

SEGURIDAD Y PROTECCIÓN DE SISTEMAS INFORMÁTICOS

---

# ATAQUES SOBRE MÉTODOS POLIALFABÉTICOS USANDO EL MÉTODO DE KASISKI Y EL ÍNDICE DE COINCIDENCIA

Antonio Miguel Pozo Cámara

Javier Bolívar Valverde

---

MUCHOS AÑOS DESPUÉS, FRENTE AL PELOTÓN DE FUSILAMIENTO, EL CORONEL AURELIANO BUENDÍA HABÍA DE RECORDAR AQUELLA TARDE REMOTA EN QUE SU PADRE LO LLEVÓ A CONOCER EL HIELO. MACONDÓ ERA ENTonces UNA ALDEA DE 20 CASAS DE BARRO Y CAÑABRAVA CONSTRUIDAS A LA ORILLA DE UN RÍO DE AGUAS DIÁFANAS QUE SE PRECIPITABAN POR UN LECHO DE PIEDRAS PULIDAS, BLANCAS Y ENORMES COMO HUEVOS PREHISTÓRICOS. EL MUNDO ERA TAN RECIENTE, QUE MUCAHS COSAS CARECÍAN DE NOMBRE, Y PARA MENCIONARLAS HABÍA QUE SEÑALARLAS CON EL DEDO.

Texto plano

Muchos años después, frente al pelotón de fusilamiento, el coronel Aureliano Buendía había de recordar aquella tarde remota en que su padre lo llevó a conocer el hielo. Macondo era entonces una aldea de 20 casas de barro y cañabrava construidas a la orilla de un río de aguas diáfanas que se precipitaban por un lecho de piedras pulidas, blancas y enormes como huevos prehistóricos. El mundo era tan reciente, que muchas cosas carecían de nombre, y para mencionarlas había que señalarlas con el dedo.

C1= MOOSSNLODSMTCNUIBDADCAUADMEEALECCLLCOENULDCSAYAVNUSOLUOGDAQECTNUCEDPDLANEMEPIRSUEACTEHOCCDMYACASIEALOD  
C2= USSPFTPTEIIOERAUIBEORETEONSDOVOEHOONCNDEADRCBASIARANDUINUPIAPNHPRUAAOSOVRSIENRNIEMASAIEBPMIRHASLANRCLO  
C3= CADUREEOFLEERLENEAIRRALARTQURLONRIMNRTAE2SERARCTDLIDREAAAERPBOLOIALSNYRCHOETCLDAREQU SARANRAEOLAQEASED  
C4= HNEEEALNUANLOALONHAEDQLREAUPELAOEADAOSAA0ABONAORAALIASFSSEIAREDESIBCEMOUSHOOMOTENUCCSENOERNNAUNRCLO

C1= MOOSSNLODSMTNCUIBDADCAUADM**E**EALECCLLCOENULDCSAYAVNUSOLUOGDAQECTNUCEDPDLAN**E**MEPIRSUEACTEHOCCDMYACASI**E**ALOD  
C2= USSPFTPT**E**IIOOERAUIBEORETEONSDOVOEHOOENCNDE**A**DRCBASIA**R**ANDUINUPIAPNHPRUA**S**OSOVRSIENRNIEM**M**ASA**I**EBPMIRHASL**A**NRCLO  
C3= CADUREEOFLEERLENE**A**IRR**R**ALARTQURLONRIMNRTE**A**E2SER**R**CTDLIDRE**AAA**ERPBOLOI**A**LSNYRCHOETCLDAREQU**S**ARANRAEOL**A**QEASED  
C4= H**N****EE**ALNUANLOALONHAEDQLREAUP**E**LA**O****E**ADAOSAA**0**ABONAOR**A**ALE**I**ASF**S**SE**I**ARE**D**ESIBCEMOUSHOMOTENUCCS**E**NOERNNN**A**BUNRCLO

Letras con mayor frecuencia en C1 C2 C3 y C4

E: 10.78 %

A: 11.43 %

A: 15.84 %

A: 16.67 %

E: 15.68 %

Letras con mayor frecuencia en el texto original

A: 14.04 %

E: 13.55 %



**¿Cuánto texto es necesario para que funcione  
el método de ataque de Kasiski?**



**3 veces el tamaño del alfabeto utilizado**

VOPVC FRTCU MBGHG KGSCT YKTNJ MP**KIB** **VGYQE**  
YSSRK YYEEJ GWGVQ RGPST LNDIF VIOMM **TGGYU**  
**SLGZN** CZCJE YGGSJ **VGJIJ** DSLRV ARWCY ECOTP  
**VWYUS** CEIQL SQLIP DMLGW RJEQJ IAZFG **JIJ**RO  
RRILV OFGWÑ ZXCY QHWYE NN**KIB** **VPYUV** GUHNE  
HCVWR RFYZQ EJIQR HNLVY KWSW**V** **GJYLR** GAZHC  
EXCUY PRQRV YLNMY AIBVG YTIPZ **ECEFN** LWSRQ  
YIYCC IÑJST **GGNMQ** YWVYT XSJ**EC** **E**OYTE BVVY

$$\text{KIB} = 135 \quad \text{YUS} = 39$$

$$\text{GJIJ} = 48 \quad \text{VGJ} = 114$$

$$\text{mcd}(135, 48, 189, 39, 114, 33) = 3$$

$$\text{TGG} = 189 \quad \text{ECE} = 33$$

$$\text{mcd}(135, 48, 189, 39, 114, 33) = 3 \longrightarrow L=3$$

sol  
pez  
rey ?

ZZEDB	QPIRD	MCIYS	ÑKEKO	ÑWOXS	ICQKD	OMIVZ	VKSAG	DMQCS	YMOOD
GNSHV	VKMJD	XOIVI	VGGDO	OZSMW	VAUDS	IWGXU	DIYVE	ZHIVZ	KATAW
HMVXH	XCEAS	IBEMW	VALJP	DIXNB	DLSLD	IAMOD	VCQUJ	XOELV	KXIAD
YMWYJ	ZAHNQ	PIVNB	OIHQO	ÑAMVV	VJIAE	ZAGJR	KSSBE	VLVNH	YMOUJ
XOELV	KSIPO	WPEVR	DKLXF	PMITK	DMNXS	ÑBEKO	YMJQB	DBMEO	TZIUC
OIHJA	ZUXNH	VSEXZ	KKYJZ	ZZETO	LMSAT	KZPJR	ZSEUO	GIWDS	NBIHE
KZSAR	ZUHNH	PATJR	NMWNZ	HCGPO	XOSPO	WPEBO	GPHXS	IWXAD	WWXNF
PMGXU	DWXAS	ÑJYNB	KATNQ	ZAOJE	NPPNG	VAIUE	IIIIVI	NPWCS	XPEJZ
HCGPO	XOSES	NIOEW	ZQSAS	BZIBO	NBSMD	ÑSSBR	DIWLD	IAYKD	OMZJQ
DWCBW	ZTTAS	WINJP	VIEHJ	YIVTS	VKEAU	VZOXH	NWOTD	ÑLIBS	YIOXS
GJMLV	ZZSHS	GIVYD	IGOJK	ZSEJG	NWOTO	YIETA	VAXQZ	GIZNZ	VMWCO
WIVNA	ZUHJR	VKSvh	VKSBR	ZOEAW	IICJG	NWOTO	YITJG	ZKMJJ	IIFJB
YMVJS	IXIAA	VUIVI	ZLIAG	KBE					

C1: ZQMÑÑIOVDYGVXVOVIDZKHXIVDDIVXKYZPOÑVZKYYXWDYPDÑ  
YDŁOZVKZLKZGNKZPNHXWGIWPÐNKZNVINXHXNZBNNDIODZWVYV  
VNNYGZGIZNYVGWZVVZINYZIYIVZK

C2: ZPCKWCMKMMNKOZAWIHAMCBAILACOXMAIIAJASLMOSPKMM  
BMBZIUSKZMZSIBZUAMCOPPWWMJAAPAIPPCOIQZBSIAMWTIIIKZ  
WLIJZIGSWIAIMIUKKOIWIKIMXULB

C3: EIIEOQISQOSMIGSUGYITVEELXSMQEIWHVHMIGSVOEIELINEJMIHX  
EYESPEWISHTWGSEHXXGXYTOPIIWEGSOSISSWYZCTNEVEOOIOMSVOE  
OEXZWVHSSECOTMFVIIIE

C4: DRYKXXVACOHJVDMDXVVAXAMJNLOULAYNNQVAJBNULPVXTXKQ  
EUJNXJTAJUDHANJNPPBXANXANNJNUVCJPEEABMBLKJBAJHTAXBXL  
HYJJTTQNCNJVB AJTJJJAVA

C5: BDSOSDZGSDVDIOWSUEZWHSPBDDJVDJQBOVEREHJVORFKSOBO  
OAHZZOTROSERHRZOOOSDFUSBQEGOISZOSWSODRDDQWSPJSUHDSS  
VSDKGOAZZOARHRWGOGJBSAIG

C1: ZQMÑÑIOVDYGVXVOVIDZKHXIVDDIVXKYZPOÑVZKYYXWDPDÑ  
YDŁOZVKZLKZGNKZPNHXWGIWPÐNKZNVINXHZNZBNNDIODZWVYV  
VNNGZGIZNYVGWZVVZINYZIYIVZK

11 veces I    18 veces V    17 veces Z

C2: ZPCKWCMKMMNKOZAWIHAMCBAILACOXMAIIAJASLMOSPKMM  
BMBZIUSKZMzsIBZUAMCOPPWWMWJAAPAIPPCOIQZBSIAMWTIIIKZ  
WLIJZIGSWIAIMIUKKOIWIKIMXULB

13 veces A    20 veces I    15 veces M

C3: EIIEOQISQOSMIGSUGYITVEELXSMQEIHVHMIIGSVOEIELINEJMIHX  
EYESPEWISHTWGSEHXXGXYTOPIIWEGSOSISSWYZCTNEVEOOIOMSVOE  
OEXZWVHSSECOTMFVIIIE

19 veces E    18 veces I    15 veces S

C4: DRYKXXKVACOHJVMDXVVAXAMJNLOULAYNNQVAJBNULPVXTXKQ  
EUJNXJTAJUDHANJNPPBXANXANNJNUVCJPEEABMBLKJBAJHTAXBXL  
HYJJTTQNCNJVBAJTJJJAVA

15 veces A    19 veces J    13 veces N

C5: BDSOSDZGSDVDIOWSUEZWHSWPBDDJVDJQBOVEREHJVORFKSOBO  
OAHZZOTROSERHRZOOOSDFUSBQEGOISZOSWSODRDDQWSPJSUHDSS  
VSDKGOAZZOARHRWGOGJBSAIG

13 veces D    18 veces O    18 veces S

[MBP-de-Antonio:SPSI repo trabajo Apozo\$ python kasiskiAttack.py

Introducir el texto cifrado:

PPQCAXQVEKGYBNKMAZUYBNGBALJONITSZMJYIMVRAGVOHTVRAUCTKSGDDWUOXITLAZUVAVVRAZCVKBQPIWPOU

YBN 8

AZU 48

VRA 8

VRA 24

Possible longitud de la clave = 8

cadena[0]== PEAAZAADAA

cadena[1]== PKZLMGUWZZ

cadena[2]== QGUJJVCUUC

cadena[3]== CYYOYOTOWV

cadena[4]== ABBNIHKXAK

cadena[5]== XNNIMTSIVB

cadena[6]== QKGTVVGTQ

cadena[7]== VMBSRRDLRP

1º caracter mas repetido de cadena[0] = A -> 6 veces

2º caracter mas repetido de cadena[0] = D -> 1 veces

3º caracter mas repetido de cadena[0] = E -> 1 veces

Indice de coincidencia de cadena[0] 0.333 (0.333333333333)

1º caracter mas repetido de cadena[1] = Z -> 3 veces

2º caracter mas repetido de cadena[1] = K -> 1 veces

3º caracter mas repetido de cadena[1] = L -> 1 veces

Indice de coincidencia de cadena[1] 0.067 (0.0666666666667)

1º caracter mas repetido de cadena[2] = U -> 3 veces

2º caracter mas repetido de cadena[2] = J -> 2 veces

3º caracter mas repetido de cadena[2] = G -> 1 veces

Indice de coincidencia de cadena[2] 0.111 (0.111111111111)

1º caracter mas repetido de cadena[3] = O -> 3 veces  
2º caracter mas repetido de cadena[3] = Y -> 3 veces  
3º caracter mas repetido de cadena[3] = V -> 2 veces  
Indice de coincidencia de cadena[3] 0.156 (0.155555555556)

1º caracter mas repetido de cadena[4] = A -> 2 veces  
2º caracter mas repetido de cadena[4] = B -> 2 veces  
3º caracter mas repetido de cadena[4] = K -> 2 veces  
Indice de coincidencia de cadena[4] 0.067 (0.066666666667)

1º caracter mas repetido de cadena[5] = I -> 2 veces  
2º caracter mas repetido de cadena[5] = N -> 2 veces  
3º caracter mas repetido de cadena[5] = M -> 1 veces  
Indice de coincidencia de cadena[5] 0.044 (0.044444444444)

1º caracter mas repetido de cadena[6] = V -> 3 veces  
2º caracter mas repetido de cadena[6] = Q -> 2 veces  
3º caracter mas repetido de cadena[6] = T -> 2 veces  
Indice de coincidencia de cadena[6] 0.133 (0.133333333333)

1º caracter mas repetido de cadena[7] = R -> 3 veces  
2º caracter mas repetido de cadena[7] = D -> 1 veces  
3º caracter mas repetido de cadena[7] = L -> 1 veces  
Indice de coincidencia de cadena[7] 0.067 (0.066666666667)

CLAVE 1 = AZU0AIVR  
CLAVE 2 = DKJYBNQD  
CLAVE 3 = ELGVKMTL