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.

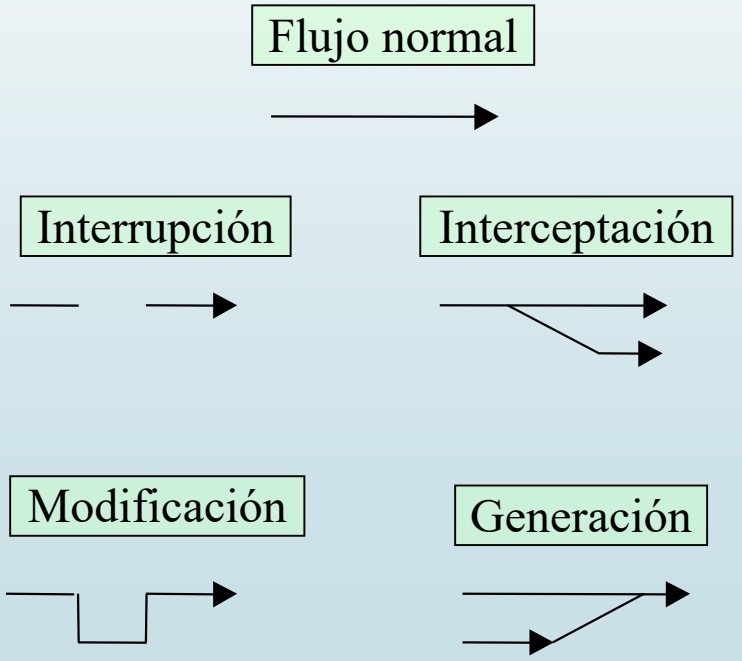
- Por software entendemos el conjunto de programas lógicos que hacen funcional al hardware, tanto sistemas operativos como aplicaciones.

- 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

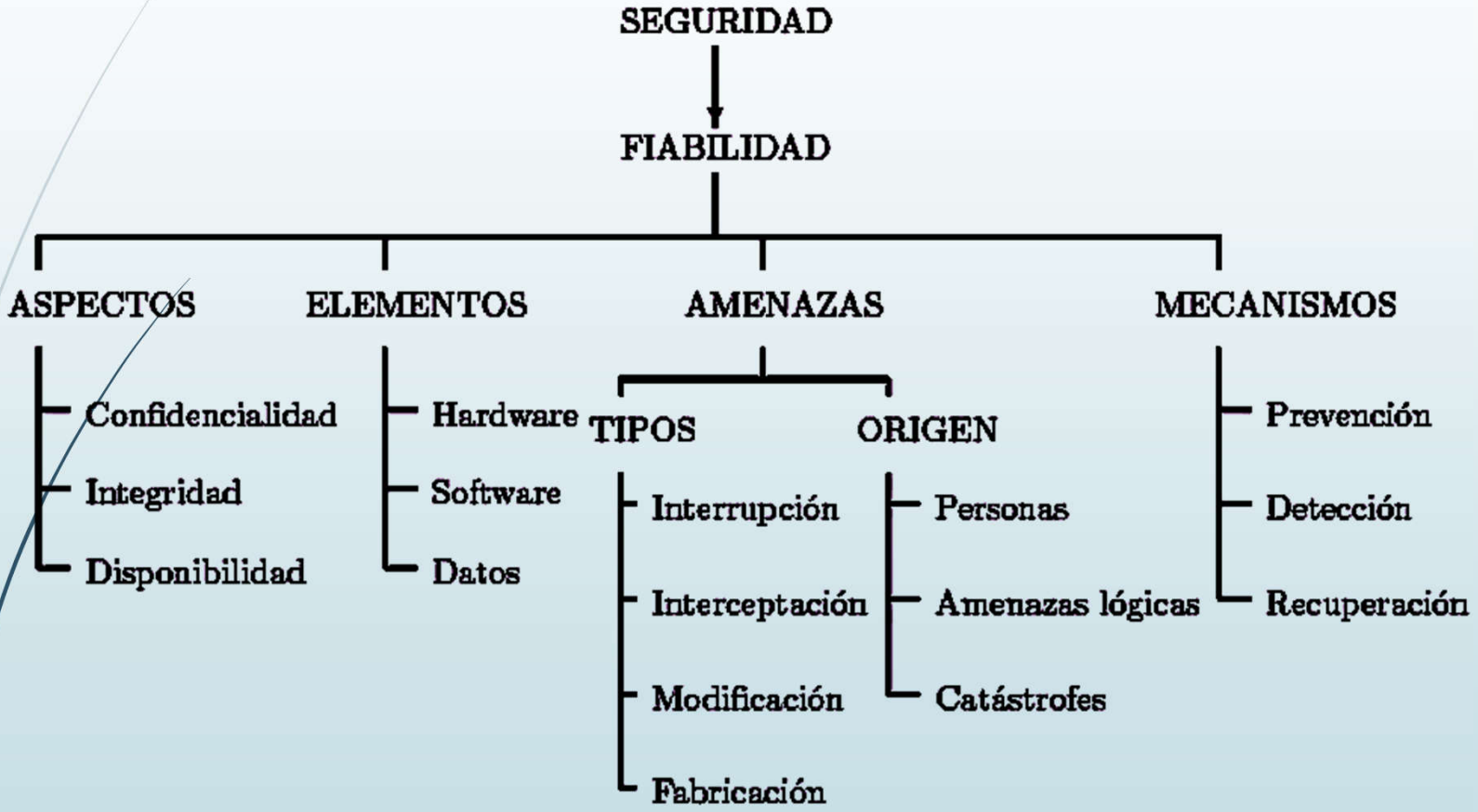
MECANISMOS DE SEGURIDAD EN LAS COMUNICACIONES

- **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

- El historiador griego Plutarco que vivió entre
describe la ***scitala espartana*** consist
preparaban dos ejemplare
persona que envi
mismo.

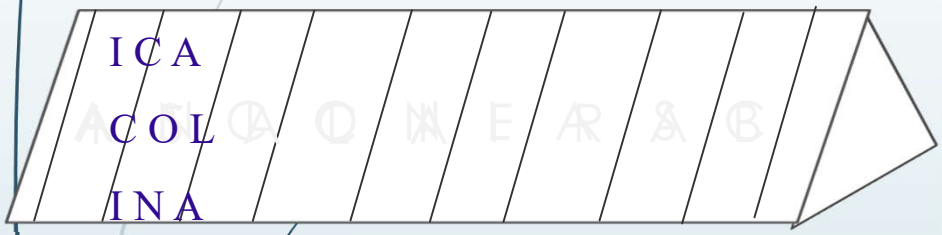
na tira
as letras en
. El mensaje no es
nino en la vara original

ecreta del que se tiene constancia
guerra entre Atenas y Esparta.

e cifrado las letras son cambiadas de posición.

1.2 Introducción histórica

SCÍTALA ESPARTANA



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

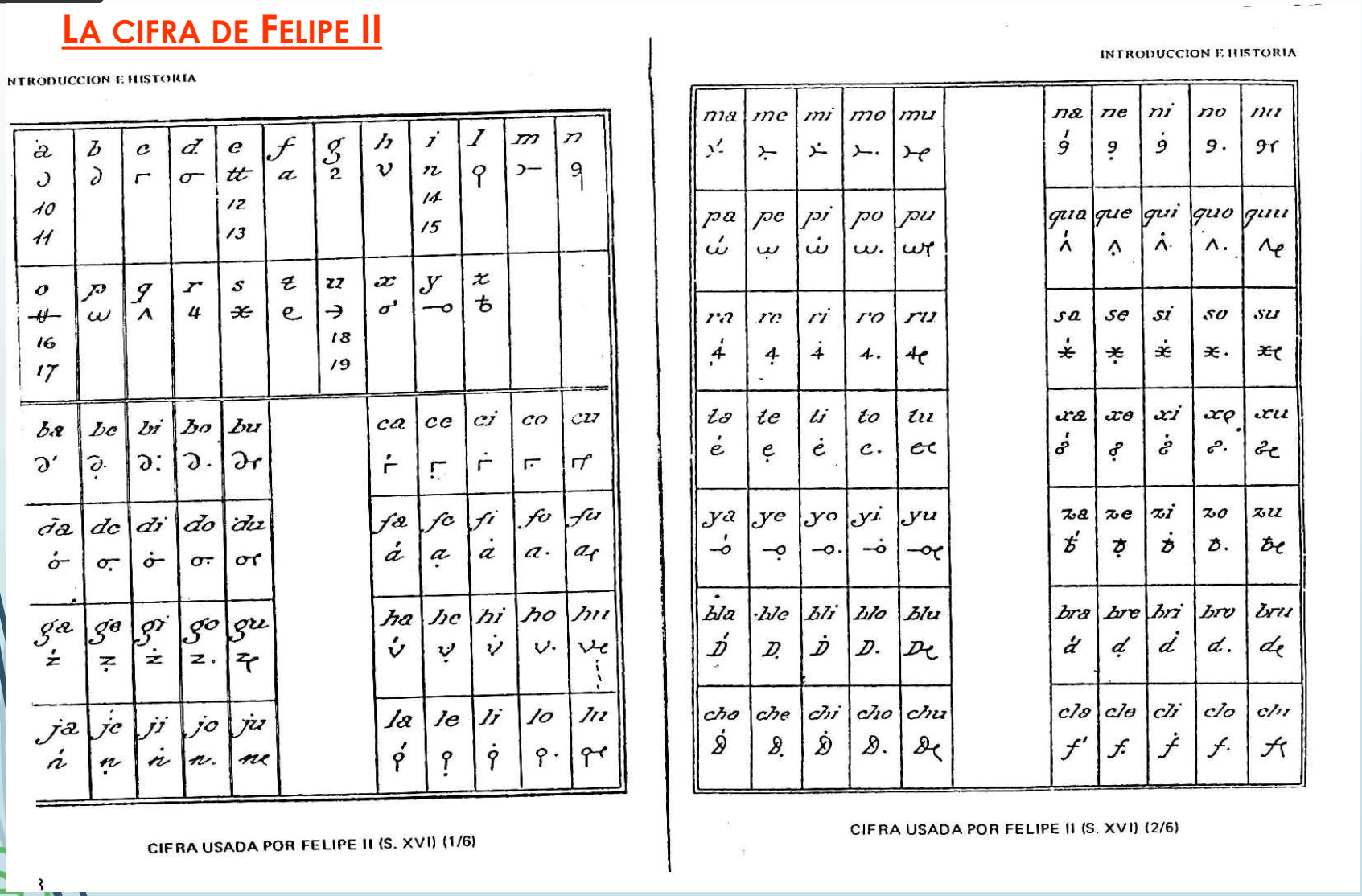
LA CIFRA DE FELIPE II

- 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



INTRODUCCION E HISTORIA

a ɔ 10 11	b ∂	c ⌐	d σ	e tt 12 13	f a	g 2	h v	i n 14 15	l ϙ	m ⊃—	n 9
o ⊕ 16 17	p ω	q ∧	r 4	s æ	t e	u → 18 19	x σ'	y —o	z ϐ		
ba ∂'	be ∂.	bi ∂:	bo ∂.	bu ∂r			ca ⌐	ce ⌐	ci ⌐	co ⌐	cu ⌐
da ȯ	de σ.	di ȯ	do σ.	du σr			fa á	fe a.	fi à	fo a.	fu ar
ga ż	ge ż	gi ż	go z.	gu zr			ha v̇	he v̇	hi v̇	ho v.	hu vr
ja ȧ	je ṇ	ji ȧ	jo n.	ju nr			la ϙ́	le ϙ	li ϙ̇	lo ϙ.	lu ϙr

CIFRA USADA POR FELIPE II (S. XVI) (1/6)

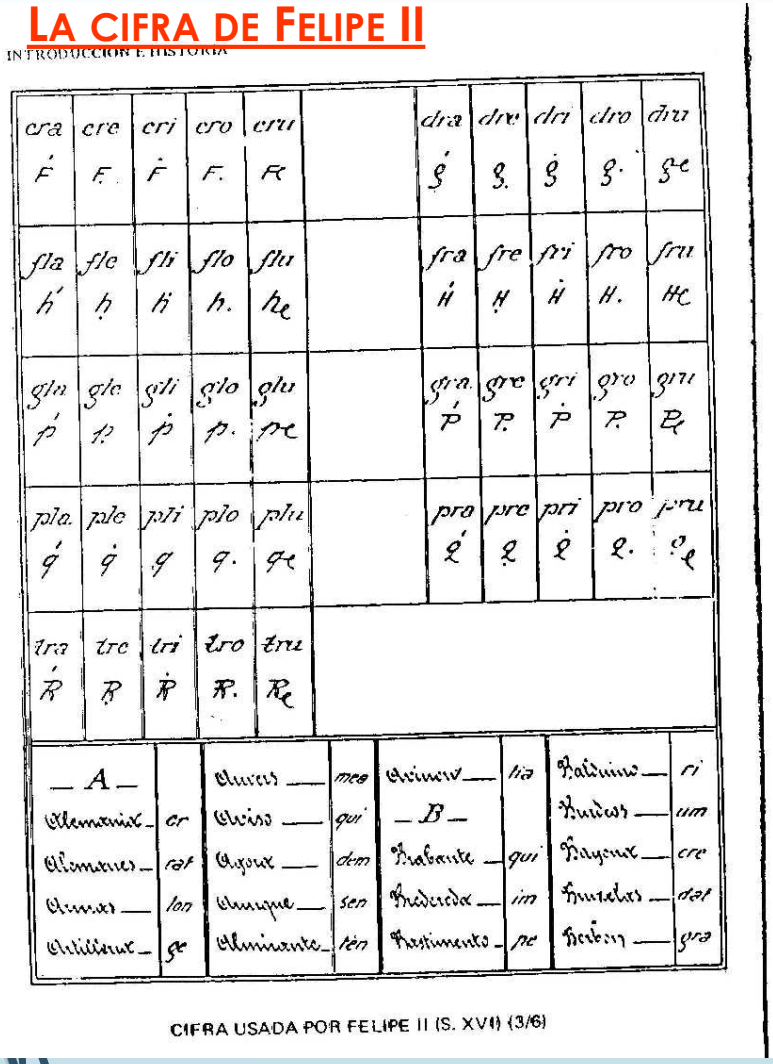
INTRODUCCION E HISTORIA

ma ɔ́	me ɔ	mi ɔ	mo ɔ.	mu ɔr			na 9́	ne 9	ni 9̇	no 9.	nu 9r
pa ώ	pe ω	pi ώ	po ω.	pu ωr			qua ∧́	que ∧	qui ∧̇	quo ∧.	quu ∧r
ra 4́	re 4	ri 4̇	ro 4.	ru 4r			sa ǽ	se æ	si æ̇	so æ.	su ær
ta é	te e	ti ė	to c.	tu er			xa σ́	xe σ	xi σ̇	xo σ.	xu σr
ya —ó	ye —o	yo —o.	yi —ȯ	yu —or			za ϐ́	ze ϐ	zi ϐ̇	zo ϐ.	zu ϐr
bla D́	ble D	bli Ḋ	blo D.	blu Dr			bra d́	bre d	bri ḋ	bro d.	bru dr
cha ∂́	che ∂	chi ∂̇	cho ∂.	chu ∂r			cla f́	cle f	cli ḟ	clo f.	clu fr

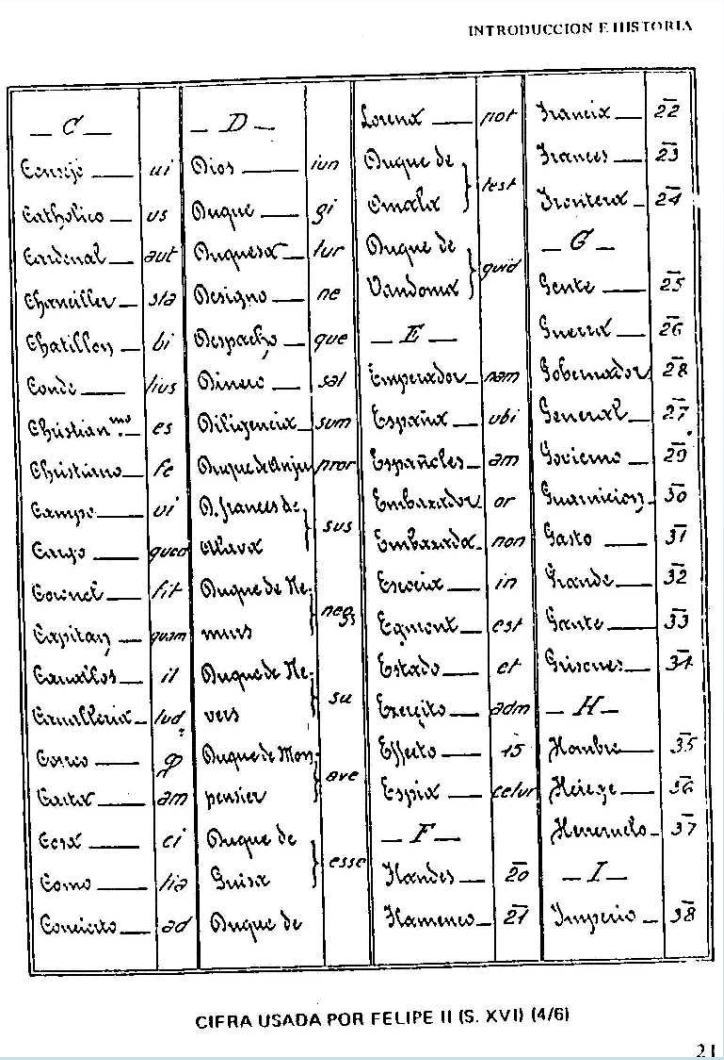
CIFRA USADA POR FELIPE II (S. XVI) (2/6)

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)