1.- Introducción a la Seguridad de la Información

1.1- Generalidades
1.2- Introducción histórica
1.3- Terminología
1.4- Criptosistemas

1.1 Generalidades

- Internet, tal y como lo conocemos hoy, nació en los años 60 bajo el nombre **ARPANET**.
- La red ARPANET era una herramienta de investigación para aquellos que trabajaban para el gobierno de los Estados Unidos bajo la dirección de la agencia ARPA (Advance Research Projects Agency).
- El tráfico de ARPANET era el originado en las comunicaciones entre los laboratorios de Universidades, ejército y el propio gobierno. Gracias a ARPANET, investigadores separados geográficamente intercambiaban entre ellos, ficheros y mensajes electrónicos.
- A medida que esta red fue creciendo se dividió en 2:
  - **MILNET**, para uso militar y
  - **ARPANET** que continuó siendo para labores de investigación

1.1 Generalidades

- A principio de los 80 se definió un estándar para los protocolos de comunicación que intervenían en ARPANET y fue llamado **TCP/IP** *(Transmission Control Protocol / Internet Protocol)*, que es la base de casi todas las redes existentes hoy día.

- Hasta finales de 1988 muy poca gente tomaba en serio el tema de la seguridad en redes de computadores de propósito general

- Sin embargo, el 22 de noviembre de 1988 Robert T. Morris protagonizó el primer gran incidente de la seguridad informática: uno de sus programas se convirtió en el famoso **worm** o gusano de Internet.
  - Miles de ordenadores conectados a la red se vieron inutilizados durante días y las pérdidas se estiman en millones de dólares.

1.1 Generalidades

- Desde ese momento el tema de la seguridad en sistemas operativos y redes ha sido un factor a tener muy en cuenta por cualquier responsable o administrador de sistemas informáticos.

- A medida que **Internet** crece también crece el número de aplicaciones y servicios que hacen uso de la misma.

- Muchos de estos servicios utilizan información que debe ser protegida, al igual que deben ser autentificados los extremos que en este servicio toman parte.

1.1 Generalidades: ¿Qué es seguridad?

- Podemos entender como seguridad una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible.

- Como esta característica, particularizando para el caso de sistemas operativos o redes de computadores, es muy **difícil de conseguir** (según la mayoría de expertos, imposible),
  - se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad;
  - por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros.

1.1.1 Aspectos de la seguridad

- A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos:
  - confidencialidad,
  - integridad y
  - disponibilidad.

- La confidencialidad exige que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades.

- La integridad significa que los objetos sólo pueden ser creados o modificados por elementos autorizados, y de una manera controlada.

- La disponibilidad indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados; es el contrario de la negación de servicio.

1.1.2 Elementos de la seguridad

- Los tres elementos principales a proteger en cualquier sistema informático son:
  - el hardware,
  - el software y
  - los datos.

- Por hardware entendemos el conjunto formado por todos los **elementos físicos** de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento secundario o tarjetas de red.

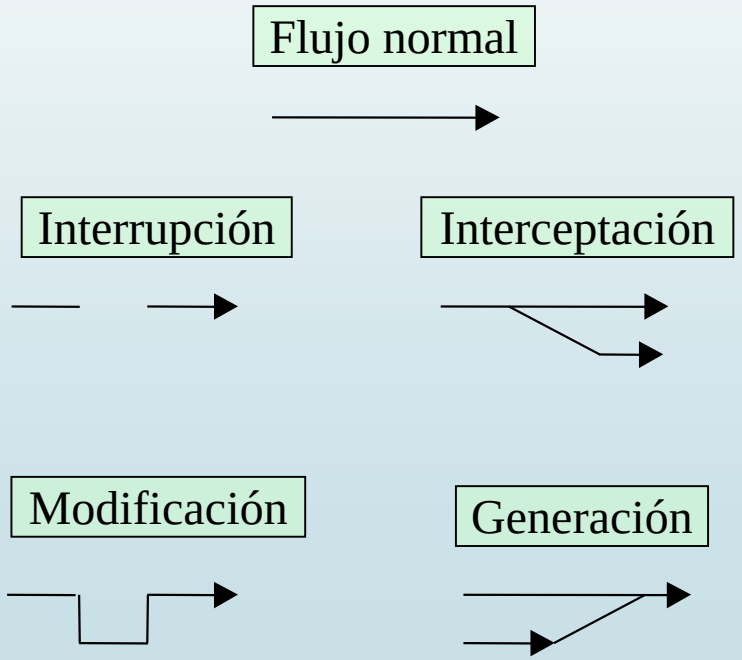
- Por software entendemos el conjunto de programas lógicos que hacen funcional al hardware, tanto sistemas operativos como aplicaciones.

- Por datos entendemos el conjunto de información lógica que manejan el software y el hardware
  - (como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos).

1.1.3 Amenazas a la seguridad

- Contra cualquiera de los tres elementos (pero principalmente sobre los datos) se pueden realizar multitud de ataques o, dicho de otra forma, están expuestos a diferentes amenazas.

- Generalmente, la clasificación más elemental de estas amenazas las divide en cuatro grandes grupos:
  - interrupción,
  - interceptación,
  - modificación
  - generación.



1.1.3 Amenazas a la seguridad

- Un ataque se clasifica como:
  - Interrupción si hace que un objeto del sistema se pierda, quede inutilizable o no disponible.
  - Interceptación si un elemento no autorizado consigue un acceso a un determinado objeto del sistema..
  - Modificación si además de conseguir el acceso consigue modificar el objeto.
  - Generación o fabricación si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el fabricado.

1.1.3 Amenazas a la seguridad

- Podemos clasificar a los elementos que potencialmente pueden amenazar a nuestro sistema en tres grupos:
  - Personas
  - Amenazas lógicas
  - Catástrofes

Personas

- La mayoría de ataques a nuestro sistema van a provenir en última instancia de personas que, intencionada o inintencionadamente, pueden causarnos enormes pérdidas.

- Generalmente se dividen en dos grandes grupos:
  - Los atacantes pasivos, aquellos que fisgonean por el sistema pero no lo modifican -o destruyen-, y
  - los activos, aquellos que dañan el objetivo atacado, o lo modifican en su favor.

1.1.3 Amenazas a la seguridad

AMENAZAS LÓGICAS

Bajo la etiqueta de "amenazas lógicas" encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (software malicioso, también conocido como malware) o simplemente por error (bugs o agujeros)

- **Software incorrecto**
  - A los errores de programación se les denomina **bugs**, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema, **exploits**
- **Herramientas de seguridad**
  - Cualquier herramienta de seguridad representa un **arma de doble filo**: de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos
- **Puertas traseras**
  - Durante el desarrollo de aplicaciones grandes es habitual entre los programadores insertar "atajos" en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando.

1.1.3 Amenazas a la seguridad

AMENAZAS LÓGICAS

- **Bombas lógicas**
  - Partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas
- **Canales ocultos**
  - Canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema; dicho de otra forma, un proceso transmite información a otros (locales o remotos) que no están autorizados a leer dicha información.
- **Virus**
  - Secuencia de código que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.
- **Gusanos**
  - Programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando bugs de los sistemas a los que conecta para dañarlos.

1.1.3 Amenazas a la seguridad

AMENAZAS LÓGICAS

- **Caballos de Troya**
  - Instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario, ocultan su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente.
  - Cuando un **intruso** consigue el privilegio necesario en el sistema, **instala troyanos** para ocultar su presencia o para asegurarse la entrada en caso de ser descubierto, por ejemplo:
    - es típico utilizar lo que se denomina un rootkit, que no es más que un conjunto de versiones troyanas de ciertas utilidades (netstat, ps, who. . .), para conseguir que cuando el administrador las ejecute no vea la información relativa al atacante, como sus procesos o su conexión al sistema;
    - otro programa que se suele suplantar es login, por ejemplo para que al recibir un cierto nombre de usuario y contraseña proporcione acceso al sistema sin necesidad de consultar /etc/passwd.

1.1.3 Amenazas a la seguridad

AMENAZAS LÓGICAS

- **Programas conejo o bacterias**
  - Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco. .), produciendo una negación de servicio.

- **Técnicas salami**
  - Robo automatizado de pequeñas cantidades de bienes (generalmente dinero) de una gran cantidad origen. El hecho de que la cantidad inicial sea grande y la robada pequeña hace extremadamente difícil su detección.
  - No se suelen utilizar para atacar sistemas normales, sino que su uso más habitual es en sistemas bancarios; sin embargo, como en una red con requerimientos de seguridad medios es posible que haya ordenadores dedicados a contabilidad, facturación de un departamento o gestión de nóminas del personal, es una amenaza a tener en cuenta.

CATÁSTROFES

Aún cuando son las amenazas menos probables, no hay que descartarlas (incendio, etc.)

1.1.4 Mecanismos de seguridad

Los mecanismos de seguridad de un sistema se dividen en tres grandes grupos:

- Prevención
- Detección
- Recuperación.

PREVENCIÓN

- Los mecanismos de **prevención** son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad;
  - **por ejemplo**, el uso de **cifrado** en la transmisión de datos se puede considerar un mecanismo de este tipo, ya que evita que un posible atacante escuche las transmisiones de información que circulen por la red.

DETECCIÓN

- Por mecanismos de **detección** se conoce a aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación;
  - ejemplos de estos mecanismos son los programas de **auditoría**.

1.1.4 Mecanismos de seguridad

RECUPERACIÓN

- Finalmente, los mecanismos de **recuperación** son aquellos que se aplican cuando una violación del sistema se ha detectado, para retornar a éste a su funcionamiento correcto;
  - ejemplos de estos mecanismos son la utilización de copias de seguridad o el hardware adicional.

- Dentro de este último grupo de mecanismos de seguridad encontramos un subgrupo denominado mecanismos de análisis forense, cuyo objetivo no es simplemente retornar al sistema a su modo de trabajo normal, sino averiguar el alcance de la violación, las actividades de un intruso en el sistema, y la puerta utilizada para entrar; de esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas de nuestra red.

1.1.4.1 Mecanismos de prevención

- Aunque los tres tipos de mecanismos son importantes para la seguridad de un sistema, se debe enfatizar en el uso de mecanismos de prevención y de detección;
  - la máxima popular "más vale prevenir que curar" se puede aplicar a la seguridad informática.

- Los mecanismos de prevención más habituales en redes son los siguientes:
  - Mecanismos de autenticación e identificación
  - Mecanismos de control de acceso
  - Mecanismos de seguridad en las comunicaciones

1.1.4.1 Mecanismos de prevención

Mecanismos de autenticación e identificación

- Hacen posible identificar entidades del sistema de una forma única, y posteriormente, una vez identificadas, autenticarlas (comprobar que la entidad es quién dice ser).
- Son los mecanismos más importantes en cualquier sistema, ya que forman la base de otros mecanismos que basan su funcionamiento en la identidad de las entidades que acceden a un objeto.
- Un grupo especialmente importante de estos mecanismos son los denominados **Sistemas de Autenticación de Usuarios**.

Mecanismos de control de acceso

- Cualquier objeto del sistema ha de estar protegido mediante mecanismos de control de acceso, que controlan todos los tipos de acceso sobre el objeto por parte de cualquier entidad del sistema.
  - Por ejemplo, dentro de Unix/Linux, el control de acceso más habitual es el discrecional (DAC Discretionary Access Control), implementado por los bits rwx y las listas de control de acceso para cada fichero (objeto) del sistema.

1.1.4.1 Mecanismos de prevención

MECANISMOS DE SEGURIDAD EN LAS COMUNICACIONES

- Es especialmente importante para la seguridad de un sistema proteger la confidencialidad y la integridad de la información que se transmite a través de la red.

- Para garantizar la seguridad en las comunicaciones, se debe hacer uso de mecanismos que se basan en la **Criptografía** (cifrado de clave pública, de clave secreta, firmas digitales, …)

- Aunque cada vez se utilizan más los protocolos seguros, aún es frecuente encontrar **conexiones en texto claro** ya no sólo entre máquinas de una misma subred, sino entre redes diferentes.

- Una de las mayores amenazas a la integridad de las redes es este tráfico sin cifrar, que hace extremadamente fáciles ataques encaminados a robar contraseñas o suplantar la identidad de máquinas de la red.

1.1.4.1 Mecanismos de prevención

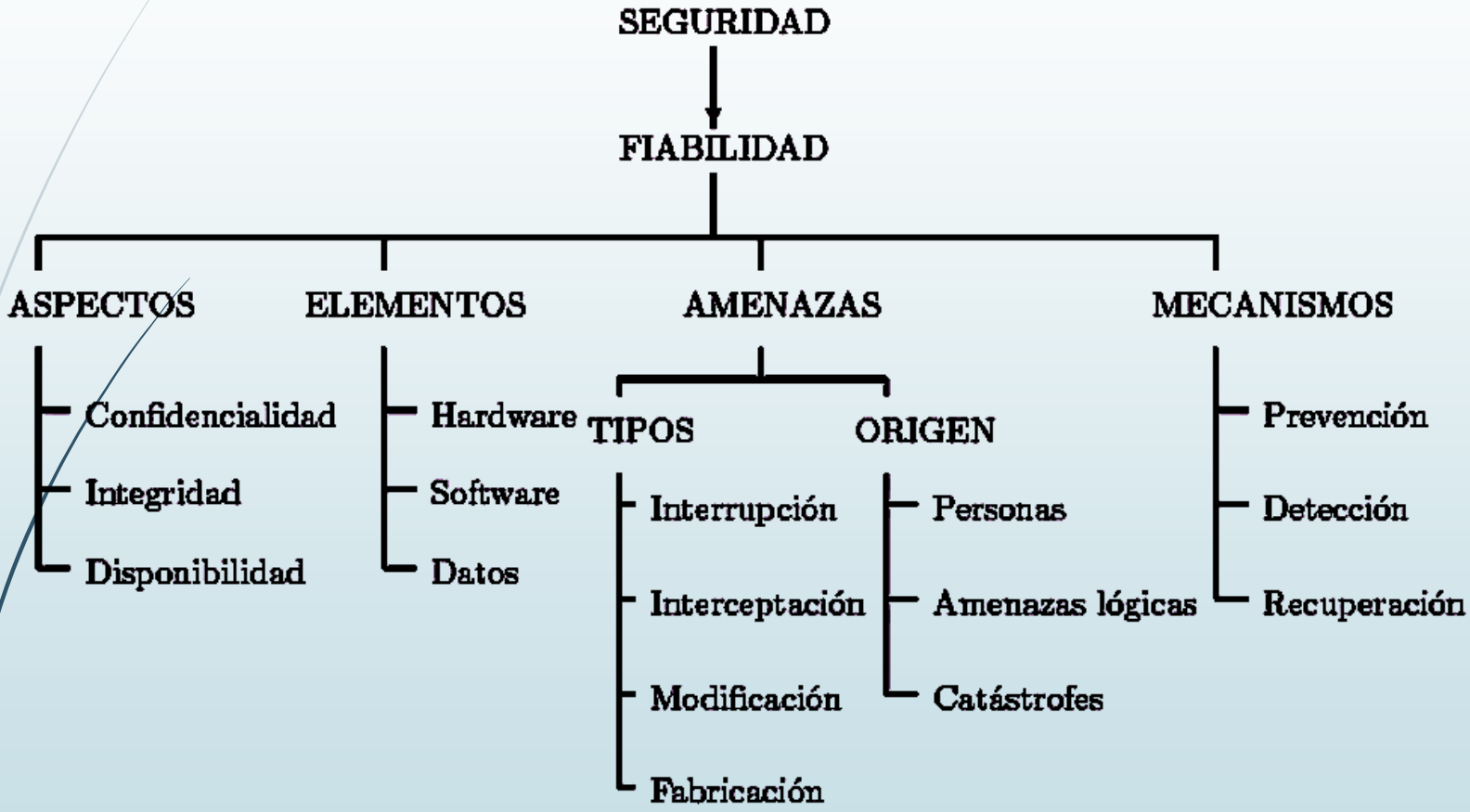
MECANISMOS DE SEGURIDAD EN LAS COMUNICACIONES

- **Cualquier sistema** establecido puede ser **atacado o roto**. Cada ataque distinto a un sistema requiere un análisis distinto para evaluar tanto su viabilidad como el daño que puede hacer si se lleva a cabo con éxito.

- Para **cada ataque** hay que encontrar **unas contramedidas** que hagan que el **coste** de llevar a cabo el ataque sea muy **superior** a lo que se puede **obtener de él**.
- Esas contramedidas están basadas en técnicas criptográficas.

- No hay una única herramienta global criptográfica si no que existen **distintas técnicas** para lograr distintos objetivos, como
  - cifrar mensajes,
  - intercambio seguro de claves criptográficas,
  - mantener y asegurar la integridad de un mensaje así como
  - garantizar la autenticidad de un mensaje recibido.

Resumen nociones generales



1.2 Introducción histórica

- Aun cuando se realizará un estudio de los métodos clásicos de cifrado más adelante, veremos algunas notas históricas.
- A lo largo de la Historia, siempre ha existido la necesidad de transmitir secretamente información de una persona a otra.
- Desde los tiempos más remotos se **han utilizado códigos secretos** para lograr que un **mensaje** resultara **incomprensible** para las **personas no autorizadas** a leerlo.
- En las tumbas del antiguo Egipto existen múltiples ejemplos de escritura cifrada.
- La **Criptología** es la rama de la ciencia que, desde antiguo, estudia la escritura secreta.
  - Etimológicamente proviene de las palabras griegas kriptos (oculto) y logos (tratado, estudio).

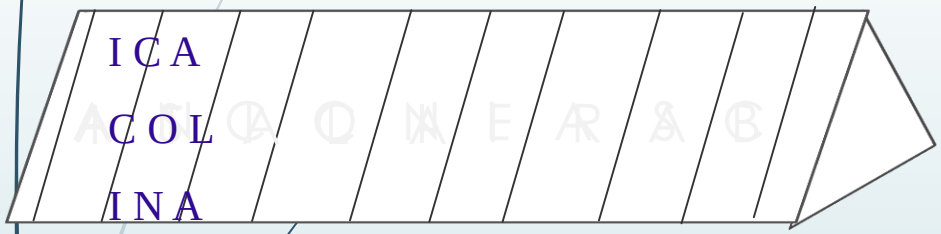
1.2 Introducción histórica

SCÍTALA ESPARTANA

- El historiador griego Plutarco que vivió entre los siglos I y II d.C. nos describe la ***scitala espartana*** consistente en una vara de la que se preparaban dos ejemplares idénticos, uno quedaba en poder de la persona que enviaba el mensaje y el otro en la del receptor del mismo.
- Para expedir un mensaje se enrollaba alrededor de la vara una tira larga y estrecha de pergamino o papiro y se escribían las letras en vertical de arriba a abajo y de izquierda a derecha. El mensaje no es descifrable si no se vuelve a enrollar el pergamino en la vara original o una idéntica.
- El primer empleo de escritura secreta del que se tiene constancia data del siglo V a.C. en la guerra entre Atenas y Esparta.
- **En este sistema de cifrado las letras son cambiadas de posición.**

1.2 Introducción histórica

SCÍTALA ESPARTANA



AA I
S N T
I C A
C O L
I N A
F L
R A
A S
B C

Texto en claro

m = ASI CIFRABAN CON LA SCITALA

Texto cifrado

c = AAISNTICACOLINAFLRAASBC

Se trata de un sistema de cifra por transposición

1.2 Introducción histórica

SCÍTALA ESPARTANA

- **Ejemplo**

El mensaje

ΤΩΝ ΕΝ ΘΕΡΜΟΠΥΛΑΙΣ ΘΑΝΟΝΤΩΝ ΕΥΚΛΕΗΣ ΜΕΝ Α ΤΥΧΑ

(de los muertos en las Termópilas es gloriosa la suerte)

en una scitala en la que se hubieren dado diez vueltas con la tira de pergamino y escrito cinco letras en cada vuelta, el mensaje en el pergamino extendido quedaría de esta forma:

ΤΜΑΚΑΩΟΝΛ ΝΠΟΕΤ ΥΝΗΥΕΛΤΣΧΝΑΩ Α ΙΝΜ ΘΣ Ε Ε ΕΝ ΡΘΥ

1.2 Introducción histórica

SCÍTALA ESPARTANA

La vista de la scitala con el pergamino enrollado se puede esquematizar en la siguiente tabla de diez filas y cinco columnas:

ΤΩΝ ΕΝ ΘΕΡΜΟΠΥΛΑΙΣ ΘΑΝΟΝΤΩΝ ΕΥΚΛΕΗΣ ΜΕΝ Α ΤΥΧΑ

Τ	Μ	Α	Κ	Α
Ω	Ο	Ν	Λ	
Ν	Π	Ο	Ε	Τ
	Υ	Ν	Η	Υ
Ε	Λ	Τ	Σ	Χ
Ν	Α	Ω		Α
	Ι	Ν	Μ	
Θ	Σ		Ε	
Ε		Ε	Ν	
Ρ	Θ	Υ		

ΤΜΑΚΑΩΟΝΛ ΝΠΟΕΤ ΥΝΗΥΕΛΤΣΧΝΑΩ Α ΙΝΜ ΘΣ Ε Ε ΕΝ ΡΘΥ

1.2 Introducción histórica

Cifrador de Polybios

- Del siglo II a.d.C., es el cifrador por sustitución de caracteres más antiguo que se conoce.

El criptograma duplica la cantidad de caracteres del texto en claro por lo que no es un buen sistema de cifra.

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

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

M_1 = QUE BUENA IDEA

C_1 = DA DE AE AB DE AE

CC AA BD AD AE EA

?

M_2 = LA DEL GRIEGO

C_2 = 31 11 14 15 31 22

42 24 15 22 34

1.2 Introducción histórica

Cifrado de Julio César

- El historiador romano Suetonio, contemporáneo de Plutarco, nos describe un sistema de ***cifrado*** utilizado por ***Julio César*** (siglo I a.C.):
  - "...Para quienes deseen saber más diré que sustituía la primera letra del alfabeto, A, por D y así sucesivamente con todas las demás...".
- También el emperador Augusto parece que utilizaba un sistema muy similar:
  - "...cada vez que escribía en código, ponía una B en lugar de A, C en lugar de B y así sucesivamente con todas las letras restantes...".

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

- El sistema de cifrado de César o de Augusto se basa en la sustitución de letras.

1.2 Introducción histórica

Cifrado de Julio César

Ejemplo

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

- La frase que pronunció en una expedición militar cuando tras bajarse de una barca cayó de bruces

  TENEO TE AFRICA

  en lenguaje cifrado se escribe como:

  AHQHR AH DIVMFD

- Para descifrar un mensaje en clave bastaba con girar, para cada letra, el círculo cifrario tres posiciones en el sentido contrario al de las agujas del reloj. Así

  BHQM BMGM BMFM

  significa

  VENI VIDI VICI

1.2 Introducción histórica

Cifrado de Julio César

- Es un cifrador por sustitución en el que las operaciones se realizan módulo n, con n el número de elementos del alfabeto.

m = **E**L PATIO D**E** MI CASA **E**S PARTICULAR

c = **H**Ñ SDWLR D**H** OL FDVD **H**V SDUWLFXÑDU

Cada letra se cifrará siempre igual: es una debilidad

Alfabeto de cifrado del César para castellano mod 27

m_i	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
c_i	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

1.2 Introducción histórica

ATBASH HEBREO

- Un método para cifrar mensajes basado también en la sustitución de letras es el ***atbash*** hebreo en el que se escriben las veintidós letras del alfabeto en dos líneas, las once primeras se sitúan en la primera línea escritas de izquierda a derecha y las otras once en la segunda línea de derecha a izquierda. Cada letra se sustituye por la situada en la misma posición de la otra línea.

1.2 Introducción histórica

- En los siglos posteriores a la caída del Imperio Romano no se tiene conocimiento del uso de la escritura secreta, hasta los siglos XIII-XIV, ahora bien es de suponer que si se utilizaron fueron con motivo militar o diplomático y basados en métodos de sustitución o transposición de caracteres.
- En el renacimiento, al igual que ocurrió con muchas ciencias, hay una evolución de la Criptología.
  - Los métodos de cifrado están basados en la sustitución de unas letras por otras o de palabras por letras u otras palabras o incluso de letras por palabras
  - Se utilizan signos no convencionales y varios alfabetos.

1.2 Introducción histórica

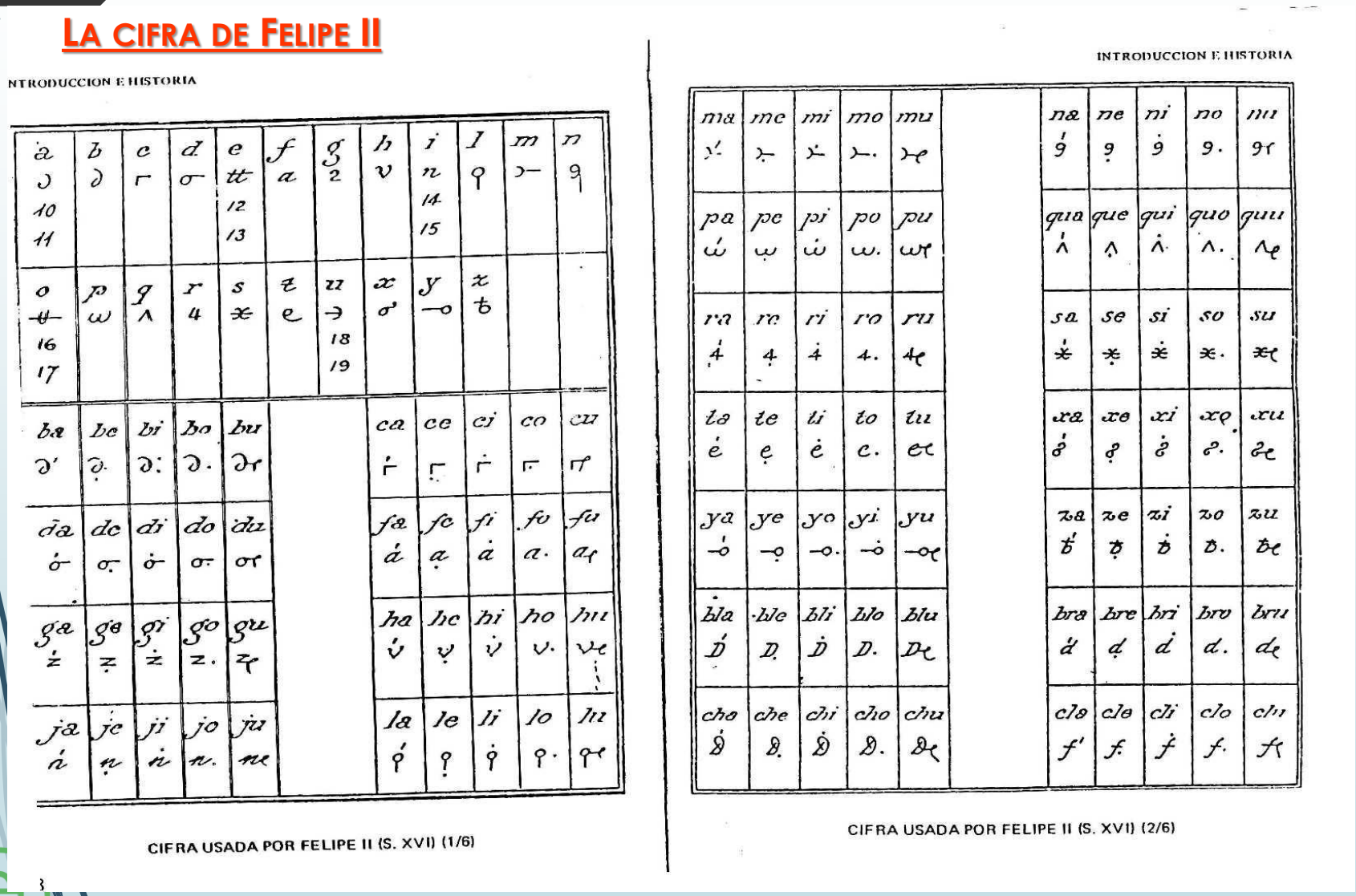
La cifra de Felipe II

- En España como en el resto de Europa el uso de información cifrada era generalizado en el ámbito diplomático y militar.
- Merece especial mención ***la cifra***, utilizada por Felipe II (siglo XVI) en la correspondencia con el Duque de Alba en las importantes misiones exteriores de éste.
  - Se compone de seis tablas divididas en cuatro grupos de casillas en los que aparecen las letras del alfabeto, las parejas y los tríos de letras más comunes y las palabras que se supone se van a utilizar con más frecuencia.
  - A cada casilla corresponde uno o más signos no convencionales formados por letras, números o trazos especiales.

Se trata pues de un sistema de cifrado por sustitución no simple

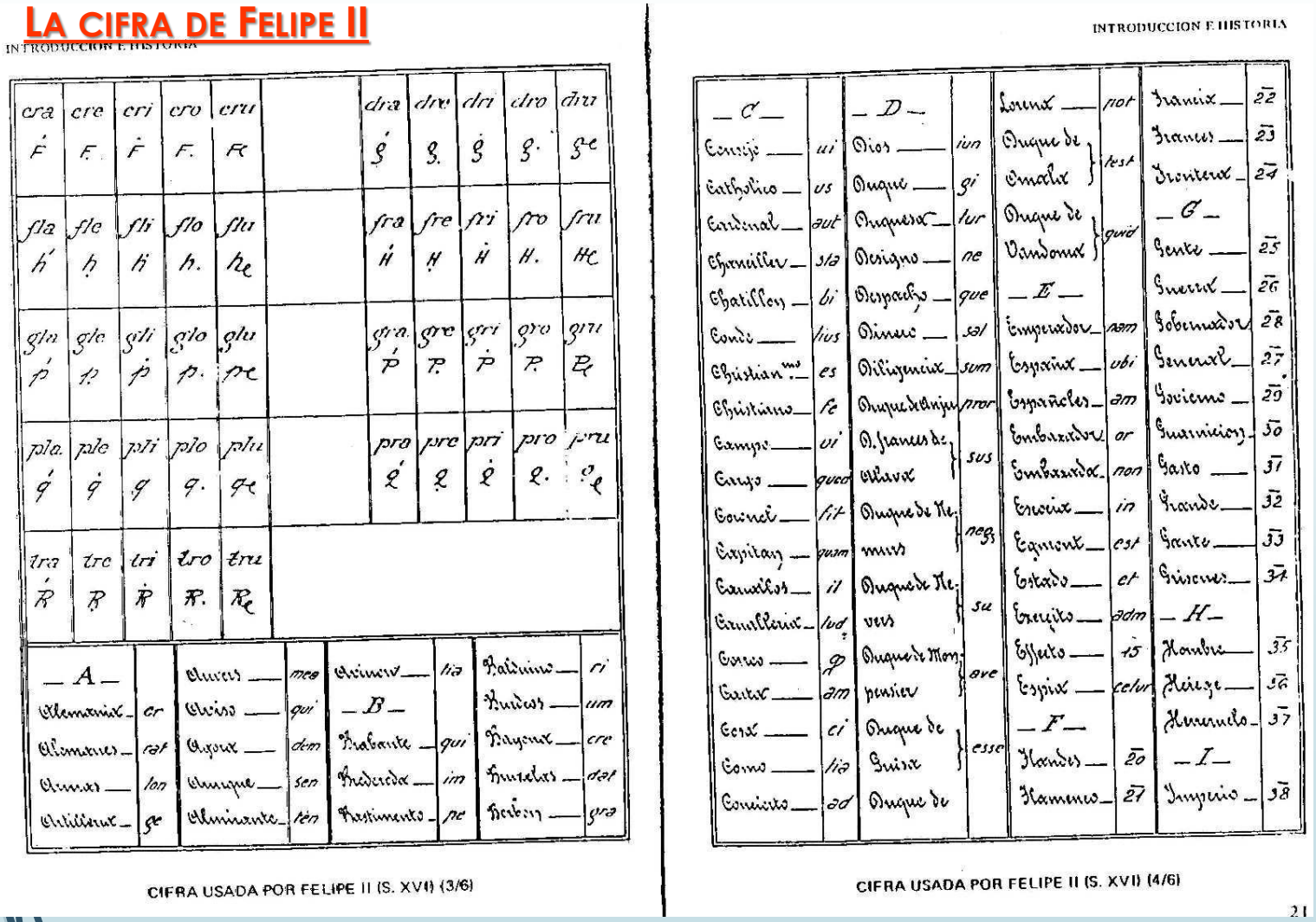
1.2 Introducción histórica

La cifra de Felipe II



1.2 Introducción histórica

La cifra de Felipe II

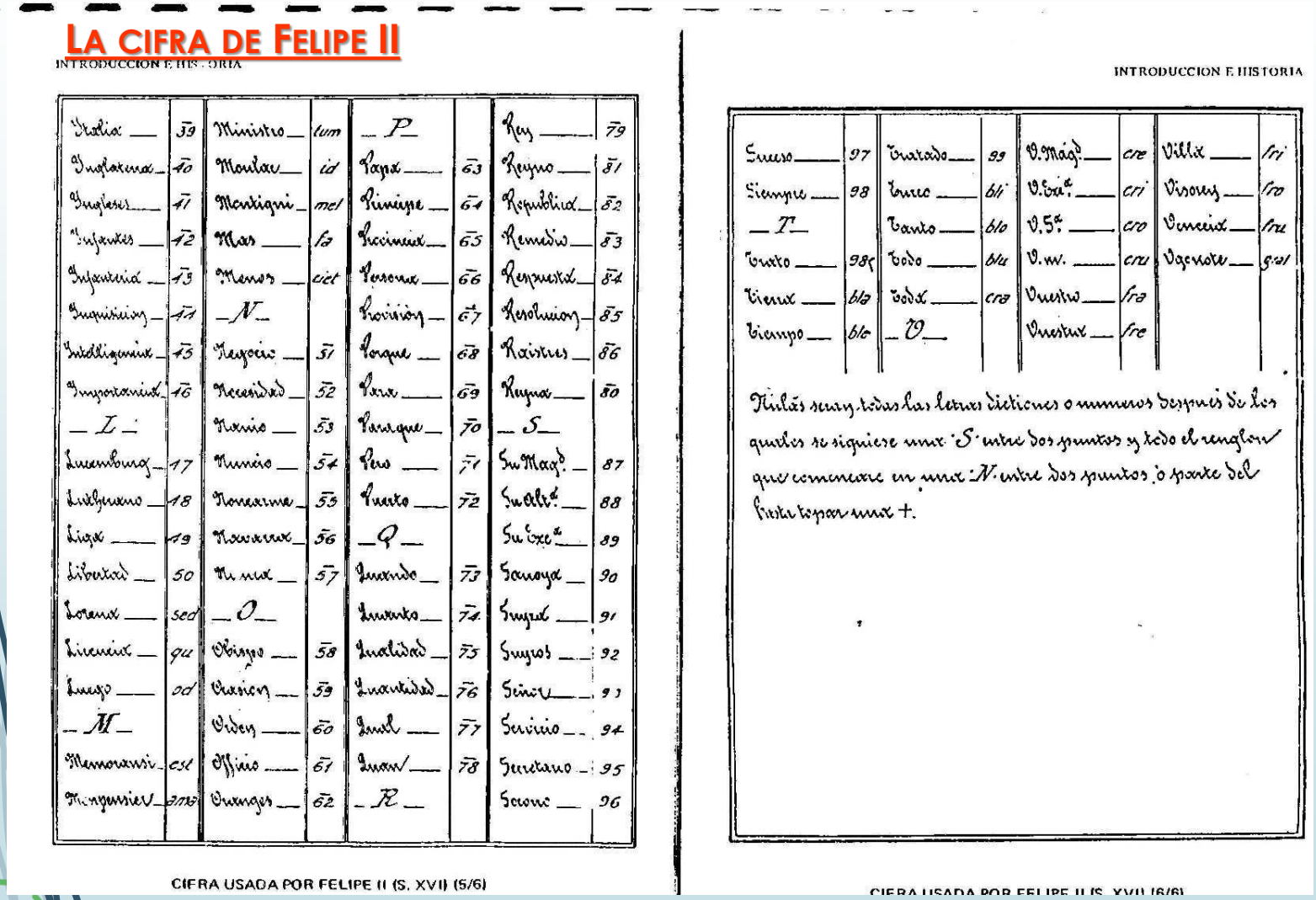


CIFRA USADA POR FELIPE II (S. XVI) (3/6)

CIFRA USADA POR FELIPE II (S. XVI) (4/6)

1.2 Introducción histórica

La cifra de Felipe II



INTRODUCCION E HISTORIA

Italia	39	Ministro	tum	P		Rey	79
Inglaterra	40	Montar	id	Papa	63	Reyno	81
Ingleses	41	Mantiqui	mel	Principe	64	Republica	82
Infantes	42	Mar	fa	Precisa	65	Remedio	83
Infantica	43	Menos	cict	Persona	66	Respuesta	84
Inquisicion	44	N		Provision	67	Resolucion	85
Intelligencia	45	Negocio	51	Porque	68	Raizes	86
Importancia	46	Necesidad	52	Para	69	Reyna	80
L		Nuevo	53	Paraque	70	S	
Luxemburg	47	Nuncio	54	Pues	71	Su Magd.	87
Lutheano	48	Nonagesima	55	Puesto	72	Su Alteza	88
Liga	49	Nosotros	56	Q		Su Excia	89
Libertad	50	Nunca	57	Quando	73	Saboya	90
Lorena	sed	O		Quanto	74	Suyos	91
Livonia	qu	Obispo	58	Qualidad	75	Suyos	92
Luego	od	Ocasion	59	Quantidad	76	Sitio	93
M		Oden	60	Qual	77	Servicio	94
Memoranda	esl	Officio	61	Quan	78	Secretario	95
Margarita	ant	Ounges	62	R		Socorro	96

CIFRA USADA POR FELIPE II (S. XVI) (5/6)

INTRODUCCION E HISTORIA

Suelo	97	Tratado	99	V. Mágd.	cre	Villa	fri
Siempre	98	Turco	bli	V. Exa.	cri	Visorey	fro
T		Tanto	blo	V. S.	cro	Venecia	fru
Tanto	98p	Todo	blu	V. m.	cru	Vagamos	gui
Tiene	bla	Todo	cra	Vuestro	fra		
Tiempo	ble	O		Vuestra	fre		

Nulas seran todas las letras dichiones o numeros despues de los quales se siguiere una S entre dos puntos y todo el renglon que comenzare en una N entre dos puntos o parte del resto topar una +.

CIFRA USADA POR FELIPE II (S. XVII) (6/6)

1.2 Introducción histórica

El cifrador de Alberti

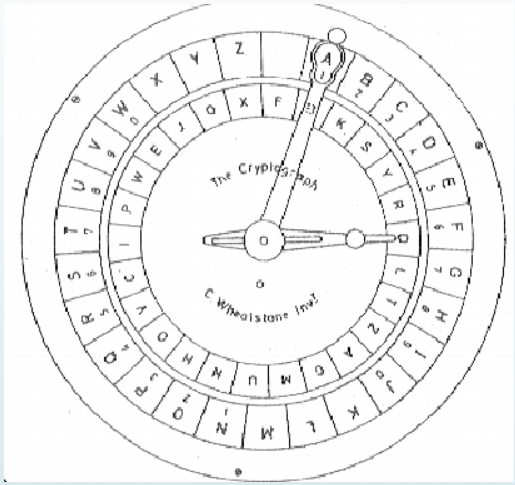
- En los siglos XVI y XVII se utiliza muy activamente la Criptología, pero no hay grandes progresos en la aparición de nuevos métodos, todos están basados en la sustitución.
- **Leon Battista Alberti diseña en el siglo XVI un disco para cifrar** en el que ya no hay una correspondencia única entre el carácter del texto en claro a cifrar y el criptograma obtenido.

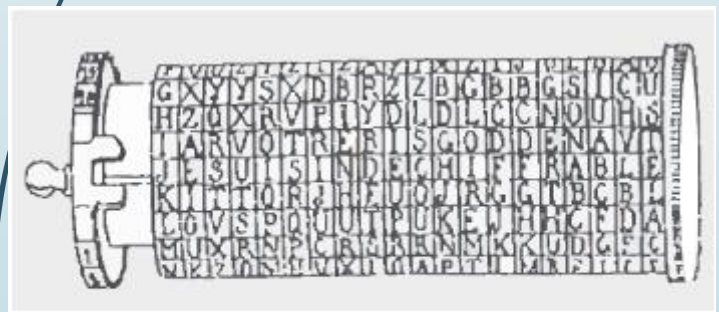
- Como este tipo de cifradores hacía uso de más de un alfabeto se les conoce como polialfabéticos, en comparación con los anteriores que se denominan monoalfabéticos.
- En este caso, se hace uso ya de una clave secreta al ajustar en una posición los discos antes de cifrar

1.2 Introducción histórica

CIFRADORES DEL SIGLO XIX

- En el siglo XIX aparece una nueva técnica (ya utilizada en cierto modo por los griegos) consistente en la alteración del orden de los símbolos del mensaje. Esta técnica es combinada con la sustitución.
- Se utilizan máquinas de cifrar, como las de Wheatstone y Brazeries.





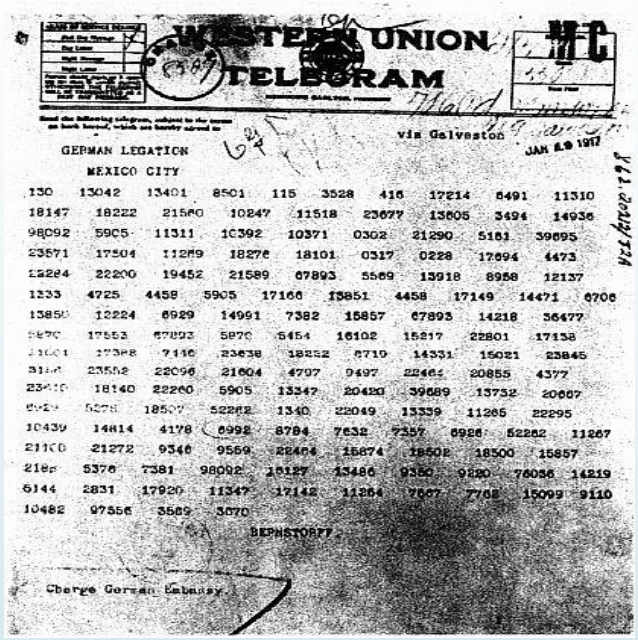
Cifrador de Bazeries (1890)

Cifrador de Wheatstone (1867)

1.2 Introducción histórica

SIGLO XX: ANTES DEL ORDENADOR

- Durante la Primera Guerra Mundial los ingleses consiguieron averiguar el método de cifrado del ***telegrama Zimmernan***, utilizado por los alemanes, que usaba un código para asignar cifras a las palabras de acuerdo con un libro de claves que poseían el emisor y el receptor del mensaje.



- Los franceses desmantelaron otro método utilizado por los alemanes, el ***sistema ADFGX***, que usaba tan solo esas letras para sustituir cada letra del mensaje sin cifrar por una combinación de dos de esas cinco letras, realizando posteriormente una transposición de longitud 20. La sustitución se hacía con la tabla

	A	D	F	G	X
A	n	b	x	r	u
D	q	o	k	d	v
F	a	h	s	g	f
G	m	z	c	l	t
X	e	i	p	j	w

1.2 Introducción histórica

SIGLO XX: ANTES DEL ORDENADOR

	A	D	F	G	X
A	n	b	x	r	u
D	q	o	k	d	v
F	a	h	s	g	f
G	m	z	c	l	t
X	e	i	p	j	w

Ejemplo 3

El mensaje

PETAIN MONTAG ATTENTAT

(Petain Lunes Atentado)

una vez hecha la sustitución, quedaría como

XFXAGXFAXDAA GGAXAAGX | FAFG FAGXGXXAAAGXFAGX

y realizando la transposición

XFFAXFAGGFXAFGAXXGDXAXAAGAGAAGXXAFAAGGXX

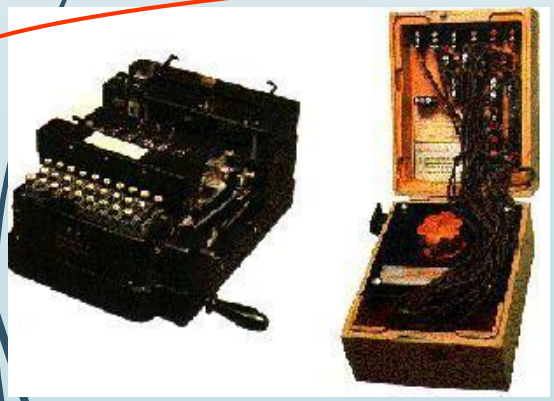
1.2 Introducción histórica

SIGLO XX: DESPUÉS DEL ORDENADOR

- El empujón decisivo para la Criptología se produce en el siglo pasado con motivo de las Guerras Mundiales.

- Se desarrollan diversas máquinas de cifrado con rotores que permiten un cifrado polialfabético.

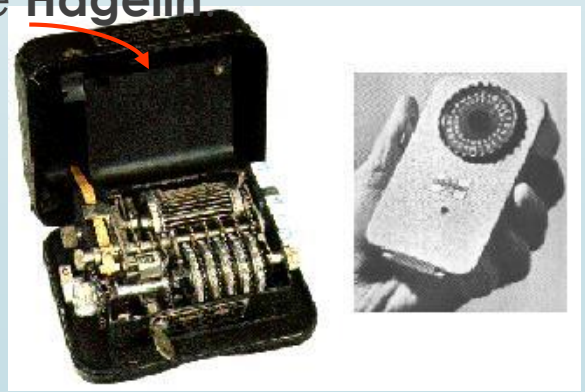
- De estas máquinas, cuyo papel principal fue su utilización para enviar mensajes cifrados precisamente en la Segunda Guerra Mundial, destacan tanto por sus características como por el halo de misterio que las rodeaba dos de ellas:
  - la máquina **Enigma** y la de **Hagelin**



Simulador enigma

Lectura 9.2 de M.J. Lucena

M.J. Lucena pdf



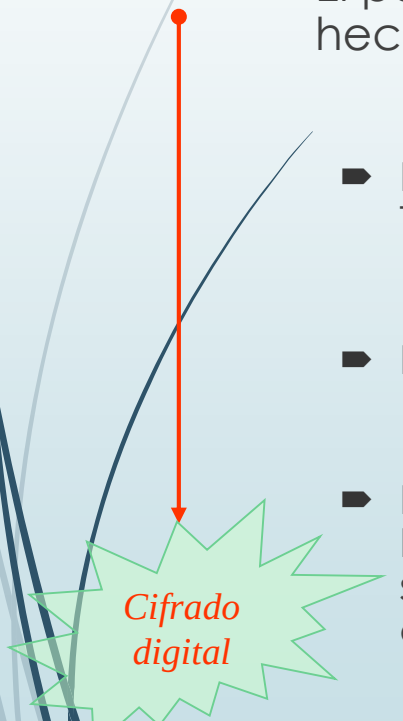
1.2 Introducción histórica

SIGLO XX: DESPUÉS DEL ORDENADOR

- Con la aparición de los ordenadores los métodos de cifrado anteriores resultan sumamente vulnerables por la capacidad de cálculo de los mismos.
- Los criterios utilizados para cifrar mensajes, en consecuencia, se establecen pensando en el posible ataque al sistema mediante un ordenador.
- Se habla así de sistemas computacionalmente seguros o inseguros, dependiendo de la potencia de cálculo de los ordenadores existentes.

1.2 Introducción histórica

- La criptografía clásica abarca desde tiempos inmemoriales hasta la mitad del siglo XX.
- El punto de inflexión en esta clasificación la marcan tres hechos relevantes:
  - En el año 1948 se publica el estudio de C. Shannon sobre la Teoría de la Información.
  - En 1974 aparece el estándar de cifrado DES.
  - En el año 1976 se publica el estudio realizado por W. Diffie y M. Hellman sobre la aplicación de funciones matemáticas de un solo sentido a un modelo de cifra, denominado cifrado con clave pública.



https://blog.segu-info.com.ar/2013/05/gchq-y-el-origen-de-la-criptografia-de.html?m=0

http://www.criptored.upm.es/intypedia/video.php?id=historia-criptografia&lang=es

1.3 Terminología

- Aunque nos hemos referido ya a algunos términos, daremos a continuación un pequeño vocabulario específico.

CIFRAR-DESCIFRAR

- Cuando deseamos enviar un mensaje de manera que resulte incompresible para aquellas personas a las que no va dirigido utilizando determinada técnica, diremos que ***ciframos*** el mensaje. El destinatario del mismo debe ***descifrarlo*** utilizando esa misma técnica.

1.3 Terminología

TEXTO EN CLARO-CRIPTOGRAMA

- Un mensaje que se desea cifrar es llamado ***texto en claro*** o ***texto plano***, una vez cifrado se dice que es un ***criptograma***.
  - Para cifrar un texto en claro normalmente se suele dividir en bloques de una longitud preestablecida, que a veces consisten en un sólo carácter. Así, cada bloque m de texto plano es convertido en un bloque de texto cifrado c.
  - Denotaremos este proceso con la letra E y lo representaremos como E(m)=c, por ejemplo en el método utilizado por Julio César

$$E(A)=D,\ E(B)=E,\ldots,E(X)=C$$

  - El proceso de descifrado lo expresaremos con D. En el cifrado de César, por ejemplo, denotaremos

$$D(D)=A,\ D(E)=B,\ldots,D(C)=X$$

- Por supuesto, resulta esencial que el proceso de descifrado sea opuesto al de cifrado, esto es

$$D(E(m))=m$$

1.3 Terminología

CRIPTOSISTEMA-CLAVE

- Una función cifradora E junto con su correspondiente función descifradora D es conocido como un ***criptosistema o sistema criptográfico***.
- El cifrado y descifrado de los mensajes regularmente requiere de una pieza especial para el conocimiento del criptosistema conocida como ***clave***.
  - Por ejemplo, en el método de J. César la clave es la cantidad con la que cada letra es desplazada a la derecha o izquierda dentro de la tabla

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

  - Con ese número podemos conocer el orden para cifrar y descifrar los mensajes.

1.3 Terminología

CRIPTOGRAFÍA-CRIPTOANÁLISIS

- La ciencia que estudia el diseño de criptosistemas es conocida como ***criptografía***.
- En la creación de un criptosistema, el ***criptógrafo*** debe tener como objetivo que el sistema sea lo más ***seguro*** posible, esto es, debe crear el sistema de manera que una persona no autorizada, que no conozca la clave, no pueda descifrar los mensajes.
- Las personas que intentan descifrar mensajes sin conocer la clave son conocidos como ***criptoanalistas*** y la ciencia que intenta romper los criptosistemas, descifrando en un tiempo razonable el contenido de un mensaje sin conocer la clave, es llamada ***criptoanálisis***.

1.3 Terminología

CRIPTOLOGÍA

- Los campos de la criptografía y el criptoanálisis, son conocidos en su conjunto como ***criptología***.

- En el análisis de la seguridad de un criptosistema frente al criptoanálisis el criptógrafo debe asumir que el criptoanalista tiene un gran conocimiento del sistema, de hecho éste puede conocer la forma de cifrar y descifrar y tener múltiples ejemplos de texto en claro y del correspondiente texto cifrado.

1.3 Terminología

ESPACIO DE CLAVES

- El componente fundamental del criptosistema del que carece el criptoanalista es la clave.
  - El objetivo de este último es descubrir la clave correcta de entre el conjunto K de todas las posibles a utilizar, este conjunto es conocido como el ***espacio de claves***.
- El criptoanalista puede conocer, por ejemplo, que el criptosistema es el método de cifrado de César pero desconocer el número de posiciones que es desplazada cada letra.
  - Su meta es averiguar la clave utilizada dentro del espacio $K=\{1,2,...,21\}$.

1.4 Criptosistemas

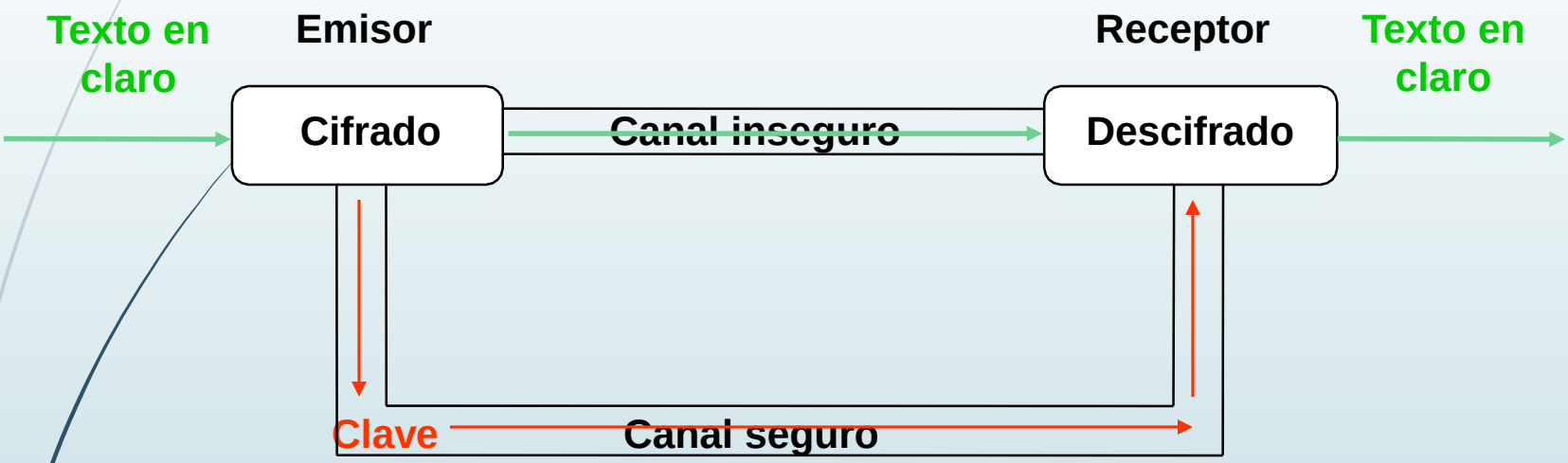
COMPONENTES

- Todo criptosistema debe constar de cinco componentes: M,C,K,E,D, donde
  - **M** es el conjunto de todos los mensajes en claro.
  - **C** es el espacio de todos los criptogramas.
  - **K** es el espacio de claves.
  - **E** es el conjunto de todos los métodos de cifrado, es decir, $E=\{E_k : M \longrightarrow C / k \in K\}$. Cada método de cifrado E_k está definido por un algoritmo de cifrado, que es común a todos los métodos, y una clave $k \in K$ que lo diferencia del resto.
  - **D** es el espacio de los métodos de descifrado, $D=\{D_k : C \longrightarrow M / k \in K\}$. Al igual que en el punto anterior, cada método de descifrado D_k está definido por un algoritmo de descifrado, común a todos los D_k, y una clave que lo distingue de los demás métodos.
- Para una clave k cualquiera la transformación D_k debe ser inversa de E_k, esto es

$$D_k[E_k(m)]=m \quad \forall m \in M$$

1.4 Criptosistemas

Esquema de un sistema de cifrado



1.4 Criptosistemas

REQUISITOS

- Todo criptosistema debe cumplir, al menos, tres requisitos esenciales:
  - Todas las transformaciones de cifrado y descifrado, E_k y D_k, deben ser eficientes para cualquier clave $k \in K$, en el sentido de que el tiempo y medios consumidos no supongan un entorpecimiento del normal proceso de la información.
  - El sistema debe resultar de fácil uso, esto es: debe ser factible la implementación de los algoritmos de cifrado y descifrado y utilizar claves lo más sencillas posible.
  - La seguridad del sistema sólo debe depender del secreto de las claves y no de los algoritmos de cifrado y descifrado. De esta manera si es descubierta la clave por un criptoanalista se puede sustituir por otra, operación que resulta mucho más sencilla que cambiar los algoritmos.

1.4.1 Criptosistemas: Clasificación

- Podemos realizar varias ***clasificaciones*** de los criptosistemas, atendiendo a diversos criterios.

ANTIGUEDAD

- **Clásicos**: Si su origen es anterior a la aparición del ordenador.
- **Modernos**: Se fundamentan en la informática. Necesitan ser actualizados (en muchos casos son desestimados) al ritmo de progreso de la potencia de cálculo de los ordenadores.

IGUALDAD ENTRE LAS CLAVES DE CIFRADO Y DESCIFRADO

- **Simétricos**: La clave de descifrado es la misma que la del cifrado o se puede obtener a partir de ella.
- **Asimétricos**: Las claves de cifrado y descifrado son distintas y no puede obtenerse una a partir de la otra, salvo que se disponga de alguna información adicional.

1.4.1 Criptosistemas: Clasificación

Forma de cifrar

- **Cifrado en bloque**: El mismo algoritmo de cifrado se aplica a un bloque de información (grupo de caracteres, número de bytes, etc.) repetidas veces, usando la misma clave.

- **Cifrado en flujo**: El algoritmo de cifrado se aplica a un elemento de información (carácter, bit) mediante un flujo de clave en teoría aleatoria y mayor que el mensaje.

Conocimiento de la clave

- **De clave privada o secreta**: Las claves de cifrado y descifrado sólo son conocidas por personal autorizado.

- **De clave pública**: El conocimiento de la clave de cifrado se puede hacer pública, pero la de descifrado sólo es conocida por el receptor del mensaje.

1.4.2 Criptosistemas: Números grandes

- Los actuales algoritmos criptográficos emplean **claves con un elevado número de bits**, y usualmente se mide su **calidad** por la **cantidad de esfuerzo computacional** que se necesita para romperlos.

- El tipo de ataque mas simple es la ***fuerza bruta***, que simplemente trata de ir probando una a una todas las claves.
  - Por ejemplo, el algoritmo DES tiene 2^{56} posibles claves.
  - ¿Cuanto tiempo nos llevaría probarlas todas si, por ejemplo, dispusieramos de un computador capaz de probar un millón de claves por segundo?

    Tardaríamos más de 2200 años
  - Si la clave tuviera 128 bits, el tiempo requerido sería de 10^{24} años, que es aproximadamente cien billones de veces la edad del universo.

- Este dato nos debe disuadir de emplear mecanismos basados en la fuerza bruta para *reventar* claves de 128 bits.

1.4 Criptosistemas

FUNDAMENTOS DE LA SEGURIDAD INFORMÁTICA

- Tres son los pilares sobre los que descansa toda la teoría asociada a los criptosistemas:
  - Teoría de la Información
    - Estudios realizados por Claude Shannon
  - Teoría de los Números
    - Estudio de las matemáticas discretas
  - Teoría de la Complejidad de los Algoritmos
    - Clasificación de los problemas

1.4.3 Criptosistema seguro de Shannon

- En **1949**, Shannon, con la publicación de su artículo "*Communication Theory of Secrecy Systems*" basado en su obra sobre la Teoría de la Información, sienta las **bases para el tratamiento matemático de la criptología** obteniendo **conclusiones válidas** para cualquier **criptosistema**.

SEGURIDAD TEÓRICA

- Si **no** se puede obtener **ninguna información del texto en claro** incluso cuando el **criptoanalista** dispone de **tiempo y recursos ilimitados**, diremos que el criptosistema alcanza la ***seguridad teórica***.
  - En realidad, en todos los criptosistemas el conocimiento de texto cifrado supone alguna información sobre el texto en claro.

1.4.3 Criptosistema seguro de Shannon

SISTEMA ROMPIBLE

- Se dice que un sistema criptográfico es ***rompible*** si a través del **análisis de texto cifrado** se puede **determinar** de una forma única el **texto en claro**.
  - Es importante resaltar que todos los **criptosistemas aceptados en la actualidad** son **rompibles** en el sentido de que no alcanzan la seguridad teórica, ahora bien **son computacionalmente seguros**, esto es, con los medios computacionales actuales la cantidad de tiempo necesario para que un criptoanalista obtenga el texto en claro a partir de uno o varios criptogramas interceptados es excesiva.

SEGURIDAD PRÁCTICA

- Se dice que en un criptosistema se cumplen los requisitos de la ***seguridad práctica*** si el sistema no se puede romper con los recursos computacionales disponibles en un tiempo razonable.

SECRETO PERFECTO

- En un criptosistema se dan las condiciones de ***seguridad perfecta*** si $\mathbf{P(m_i/c_j)=P(m_i)}$ $\forall \mathbf{i,j}$, o sea, si se intercepta un mensaje cifrado c_j no aporta ninguna información sobre el texto en claro original m_i.

1.4.3 Criptosistema seguro de Shannon

- Si por el contrario el sistema cumpliera la condición I(C,M)=0, jamás podríamos romperlo, ni siquiera empleando una maquina con capacidad de proceso infinita.
  - Por ello los criptosistemas que cumplen esa condición de Shannon se denominan también ***criptosistemas ideales***.

TEOREMA

- El secreto perfecto requiere que el número de claves en el criptosistema sea al menos tan grande como el de posibles mensajes. O, equivalentemente, *la longitud de la clave debe ser mayor o igual que la del texto en claro*.
  - Esto vuelve inútiles a estos criptosistemas en la práctica, porque si la clave es tanto o más larga que el mensaje, a la hora de protegerla nos encontraremos con el mismo problema que teníamos para proteger el mensaje.

1.4.3 Criptosistema seguro de Shannon

DIFUSIÓN Y CONFUSIÓN

- Según la Teoría de Shannon, las **dos técnicas básicas para ocultar la redundancia** en un texto en claro son la difusión y la confusión.
  - Estos conceptos, a pesar de su antigüedad, poseen una importancia clave en la Criptología moderna.
- **Difusión:** Transformación del texto en claro con objeto de **dispersar las propiedades estadísticas** del lenguaje sobre todo el criptograma.
- **Confusión:** Transformación del texto en claro con objeto de **mezclar sus elementos**, aumentando la complejidad de la dependencia entre clave y criptograma.