

	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
0:	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
1:	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
2:	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
3:	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
4:	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
5:	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
6:	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
7:	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
8:	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
9:	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

Figura 1.1: Cifrado de Gronsfeld

Contra este criptosistema no se puede usar ni el método de fuerza bruta ni el estudio de las frecuencias de las letras del texto, pues altera la frecuencia de una misma letra. La E se ha cifrado de varias formas distintas en el ejemplo anterior.[4]

Ejercicio 1.3.1 *¿Con cuántas claves tendríamos que analizar por fuerza bruta para descifrar un mensaje cifrado con este método? Si un ordenador tardara 1 seg en analizar cada clave, ¿sería factible analizarlas todas? ¿Serías recompensado con alguna medalla o te expulsarían de los servicios secretos?*

Ejercicio 1.3.2 *¿Porqué no podemos usar el análisis de frecuencias?.*

Ejercicio 1.3.3 *Con la tabla anterior cifrar el mensaje LOS EXAMENES HAN SIDO ROBADOS*

Ejercicio 1.3.4 *Construir una tabla y la clave para cifrar el mensaje EL PRISIONERO SERA TRASLADADO MAÑANA*

El método bívido comienza utilizando un alfabeto desordenado en un cuadrado 5×5 . Vamos a usar la clave DIPLOMA:

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

Al tener el alfabeto 26 letras y el cuadrado ser 5×5 nos vemos obligados a cifrar de la misma forma la I y la J. El contexto del mensaje nos permitirá distinguir cuál de las dos letras se quería cifrar. Para cifrar el texto claro se escriben los equivalentes numéricos de cada letra utilizando sus coordenadas en el cuadrado:

VEN A LAS TRES

tiene por equivalente numérico

51 25 35 22 14 22 43 44 42 25 43

y lo dividimos en dos partes

5 1 2 5 3 5 2 2 1 4 2
2 4 3 4 4 4 2 2 5 4 3

leemos los números por columnas en lugar de filas resultando

52 14 23 54 34 54 22 22 15 44 23

y consultando de nuevo en la tabla aparece el mensaje cifrado

WLBYKYAAOTB [5]

Ejercicio 1.3.5 *Cifrar, con la tabla anterior, el mensaje NECESITAMOS MAS PROVISIONES.*

Ejercicio 1.3.6 *Descifrar con la tabla anterior el mensaje IHAYIQO.*

Ejercicio 1.3.7 *Construir una tabla 5×5 para cifrado bífido inventándose la palabra clave y cifra el mensaje NECESITAMOS MAS PROVISIONES.*



Figura 1.2: La máquina enigma

1.4 La máquina enigma.

En el año 1923 el ingeniero alemán *Arthur Scherbius* patentó una máquina diseñada para facilitar las comunicaciones seguras. Era un instrumento parecido a una máquina de escribir, se escribía el mensaje y las letras correspondientes al mensaje cifrado se iban iluminando. Si se escribía el mensaje cifrado, el mensaje original aparecía de nuevo.

Esta máquina llamó la atención del Ejército Alemán, fue mejorada e incorporada al Ejército. Un tremendo error provocó que el servicio secreto polaco conociera la máquina. Se mandó, un viernes, por correo ordinario una máquina a la Embajada alemana en Varsovia y esta fue interceptada por los servicios secretos. Cuando los alemanes reclamaron en la oficina de correos el paquete, los polacos durante el fin de semana habían desarmado y analizado la máquina. La volvieron a armar y el lunes la devolvieron como si no hubiera pasado nada. Un equipo de tres matemáticos polacos construyó otra máquina, *Ciclómetro*, para descifrar los mensajes.

En 1938 Alemania varía la máquina complicando su funcionamiento y Polonia, por carecer de suficientes medios económicos, no podía afrontar la construcción de la descifradora. La invasión de Polonia era inminente y decidieron poner sus conocimientos a disposición de Francia y Gran Bretaña. Destruyeron todas las pruebas que permitieran descubrir a los alemanes que sabían el funcionamiento de ENIGMA y el equipo de matemáticos huyó hacia París donde empezaron a colaborar con siete expertos en Criptografía, españoles, exiliados republicanos liderados por un tal *Camazón*. Cuando Alemania invade Francia, los polacos huyen a España y los españoles a África donde se les pierde la pista. Los polacos llegan a Gran Bretaña y no se les considera seguros dándoles trabajos de poca importancia.

Alan Turing y *John von Neumann* llegaron, por aquel entonces, a fabri-

car máquinas descifradoras, La Bomba de Turing, aprovechando una debilidad del Ejército Alemán: siempre empezaban sus mensajes con las mismas palabras.

Para terminar decir que Alemania regaló al régimen de Franco una veintena de estas máquinas que se emplearon hasta los años cincuenta, para regocijo de los servicios secretos británico y norteamericano que siempre conocían nuestros mensajes.[6]

1.5 John von Neumann y Alan Turing



Figura 1.3: John von Neumann y Alan Turing

John von Neumann nació en Budapest (Hungría) en 1903. Su profesor de Matemáticas se dio cuenta de que John era un niño prodigio y recomendó a su padre que le proporcionara clases particulares de matemáticas por un profesor de universidad. De hecho, sin acabar el bachiller resolvía problemas planteados en la universidad. Ganó el premio al mejor alumno de secundaria en ciencias de Hungría.

En 1927 fue nombrado profesor de la Universidad de Berlín. Allí tenía fama de *bon vivant*, frecuentando los cabarés y la vida nocturna. En 1933, tras la llegada al poder de los nazis, es expulsado de la Universidad y huye a Princeton, USA.

Intervino en el diseño de los primeros ordenadores y fue el creador de la arquitectura de los ordenadores modernos y de la misma idea del software.

A partir de 1943 trabaja en el Proyecto Manhattan: diseño, desarrollo y construcción de la primera bomba atómica.

En 1954 es nombrado comisario de la Energía Atómica, el puesto más alto que un científico puede alcanzar en el gobierno de los USA.

En 1955 descubre que ha contraído cancer y el deterioro es imparable. Al final, él que era un judío ateo, buscó consuelo en la Iglesia Católica. Murió el 8 de Febrero de 1957.

Alan Turing nació en Inglaterra el 22 de Junio de 1912. Hijo de Julius, funcionario británico en la India, y de Ethel, inglesa también de la India. Después de nacer, sus padres vuelven a la India y Alan es criado por un matrimonio formado por un militar retirado y su mujer. Pronto llama la atención por asocial, ensimismado, desaliñado, indisciplinado, ocurrente y respondón.

Era un alumno atípico, muy malo en inglés y latín (la principal asignatura de la época), entregaba sus trabajos llenos de tachones y manchas. En cambio tenía gran facilidad para las matemáticas y la física.

Descubre su homosexualidad al ingresar en la Universidad de Cambridge, allí fue amante de James Atkins, otro gran matemático.

Trabajando en un problema de Hilbert, propuesto en el Congreso Mundial de Matemáticas de 1928, Alan Turing escribió su teoría sobre "las máquinas de Turing", idealización matemática de una computadora sin limitación de memoria ni tiempos de ejecución.

Conoce a Neumann en 1935 y este le ofrece una plaza en Princeton, USA, un trabajo bien remunerado y de mucho prestigio. Prefiere el ambiente bohemio de Cambridge y declina la oferta.

En 1939 acepta colaborar con el departamento británico de análisis criptográfico. Aplicando ideas lógicas y métodos estadísticos descifra los códigos de la marina alemana, por lo que recibe la Orden del Imperio Británico.

Era un consumado deportista, hasta el punto de ser seleccionado para correr la maratón olímpica en 1948, pero una lesión se lo impide.

El 7 de Febrero de 1952 fue arrestado acusado de indecencia por homosexual. El 31 de Marzo es juzgado y no reniega de su condición afirmando que no hay nada de malo en ello. Condenado a pena de cárcel, esta es conmutada por un tratamiento de inyecciones destinadas a dejarlo impotente, su forma física empeora sumiéndole en la frustración y rabia. Perseguido por la policía y obligado por el gobierno a dejar sus trabajos sobre criptografía, Alan Turing decidió que no valía la pena seguir viviendo. Se suicidó el 8 de Junio de 1954 tomando cianuro potásico, tenía 42 años.

En 1967 dejó de ser crimen la homosexualidad en Gran Bretaña.[1]

1.6 Consejos sobre las claves

Aquí tienes algunos consejos para proteger tus criptosistemas por si trabajas en los servicios secretos.

- Nunca hay que elegir como clave la fecha de nacimiento, el nombre de los hijos o la matrícula del coche.

- La clave debe ser memorizada y jamás escrita en un papel.
- Debe constar de por lo menos ocho caracteres. Si empleamos sólo seis distintos (números y letras) tendremos $37 \times 36 \times 35 \times 34 \times 33 \times 32 = 1.673.844.480$ posibilidades. Como hay programas de ordenador que prueban cuarenta mil claves por segundo, se tardarían $11^h 37^m 26^s$
- La clave, como no podemos escribirla, debe ser sencilla memorizarla.
- Debe ser modificada con frecuencia. Los servicios secretos enemigos seguro que descubrirán en algún momento nuestra clave por lo que conviene cambiarlas periódicamente.

Ejercicio 1.6.1 *¿Cómo hemos calculado las $11^h 37^m 26^s$?*

Ejercicio 1.6.2 *Leer del libro *Narraciones Extraordinarias* de Edgar Allan Poe el cuento *El Escarabajo de Oro**

1.7 Soluciones a los ejercicios del capítulo 1

Ejercicio 1.2.1

La tabla sería, después de correr siete posiciones el alfabeto, y no contar la ñ, pues somos unos anglófilos perdidos:

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

El mensaje se traduce como:

LS WHXBLAL SSLNHYH H SHZ VUJL KL SH UVJOL LU LS BSAPTV
AYLU

Ejercicio 1.2.2

En este caso $k=3$ por lo que la tabla de sustitución sería

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

y el mensaje descifrado es

AHORA HE CAMBIADO LA CLAVE

Ejercicio 1.2.4

La tabla de sustitución es

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

y el mensaje que se cifró:

AL QUE DESCIFRE ESTE MENSAJE LO INVITO EN LA CANTINA,
AHORA ME ENROLLO PARA FACILITAR EL DESCIFRADO Y QUE
SEA FACIL EL EJERCICIO

Ejercicio 1.3.1

Tendríamos que estudiar $27! \cdot 10! = 3.9514 \times 10^{34}$ (tiene 35 cifras) claves, como tarda 1 seg por cada una tendríamos $\frac{27! \cdot 10!}{6} =: 6.5856 \times 10^{33}$ seg, que pasados a horas son $\frac{6.5856 \times 10^{33}}{3600} = 1.8293 \times 10^{30}$ h, que traducidos a días son $\frac{1.8293 \times 10^{30}}{24} = 7.6221 \times 10^{28}$ d, y terminamos escribiendolo en siglos $\frac{7.6221 \times 10^{28}}{36500} = 2.0882 \times 10^{24}$, es decir, 2.088.200.000.000.000.000.000 siglos. No sólo te expulsarán de los servicios secretos, quizás también te fusilen por lento.

Ejercicio 1.3.2

Lo deja bien claro el ejemplo, la E se cifra de dos formas distintas.

Ejercicio 1.3.3

Si usamos la clave 1203456987, y despues de marearnos mirando semejante tabla, el mensaje cifrado sería:
OTU LINDGKXU MCU DVUQ OHEFFVD

Ejercicio 1.3.5

El equivalente numérico de cada letra es

N	E	C	E	S
35	25	24	25	43
I	T	A	M	O
12	44	22	21	15
S	M	A	S	P
43	21	22	43	13
R	O	V	I	S
42	15	51	12	43
I	O	N	E	S
12	15	35	25	43

dividiendo en dos partes quedan $3525242543124422211543212$ y leyéndolos por columnas $2431342155112431215352543$

32	54	23	51	23
G	Y	B	V	B
44	22	51	45	35
T	A	V	U	N
11	21	42	44	23
D	M	R	T	B
21	22	11	15	53
M	A	D	O	X
45	32	25	14	23
U	G	E	L	B

con lo que se cifraría como:
GYBVBTAVUNDMRTBMADOXUGELB

Ejercicio 1.3.6

El equivalente numérico es 12 33 22 54 12 41 15, los escribimos en columnas $\begin{matrix} 1 & 3 & 2 & 5 & 1 & 4 & 1 \\ 2 & 3 & 2 & 4 & 2 & 1 & 5 \end{matrix}$ y quedan las parejas 13 25 14 12 32 42 15 que corresponden a PELIGRO.

Ejercicio 1.6.1

Dividiendo las posibilidades por 40.000 y pasando a horas, minutos y segundos:

$$\frac{37 \times 36 \times 35 \times 34 \times 33 \times 32}{3600 \times 40000} = 11.624h = 11^h 37^m 26^s$$

