

**Ejercicio 1.** Se recibe el siguiente criptograma:

**JGAZN** WINHY LZDYV BBJLC QHTNK UDQXM OXJNO ZMUSP NONYJ MTEJH QHQFO  
 OPUPB CYAÑJ ONCNN QHNMO NDHKU TJMQC MOPNF AOXNT NLOAZ MJDQY MOZCJ  
 RNBAO QTUIE NFAIX TLXJG AZMJA XJVAZ MUDNM YLNLJ MUMUY HVUMH TÑIGD  
 XDQUC LSJPI BCUSF NUGXX GEEXK AEJME SJÑEN ASLHL BAEYJ ROJXA CQTCN  
 MYPUC UNMJW OYNHZ NKUOG AJDUJ XENRY TENJS CNMON TYJNM JYFXF IGJMI  
 BUUSN TFAPN FAFKU ROJNY CTUYN BYSGJ VACAU CGQWA ZMJJH JHSNT PAPXM  
 GNECO GJUTE NCNGJ GEGAJ SPNUL GDMAÑ JDOFD NPUNN PNTGE NMJSN TTOFD  
 KIOXS SQNNF BATOC XMMNV ÑEZNM EZBOS NTUSQ BUDBT JRBBU YPQZI OQFTB  
 ANIBV MEDDY RUMUP NAULB OMAED HVHNF OCJOS NMJ.

Ayuda: Aparecen 4 cadenas de 4 caracteres que se repiten en el criptograma: JGAZ, NMON, PNFA y AZMJ.

Al romper el criptograma en cuatro subcriptogramas (C1, C2, C3, C4) se contabilizan las siguientes frecuencias de caracteres en cada uno de ellos:

	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
C1	7	5	6	8	1	0	0	1	0	21	3	3	12	17	0	1	1	6	1	0	11	2	3	0	9	2	0
C2	1	1	3	1	0	8	5	6	0	15	2	0	14	8	3	5	2	0	0	2	4	22	2	3	3	9	1
C3	18	0	2	6	9	1	2	0	9	2	1	8	4	4	0	15	5	2	5	12	6	0	2	0	0	5	1
C4	0	10	8	1	8	5	9	7	1	0	0	0	1	24	2	6	6	7	0	2	0	6	0	0	4	2	10

Si se conoce que ha sido cifrado mediante el algoritmo de Vigenère, se pide:

- Comprobar con el Método de Kasiski la longitud de la clave.
- Encontrar la clave del sistema y descifrar sólo los diez primeros caracteres.

**Solución:**

Las cadenas presentan las siguientes separaciones en el criptograma:

JGAZ 128 caracteres                      NMON 184 caracteres  
 PNFA 196 caracteres                      AZMJ 32 y 184 caracteres

- El  $mcd(128,196,184,32) = 4$ . Se comprueba que la longitud de la clave es 4.
- Aplicando la Regla AEO de separación de letras en los criptogramas, encontramos finalmente las

**CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE  
 LLAMA O ENVÍA WHATSAPP: 689 45 44 70**

---

**ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
 CALL OR WHATSAPP:689 45 44 70**





Fundamentos de Seguridad  
Cifrado por sustitución  
Propuestos y Resueltos



	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
C1	7	5	6	8	1	0	0	1	0	21	3	3	12	17	0	1	1	6	1	0	11	2	3	0	9	2	0
C2	1	1	3	1	0	8	5	6	0	15	2	0	14	8	3	5	2	0	0	2	4	22	2	3	3	9	1
C3	18	0	2	6	9	1	2	0	9	2	1	8	4	4	0	15	5	2	5	12	6	0	2	0	0	5	1
C4	0	10	8	1	8	5	9	7	1	0	0	0	1	24	2	6	6	7	0	2	0	6	0	0	4	2	10

C1: AEO JNX; C2: AEO UYJ;  
C3: AEO AEO; C4: AEO NQB

Luego la clave es K = JUAN

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

J	G	A	Z	N	W	I	N	H	Y	L
J	U	A	N	J	U	A	N	J	U	A
9-9	6-21	0-0	26-13	13-9	23-21	8-0	13-13	7-9	25-21	10-0
0	12	0	13	4	2	8	0	25	4	10
A	m	A	N	E	C	I	A	y	E	L

M = AMANE CIAYE L nuevo sol pintaba de oro las ondas de un mar tranquilo. Chapoteaba un pesquero a un kilómetro de la costa cuando... (párrafo de Juan Salvador Gaviota)

**Ejercicio 2.** Se recibe el siguiente criptograma cifrado mediante el método de *Vigenère*:

NSZEF UAEIR BXJNO ATOYX EXDZA CNRBE KVQVE ZOKIX NQHIV RQBEZ ADOEJ RNSZE  
FUAEI RTNVC NLZEZ CELFJ INZUQ SZTQT AÑESE FMEFE XUEXT QVRAY JTNRM NPXSG  
RVSHV PMSZT BYAXA ETQUA EIRUZ MOFTJ EFDNC AKIGX PNTJA FDNPO KTENS HNHF  
QTBPR LNVTQ MRRUJ UZDGS GAUFU EPNBI GOHAG AAF



**CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE**  
**LLAMA O ENVÍA WHATSAPP: 689 45 44 70**

---

**ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS**  
**CALL OR WHATSAPP:689 45 44 70**



b) Descifre los 2 primeros bloques (10 caracteres) del criptograma según la clave encontrada en el punto anterior.

**Solución:**

a) Encontramos entre otras la cadena UAEIR en la posición 6, luego se repite en la posición 62, separados  $(62-6) = 56$  caracteres. Por último, se vuelve a repetir en la posición 139, con una separación de  $(139-62) = 77$ . Calculamos el máximo común divisor entre estos valores obteniendo  $\text{mcd}(56,77) = 7$ .

A lo mismo se llega eligiendo la cadena de tres caracteres iniciales NSZ que aparece luego en la posición 57, separadas entonces  $(57-1) = 56$  caracteres y que vuelve a repetirse en la posición 127, separada ahora  $(127-57) = 70$  caracteres, con lo que  $\text{mcd}(56,70) = 14$ . El resultado de las dos cadenas es 7. No obstante, es más fiable la primera solución con la cadena de 5 caracteres por ser más larga.

Como la única clave con longitud 7 es la  $a_5$ , la clave podría ser NARANJA, lo que se comprueba descifrando el comienzo del criptograma en busca de un mensaje inteligible.

b) Utilizando bien aritmética modular mod 27 o la tabla de Vigenère, se obtiene el siguiente texto escrito en minúsculas en el que se ha incluido puntuación:

M = **ASÍ ES MARÍA**, blanca como el día,  
pero es veneno si le quieres enamorar.  
Así es María, tan caliente y fría,  
que si te la bebes de seguro te va a matar.  
Un dos tres, un pasito p' delante María,  
un dos tres, un pasito p' atrás.  
Un dos tres, un pasito p' delante María,  
un dos tres, un pasito p' atrás.

**Ejercicio 3** Se sospecha que el siguiente criptograma ha sido cifrado con un sistema de cifra clásica elemental muy conocido. Algunos n-gramas repetidos en el criptograma se muestran subrayados o en negrita. ¿De qué sistema estamos posiblemente hablando? ¿Cuál de estas cinco claves habrá cifrado el mensaje M?  $K_1 = \text{CARMELE}$ ,  $K_2 = \text{MARIA}$ ,  $K_3 = \text{BEGOÑA}$ ,  $K_4 = \text{JOAQUIN}$ ,  $K_5 = \text{PEDRO}$ ? Justifique su respuesta. Descifre sólo los 9 primeros elementos del criptograma.

HSSFL CQHDP QMIZX OGFVP NAQOD ZSBAS SQGIE QOPQM IZXOS UXPNA **ZASJU**  
YQONK JSBOW ATYAN KONQN NEQOS OUSOX PAJPI OQOSG UZNVD CFGXE JGLQW  
WZKWS LÑMEQ ONYNM ENZFO HBBLV EHOMI JSNIJ TQAWA **SJUXJ** QOVMI PQODU  
FANVI OIYXE XQHUÑ IZCDL QLCQA WAHOM GJGDU YUNYG EDXME JDLMC LNAZA

**CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE  
LLAMA O ENVÍA WHATSAPP: 689 45 44 70**

---

**ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP:689 45 44 70**

