

RTOJXRVIHSIXL**MYM**CVKCLYTHJBLHFFCYJKPXZVZIIVOBTKUBICM**Y****P****G**TM**ZOX**ZZOUO**VVZ**PHE**BNL**  
R**Y****IBL**TKWTJXSMKUVRTLWZVYLIRZGIEVITKARDKIX**VVZOXJCH**QXTBUMGLUKYHLAJPOFZILLKZGC  
XCAG**UW**KWXT**XEBY****P****G****K**LGJCOUZPMGYLF**BNL**KTPGYTTBKYL**YIBL**CFQLTW**KPK**PKTZEWMFOXHI  
YQIMTDQR**FMYM**XLLVD**ZOX**GIYZBMM**GUWJCH**TBJAOCXV**IBLL**UZUWIVZ**SHE**CWX**FMYM****SHE**ZKOV  
NJIZATTSKYTELZY**XEB**ZYNJBKKUPIRSCLAZAHEISLTWMC

Paso 1. Cadenas de letras repetidas

**MYM** 215, 265

**ZOX** 60, 180

**IBL** 120, 185

**KPK** 40, 42

**YPG** 110

**VVZ** 50

**BNL** 110

**YIB** 120

**JCH** 130

**GUW** 95

**XEB** 145

**FMY** 50

**SHE** 10

Paso 2. Posible longitud clave

**MCD(215, 265, 60, 180, 120, 185, 40, 110, 50, 130, 95, 145, 50, 10) = 5**

Paso 3. Frecuencia en subcriptogramas

Separar de 5 en 5

Alfabeto ingles: 26 caracteres

RTOJX RVJIH SIXLM YMCVK CLYTH JBLHF FCYJK PXZVZ IIOB TKUBI CMYPG TMZOX ZZOUO  
VVZPH EBNLR YIBLT KWTJX SMKUV RTRLW ZVYLI RZGIE VITKA RDKIX VVZOX JCHQX TBUMG  
LUKYH LAJPO FZILL KZGCX CAGUW KWXTX EBYPG KPKLG JCOUZ PMGYL FBNLK TPGYT TBKYL  
YIBLC FQTLW KPKPK TZEWM FOXHI YQIMT DQRFM YMXLL VDZOX GIYZB MMGUW JCHTB JAOCX  
VIBLL UZUWI VZSHE CWXFM YMSHE ZKOVN JIZAT TSKYT ELZYX EBZYN JBKKU PIRSC LAZAH EISLT  
WMC

Concatenamos todos los caracteres de posición 1, los 2 con los 2, los 3 con los 3, los 4 con los 4  
y los 5 con los 5:

(1, 'RRSYCJFPITCTZVEYKSRZRVRVJTLLFKCKEKJPFTTYFKTFYDYVGMJJVUVCYZJTTEEJPLEW')  
(2, 'TVIMLBCXIKMMZVBIWMTVZIDVCBUAZZAWBPCMBPBIPZQOQMDIMCAIZZWMKISLBBIAM')  
(3, 'OJXCYLZYVUYZONBTKRYGKZHUJIGGXYKOGNGKBTKEKXIRXZYGHOBUSXS0ZKZZKRZSC')  
(4, 'JILVTHJV0BPOUPLJULLIKIOQMYPLCUTPLUYLYLLPWHMFLOZUTCLWHFHVAYYYKSAL')  
(5, 'XMHKHFCKZBIGX0HRTXVWIEAXXXGHOLXWXGGZLKTLCWKMITMLXBWBXLIEMENTTXNUCHT')

#### 4. Obtenemos las frecuencias mas altas de cada subcriptograma

```

1
Counter({'J': 7, 'T': 7, 'V': 6, 'Y': 6, 'E': 5, 'F': 5, 'K': 5, 'R': 5,
'C': 4, 'L': 3, 'P': 3, 'Z': 3, 'S': 2, 'D': 1, 'G': 1, 'I': 1, 'M': 1,
'U': 1, 'W': 1})

2
Counter({'I': 10, 'M': 9, 'B': 8, 'Z': 7, 'A': 4, 'C': 4, 'V': 4, 'Q': 3,
'P': 3, 'W': 3, 'D': 2, 'K': 2, 'L': 2, 'T': 2, 'O': 1, 'S': 1, 'U': 1,
'X': 1})

3
Counter({'Z': 9, 'K': 8, 'G': 6, 'Y': 6, 'O': 5, 'X': 5, 'B': 3, 'S': 3,
'R': 3, 'U': 3, 'T': 3, 'C': 2, 'I': 2, 'H': 2, 'J': 2, 'N': 2, 'E': 1,
'L': 1, 'V': 1})

4
Counter({'L': 13, 'Y': 7, 'P': 5, 'U': 5, 'H': 4, 'O': 4, 'I': 3, 'J': 3,
'T': 3, 'V': 3, 'A': 2, 'C': 2, 'F': 2, 'K': 2, 'M': 2, 'W': 2, 'B': 1,
'Q': 1, 'S': 1, 'Z': 1})

5
Counter({'X': 11, 'T': 6, 'H': 5, 'L': 5, 'G': 4, 'I': 4, 'K': 4, 'M': 4,
'W': 4, 'B': 3, 'E': 3, 'C': 2, 'O': 2, 'N': 2, 'Z': 2, 'A': 1, 'F': 1,
'R': 1, 'U': 1, 'V': 1})

```

Lo anterior nos da una pista de donde pueden estar las letras “a” y “e”, aplicar regla

0	1	2	3	4	5	6	7	8	9	1	1	1	1	1	1	1	1	1	1	2	2	22	2	2	2	2
										0	1	2	3	4	5	6	7	8	9	0	1		3	4	5	6
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

- Buscamos en cada subcriptograma  $C_i$  las cuatro letras con una alta frecuencia y que cumplan, **ADEMÁS**, con una distribución en posiciones relativas separadas igual que las letras A, E, O y S, las cuatro letras más frecuentes del lenguaje mod 27

$$A + 4 = 0 + 4 = 4 = E$$

$$E + 11 = 4 + 11 = 15 = O$$

$$O + 4 = 15 + 4 = 19 = S$$

- Intentamos buscar cómo se ha cifrado la letra A (código 0) del texto en claro
- Donde esté esa posición relativa de la A, nos marcará la letra de la clave

Etao -> ingles

Aplicar regla de kasisiki en cada subcriptograma (ETA0 -> 4,10,5)(inshrd)

	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
#	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
1			4	1	5	5	1		1	7	5	3	1			3		5	2	7	1	6	1		6	3
2	4	8	4	2					10		2	2	9		1	3	3		1	2	1	4	3	1		7
3		3	2		1		6	2	2	2	8	1		2	5			3	3	3	3	1			6	9
4	2	1	2			2		4	3	3	2	13	2		4	5	1		1	3	5	3	2		7	1
5	1	3	2		3	1	4	5	4		4	5	4	2	2			1		6	1	1	4	11		2

Posible clave: R I G H T

Prueba y error con la llave encontrada:

ALICEANDBOBARETHEWORLDSMOSTFAMOUSCRYPTOGRAPHICCOUNPLESINCETHEIRINVENTIONTHEYHVE  
EATONCEBEENCALLEDINSEPARABLEANDHAVEBEENTHESUBJECTOFNUMEROUSDIVORCESTRVELSANDT  
ORMENTSINTEENSUINGYEARSOOTHERCHARACTERSHAVEJOINEDTHEIRCRYPTOGRAPHICFAMILYTHERESE  
VTHEPASSIVEANDSUBMISSIVEEAVESDROPPERMALLORYTHEMALICIOUSATTACKERANDTRENTTRUSTEDBY  
ALLJUSTTONAMEAFEW

ALICE Y BOB SON LAS PAREJAS CRIPTOGRÁFICAS MÁS FAMOSAS DEL MUNDO DESDE SU INVENCION, SE  
HAN LLAMADO UNA GRAN CANTIDAD INSEPARABLES Y HAN SIDO SUJETO DE NUMEROSOS DIVORCIOS,  
VIAJES Y TORMENTOS EN EL AÑO CONSECUTIVO. EL MALICIOSO ATACANTE Y ALQUILO CONFIAN EN  
TODOS SOLO PARA NOMBRAR UNOS POCOS

Kakashi test: <https://www.boxentriq.com/code-breaking/vigenere-cipher>