado (lo haremos en prácticas).
- En 1935 El criptógrafo americano G. S. Vernam que para que este cifrado fuera seguro la clave debería ser del mismo tamaño que el texto a cifrar, y además aleatoria sin ningún tipo de estructura predecible.

- **Problema propuesto;** demostrar que el cifrado resultante de dos cifrados consecutivos de Vigenère tiene por clave la suma de las otras dos claves

La evolución de los métodos clásicos de cifrado

- En 1854 C. Wheatstone diseño un procedimiento de cifrado de sustitución basado en el cifrado de Polybios: conocido por el cifrado de Playfair (llamado así en honor a su amigo Lord Playfair).
- Por ejemplo si queremos utilizar la clave NORIA, podemos generar la matriz de cifrado siguiente de la derecha, y el cifrado del texto plano:
  - ATAQUECEROHORASX
- es el testo cifrado
  - IUOUTFDFIRQCINXR.
- Ya no es tan fácil como el cifrado Poybios (la matriz cambia en función de la clave).

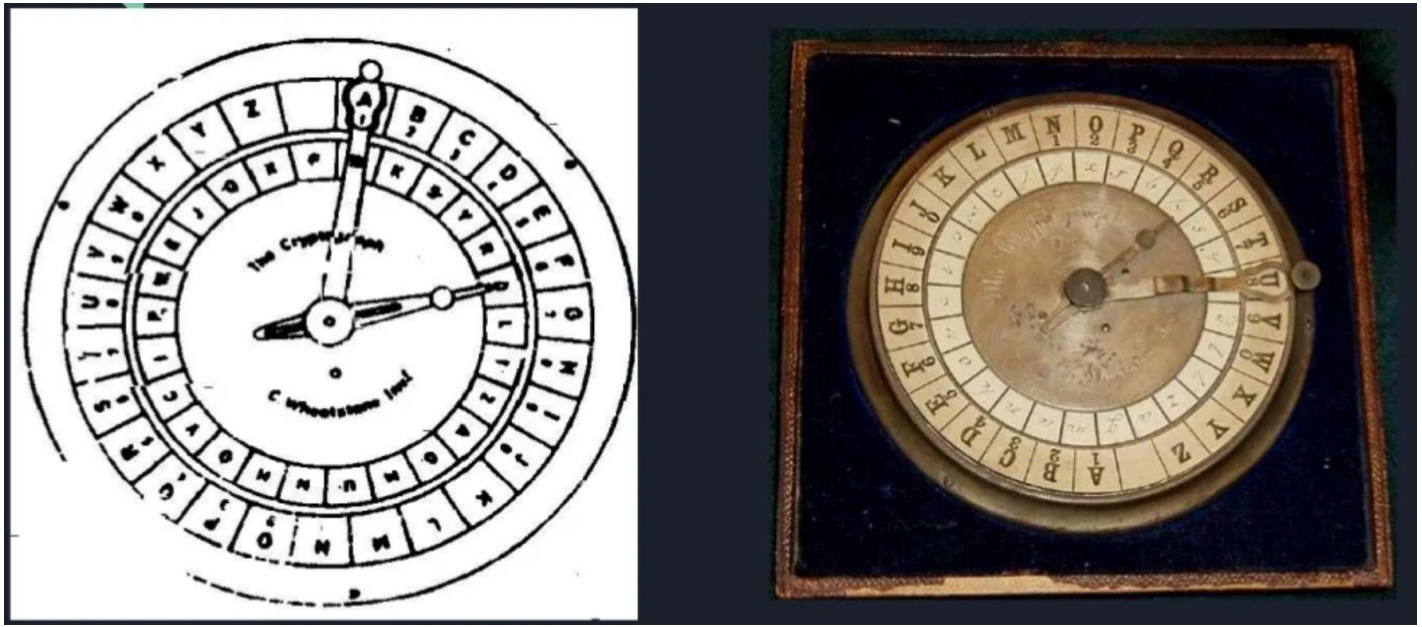
N	O	R	I	A
B	C	D	E	F
G	H	K	L	M
P	Q	S	T	U
V	W	X	Y	Z

- **Problema propuesto:** Estudiar con más detalle en casa el método de cifrado de Playfair y su fortaleza.

Imagen extraída de https://es.wikipedia.org/wiki/Cifrado_de_Playfair#Creaci%C3%B3n_de_la_matriz_de_cifrado

La evolución de los métodos clásicos de cifrado

- En 1857 C. Wheatstone diseño mecánicamente el denominado disco de Wheatstone, basándose en la idea del cifrador de discos de L. B. Alberti.



La evolución de los métodos clásicos de cifrado

- Un hecho muy importante que marcó el desarrollo de este tipo de cifradores fue el paso de dispositivo planos a dispositivos con multitud de discos concéntricos coaxiales:
  - Se escribía un mensaje en la generatriz del cilindro de discos y se leía en cualquier otra línea.
- Este dispositivo fue creado por T. Jefferson en 1790, y fue utilizado por el ejército americano hasta finales de 1930.
- Por ejemplo 10 discos, y la «clave» o la secuencia de discos, a utilizar es 7,9,5,10,1,6,3,8,2,4 (cada disco tiene un orden especifico de los caracteres):

7:	< R AFDCE O NJQGWTHSPYBXIZULVKM <
9:	< E NYVUB M CQWAOIKZGJXPLTDSRFH <
5:	< T SGJVD K CPMNZQWXYIHFRLABEUO <
10:	< I SCZQK E LMXYRHPUDNAJFBOWTGV <
1:	< R ZWAXI G DLUBVIQHKYPNTCEMOSF <
6:	< E MKGHI W PNYCJBFZDRUSLOQXVAT <
3:	< S EQGYX P LOCKBDMAIZVRNTJUWFH <
8:	< E OZUTW D CVRJLXKISNFAPMYGHBQ <
2:	< Y OHGVS F UWIKPBELNACZDTRXMJQ <
4:	< A WORPL N DVHGFCUKTEBSXQYIZMJ <

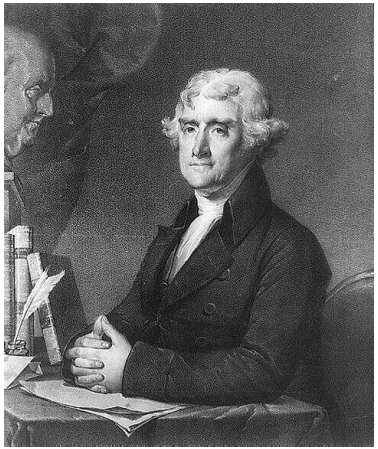


Imagen extraída de https://es.wikipedia.org/wiki/Discos_de_Jefferson

Imagen extraída de https://fr.wikipedia.org/wiki/Cylindre_de_Jefferson

La evolución de los métodos clásicos de cifrado

- Finalmente se conectaron eléctricamente los discos, y las conexiones cambiaban con el tiempo en una secuencia predeterminada.
- Esto llevo a la creación de las diferentes versiones de la famosa máquina ENIGMA:
  - La máquina de rotores para cifrar y descifrar que se patentó en 1918 por Arthur Scherbius:

Abb. 1. Chiffriermaschine mit Verschluß-kappen.

Abb. 2. Chiffriermaschine ohne Verschluß-kappen.

Imagen extraída de https://de.wikipedia.org/wiki/Arthur_Scherbi

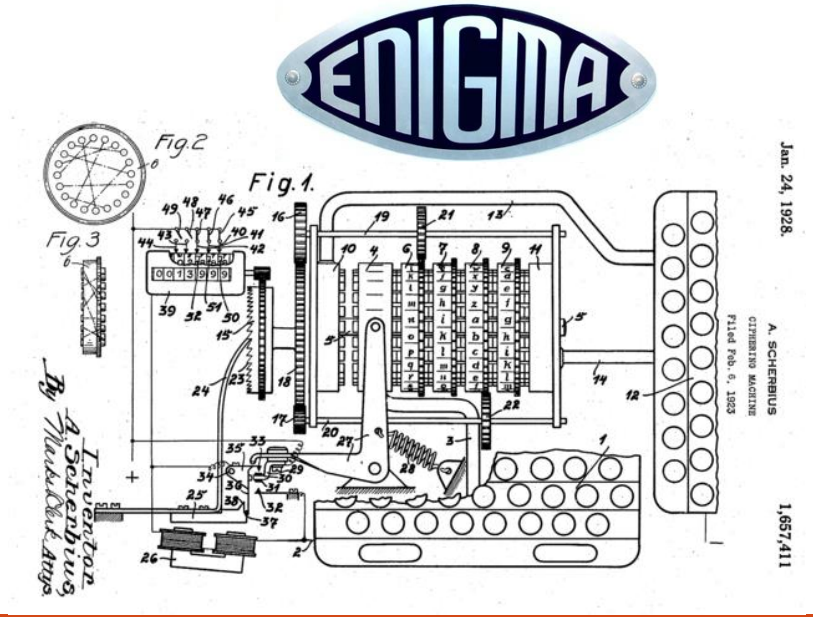


Imagen extraída de https://es.wikipedia.org/wiki/Arthur_Scherbius

La evolución de los métodos clásicos de cifrado

- O la máquina de la competencia sueca de B. Hayelim:

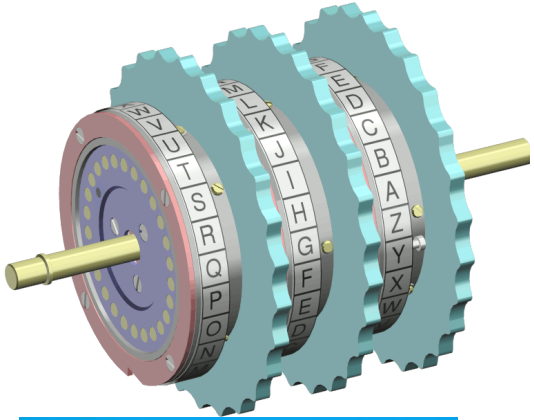
HAGELIN M-209 CIPHER MACHINE (GVG / PD)

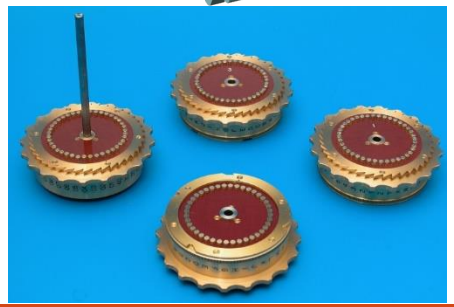
Imagen extraída de https://nl.wikipedia.org/wiki/Boris_Hagelin

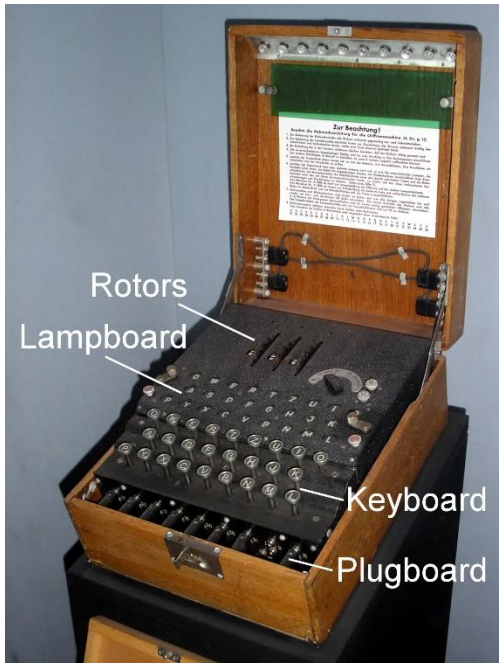
Imagen extraída de https://es.wikipedia.org/wiki/Boris_Hagelin

La evolución de los métodos clásicos de cifrado

- El funcionamiento de todos estos dispositivos enigma es mediante las conocidas máquinas de rotores:







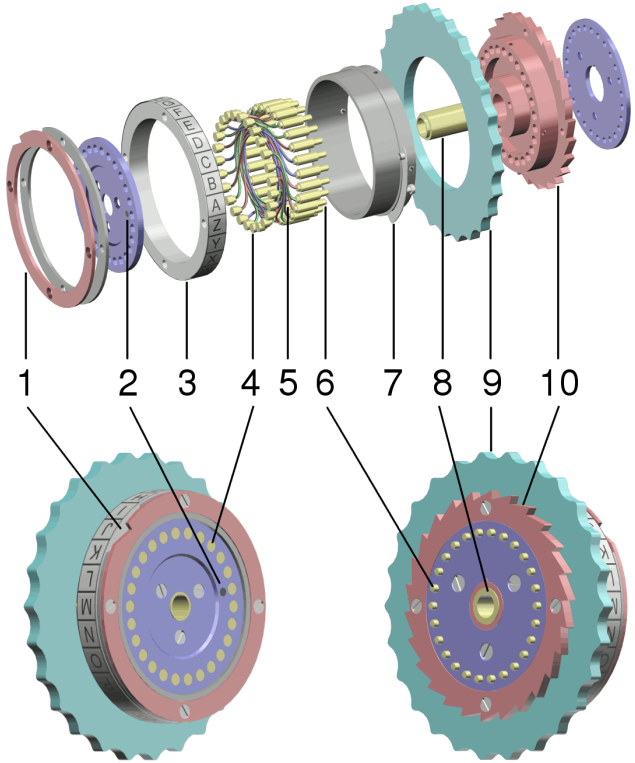


Imagen extraída de https://en.wikipedia.org/wiki/Rotor_machine

La evolución de los métodos clásicos de cifrado

- Entendiendo mejor la máquina ENIGMA:
  - La máquina ENIGMA en Python:
    - https://www.101computing.net/enigma-encoder/
  - Simulación del funcionamiento:
    - https://www.101computing.net/enigma/enigma-M3.html

- Libros gratuitos de criptografía:
  - Criptografía y Seguridad en Computadores. Manuel J. Lucena López
  - Libro de criptografía aplicada: A. J. Menezes; P. C. van Oorschot; S. A. Vanstone (1997). Handbook of Applied Cryptography

La evolución de los métodos clásicos de cifrado

- Las diferencias entre la criptografía clásica y moderna es que los algoritmos públicos y lo único que es secreto es la clave.
- La idea de que los algoritmos de cifrado y descifrado deben ser públicos y la clave secreta fue propuesta por A. Kerckoffs, criptógrafo holandés del siglo XIX, y se conoce como
  - **Principio de Kerckoffs**.
- La fuerza reside en la clave, y no en el algoritmo que sea secreto, como pasaba en la criptografía clásica.
  - Es decir los algoritmos criptográficos son públicos.

POSIBLE Tarea de Evaluación Continúa: trabajo de historia de la criptografía.

La criptografía en las tecnologías de la información

- La seguridad de los sistemas de información está relacionada con la informática y comunicación en presencia de **adversarios.**
- **Sistemas de información:**
  - PC
  - Teléfonos
  - Redes de computadores
  - Cajeros automáticos
  - RFID
  - Puntos de Wireless
  - Dispositivos médicos
  - Email
  - Coches
  - …..
- Todo es digital hoy en día, o casi todo…….
- La **seguridad informática** se refiere a los objetivos de seguridad o las políticas de seguridad: que se quiere proteger, que actividades o eventos deberían ser prevenidos o detectados.

La criptografía en las tecnologías de la información

- Los métodos básicos para obtener la seguridad a través de criptografía pueden agruparse en 4 principales áreas:
  - Cifrado Simétrico
  - Cifrado Asimétrico
  - Algoritmos de integridad de datos
  - Protocolos de seguridad (engloban a los anteriores)

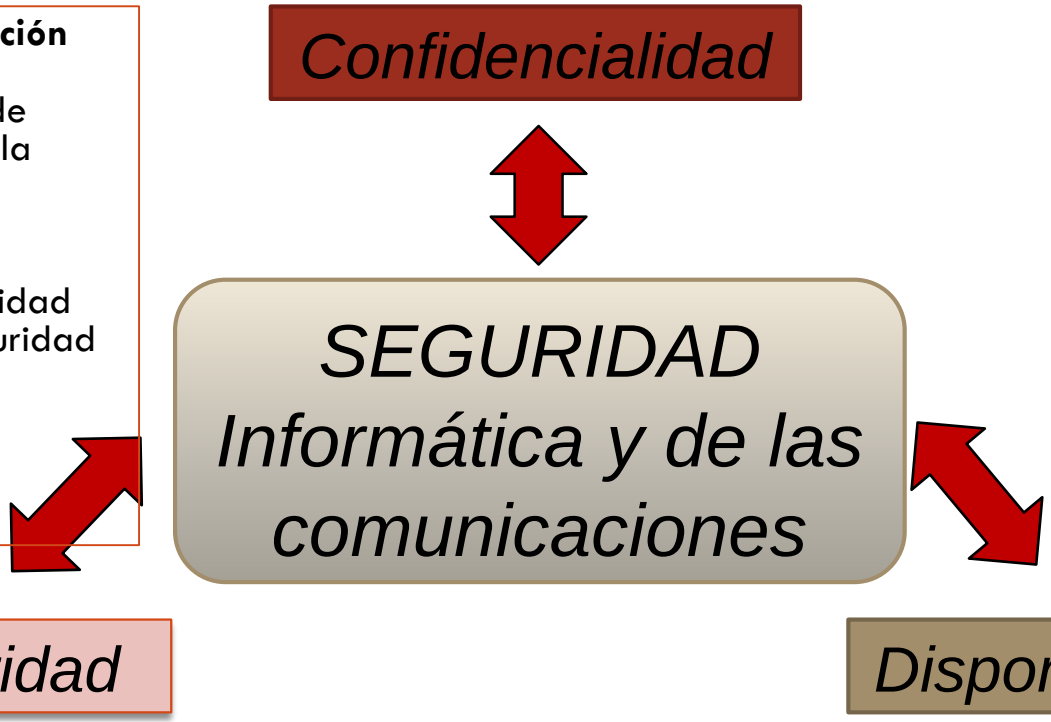
- El libro del NIST (actualizado) define el término seguridad informática más o menos como:
  - ***la protección que se otorga a un sistema de información automatizado con el objetivo de alcanzar la preservación de la integridad, disponibilidad y confidencialidad de la información y los recursos del sistema (incluye hardware, software, firmware, información / datos, y telecomunicaciones).***

- NIST: National Institute of Standards and Technology

La criptografía en las tecnologías de la información

POSIBLE Tarea de Evaluación Continúa: Implantación y organización de Sistema de Gestión de Seguridad de la Información (SGSI):

- LOPD y LSSI.
- Arquitectura de seguridad OSI (servicios de Seguridad X.800).
- ISO/IEC 27001.
- Auditorías.



- Para chequear y testear CIA (Confidentiality Integrity Availability): **Auditorías** (verificar que se cumplen las normas de seguridad apropiadas).

La criptografía en las tecnologías de la información

- Los mecanismos de seguridad o control de seguridad son las componentes técnicas o métodos para asegurar los servicios de seguridad, típicamente dos formas:
  - **Prevención**: Mantener la política de seguridad para no ser violada.
    - *Passwords*, cifrados, etc.
  - **Detección**: Detectar cuando la política de seguridad es violada.
    - Detección de intrusión en redes, chequeos de virus, etc.
- Quienes son los **adversarios:**
  - Puede ser interior/exterior al sistema de información, vendedor, empresas, etc.
    - Un **vendedor** puede instalar un *rootkit* en el sistema (es un programa que se ejecuta en un ordenador con medidas para **mantener su presencia oculta** y para **impedir su eliminación**).
      - El *rootkit* más conocido fue desarrollado y diseminado subrepticiamente por Sony en 2005. (https://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html). Y lo más grave que OJO que los virus se pueden aprovechar de esto.
    - Una **escucha ilegal** de un canal puede manipular las comunicaciones.

La criptografía en las tecnologías de la información

- Los servicios de seguridad junto con los mecanismos para alcanzar esos servicios están definidos en el documento de recomendación X.800.
- Esta recomendación forma parte de la Unión Internacional de Telecomunicaciones, aprobaba el 22 de marzo de 1991 en Ginebra, que fue elaborado por el Comité Consultivo Internacional Telegráfico y Telefónico.
- No es una especificación de implementación, sino una descripción de los servicios de seguridad junto con los mecanismos para alanzar estos servicios.
- X.800 define en que capa del Modelo OSI (Open System Interconnection) se deben aplicar los servicios de seguridad junto con los mecanismos o funciones que pueden ser implementados para ofrecer esos servicios.
- También se hace en este documento una recomendación de la administración de la seguridad.

La criptografía en las tecnologías de la información

- En los Servicios de Seguridad, **Parte, Actor o Entidad**: Puede ser un usuario, proceso, sistema, ……
- La criptografía puede generar los siguientes servicios para protección en las tecnologías de la información:
  - **Autenticación**:
    - Asegura que la identidad de un actor, entidad o entidades conectadas a un actor, entidad o entidades sea autentica y verdadera.
    - Asegura y corrobora a una entidad que la información proviene de otra entidad es auténtica y verdadera.
  - **Control de acceso:**
    - Protege a una entidad contra el uso no autorizado de sus recursos.
    - Se puede aplicar a varios tipos de acceso:
      - uso de medios de comunicación, la lectura, escritura o eliminación de información y la ejecución de procesos, etc.
  - **Confidencialidad:**
    - Protege a una entidad contra la revelación deliberada o accidental de cualquier conjunto de datos a entidades no autorizadas.
    - Cuando el conjunto de datos a proteger se refiere a información propia de un individuo (dirección postal, entorno familiar, cuentas bancarias, actividades personales, etc.) generalmente se suele hablar de **privacidad**.

La criptografía en las tecnologías de la información

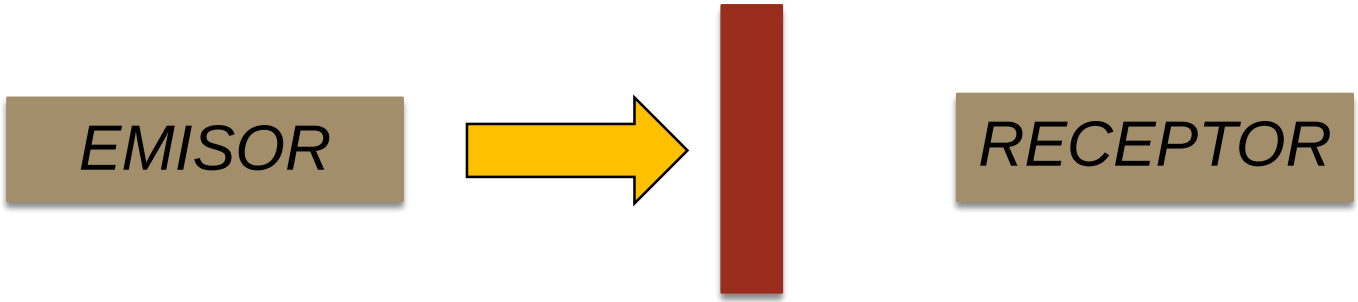
- **Integridad**:
  - Asegura que los datos almacenados en las computadoras y/o transferidos en una conexión no fueron modificados.
  - Su aplicación es variable: se puede aplicar a un flujo de mensajes, un mensaje solo, o campos seleccionados dentro de un mensaje.
  - Asegura que los mensajes son recibidos tal como se enviaron, sin duplicación, inserción, modificación, reorganización, o repeticiones.
  - En general, proporciona protección contra toda alteración de mensaje no autorizado.

- **No repudio**:
  - Protege contra usuarios que quieran negar falsamente que enviaran o recibieran un mensaje.
  - Cuando se envía un mensaje, el receptor puede probar que el emisor de hecho, ha enviado el mensaje (Origen).
  - Cuando se recibe un mensaje, el emisor puede demostrar que el receptor de hecho recibió el mensaje (Destino).

La criptografía en las tecnologías de la información

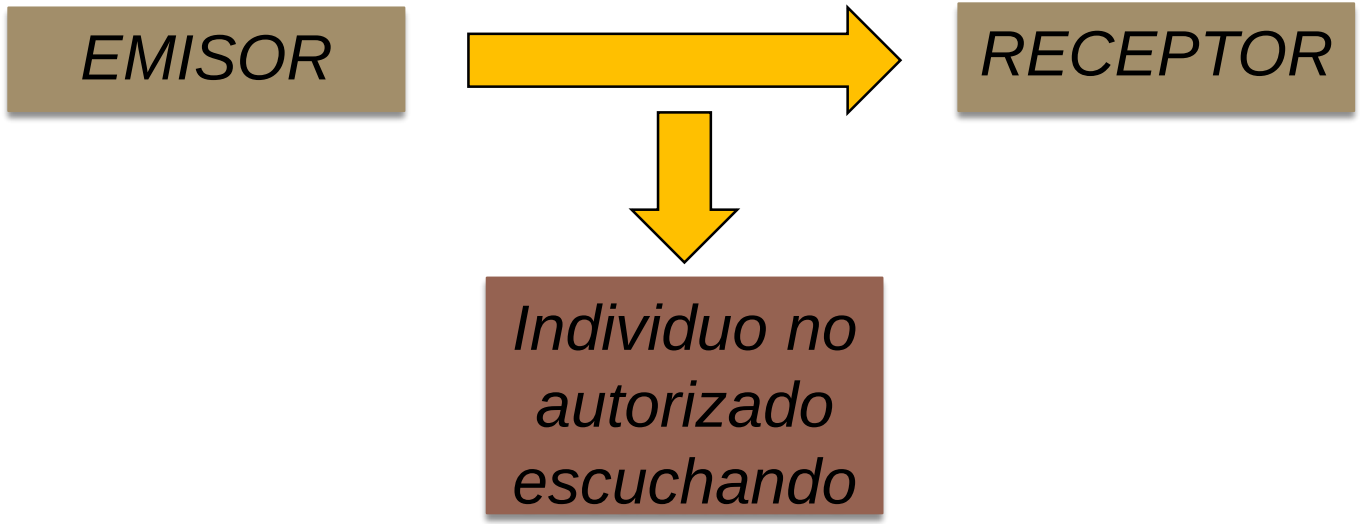
- El flujo normal de la información sería:

- Los diferentes esquemas generales de ataques que se pueden se pueden dar en tecnologías de la información son:
  - **Interrupción** (se destruye la comunicación):



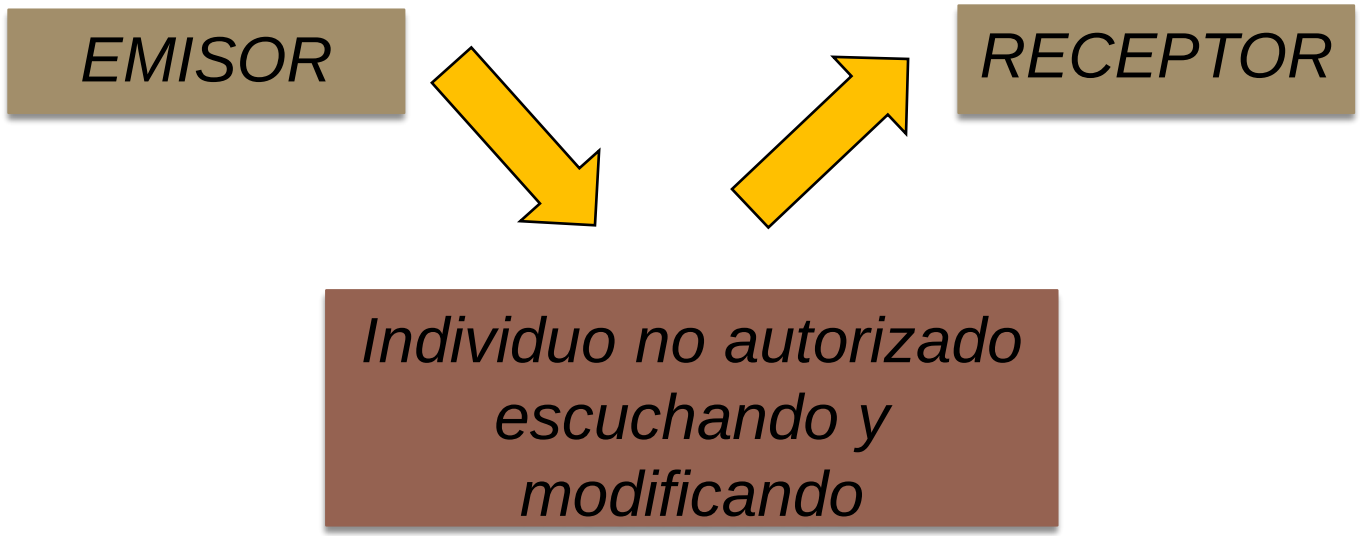
La criptografía en las tecnologías de la información

- Los diferentes esquemas generales de ataques que se pueden se pueden dar en tecnologías de la información son (cont.):
  - **Intercepción** (se viola la confidencialidad):



La criptografía en las tecnologías de la información

- Los diferentes esquemas generales de ataques que se pueden se pueden dar en tecnologías de la información son (cont.):
  - **Modificación** (se viola la integridad):



La criptografía en las tecnologías de la información

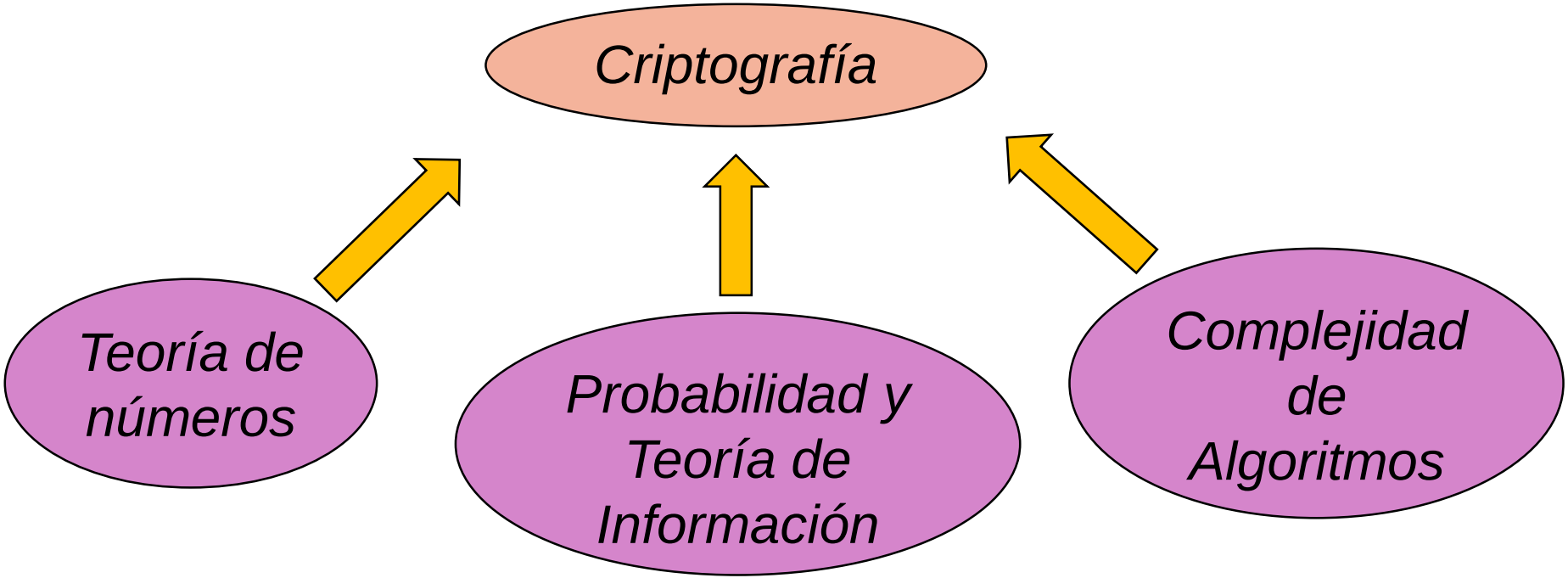
- Los diferentes esquemas generales de ataques que se pueden se pueden dar en tecnologías de la información son (cont.):
  - **Engaño** (se viola la autentificación):

La criptografía en las tecnologías de la información

- Por otro lado los diversos ataques se pueden clasificar en:
  - **Activos:**
    - Interrupción.
    - Intercepción.
    - Modificación.
    - Engaño (*fabrication*).
    - Suplantación de identidad.
    - Repetición (captura el mensaje y lo reenvía).
  - **Pasivos:**
    - Cuando se actúa directamente en la comunicación en emisor y receptor. Por ejemplo el atacante se limita a grabar el mensaje, a observar tráfico (análisis de tráfico), etc.

Los pilares teóricos de la criptografía

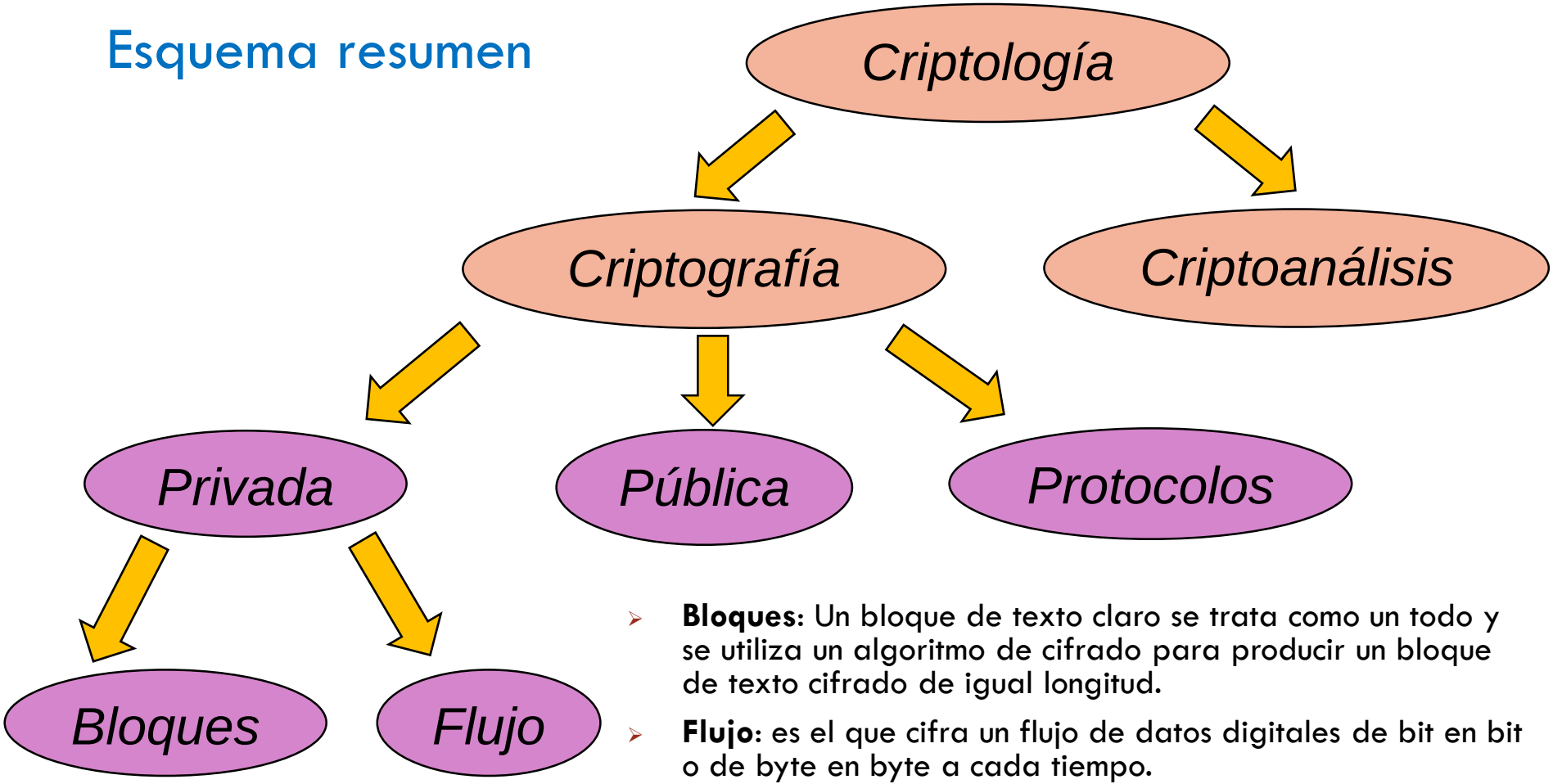
- Los pilares teóricos de la criptografía son:



Los pilares teóricos de la criptografía (las claves)

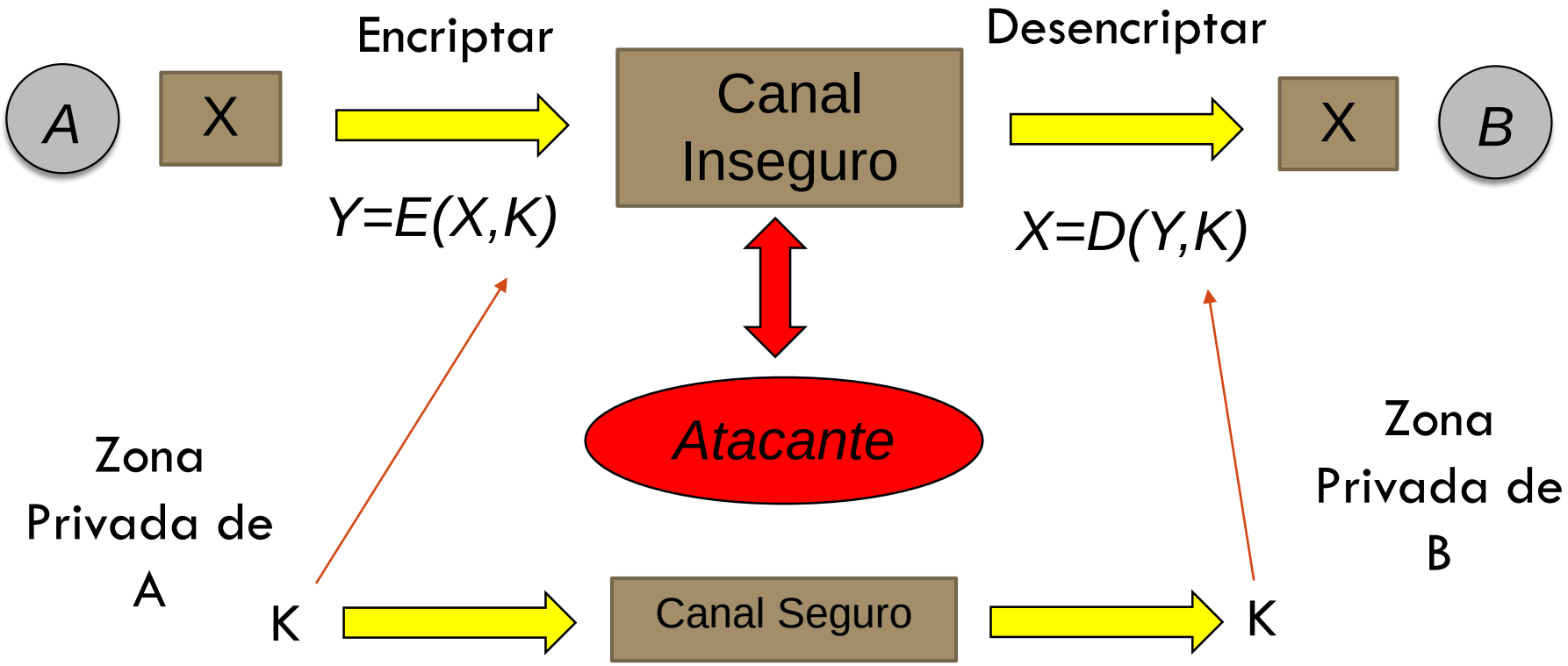
- Los algoritmos criptográficos modernos emplean una gran cantidad de claves, por tanto es difícil romper estos por la fuerza bruta.
- Por poner un ejemplo simple con algoritmo antiguo, el DES utiliza 2^{56} claves, es un número muy grande:
  - Si hiciésemos 1.00.000 de operaciones por segundo romperíamos el DES por la fuerza bruta (con 2^{56} tardaríamos 10^{24} años). Para hacernos una idea de lo grande que son estos número:
    - La probabilidad de ser fulminado por un rayo es 1 entre 2^{33}.
    - La probabilidad de que te toque la LOTO es 1 entre 2^{32}.
    - La probabilidad de ser fulminado por un rayo y te toque la LOTO en el mismo día es 1 entre 2^{56}.

Esquema resumen



- **Bloques:** Un bloque de texto claro se trata como un todo y se utiliza un algoritmo de cifrado para producir un bloque de texto cifrado de igual longitud.
- **Flujo:** es el que cifra un flujo de datos digitales de bit en bit o de byte en byte a cada tiempo.

Esquema de cifrado de clave privada



Criptosistema

- Concepto de **criptosistema:**
  - Podemos definir un criptosistema como un conjunto de 5 elementos (quintupla) { P, C, K, E_k, D_k}:
    - Un conjunto finito de textos planos asignado a P
    - Un conjunto finito de textos cifrados asignado a C
    - Un conjunto finito de claves a K
    - Una función de cifrado (algoritmo de encriptación): E_k
    - Una función de descifrado (algoritmo de desencriptación): D_k
    - Para todo elemento x perteneciente a P se verifica que
      - **$D_k(E_k(x))=x$ (Inyectividad del criptosistema)**
  - Esta definición es para un criptosistema simétrico por bloques, para cualquier otro criptosistema la definición es análoga teniendo en cuenta siempre la condición indispensable de inyectividad o función uno a uno:

Imagen extraída de http://commons.wikimedia.org/wiki/File:Injection.svg