

Un cifrario a sostituzione

QANGH TGM YJ XGHTN AVUNG TTYSH LUXYU OUAUD UQQYJ UJAXX
YNUTY NGKGB BUGMA XASLG KJUGX YQANG HTGMY JXGHT DABBY
VUJAK TYTYT ANGHT JAKTY VUJHS SYOGH TSAOD JUQAD ABBYV
GQG XG SXGVU IHAJJ UQPAV UTMAN TYSUO AXXYT YTAJJ ASXHF
AATAU QGOUT AXXUD ANGQQ ATVAN AUJFH YQYAD ANNUS QGJVG
NAJAS XGTBA TYTSY QYOAG TVGSS AOGUJ FGXXY KJUAQ PAHTL
AJKUY NTYIH ASXYD ABBYV UJAKT YQGDU XYTAJ JGLYX XAKGV
UHTMA QPQYU FGJAK TGOAU JIHGJ AGMAM GTYOA OGSXN GTXYT
UYSAT YTQPA XHXXU JYQPU GOGMG TYOGA SXNYQ UJUAK UGDAN
MUGVA JJGDH TXGVA JSHYT GSYQP AANGS AODNA JHSXN GADGY
TGBBG QYOAH TGQUJ UAKUG OGXHN GGDDA TGOGA SXNYQ UJUAK
UGALL AMUSX YIHAI DABBY VUJAK TYSUN GJJAK NYXHX XYAVG

frequenze dei caratteri % in italiano

A 10,41	B 0,95	C 4,28	D 3,82	E 12,62	F 0,75	G 2,01	H 1,10	I 11,62
J 0	K 0	L 6,61	M 2,58	N 6,49	O 8,71	P 3,20	Q 0,75	R 6,70
S 6,04	T 6,06	U 3,04	V 1,51	W 0	X 0	Y 0	Z 0,93	

frequenze dei caratteri % nel nostro testo

A 13,52	B 2,41	C 0	D 2,78	E 0	F 0,74	G 11,30	H 4,26	I 0,74
J 6,85	K 2,59	L 1,11	M 1,85	N 4,44	O 2,96	P 1,11	Q 4,44	R 0
S 4,44	T 7,78	U 8,52	V 2,78	W 0	X 6,48	Y 8,89	Z 0	

A=e

QeNGH TGM YJ XGHTN eVUNG TTYSH LUXYU OUeUD UQQYJ UJeXX
YNUTY NGKGB BUGMe XeSLG KJUGX YQeNG HTGMY JXGHT DeBBY
VUJeK TYTYT eNGHT JeKTY VUJHS SYOGH TSeOD JUQeD eBBYV
GQG XG SXGVU IHeJJ UQPeV UTMen TYSUO eXXYT YTeJJ eSXHF
eeTeU QGOUT eXXUD eNGQQ eTVen eUJFH YQYeD eNNUS QGJVG
NeJeS XGTBe TYTSY QYOeG TVGSS eOGUJ FGXXY KJUeQ PeHTL
eJKUY NTYIH eSXYD eBBYV UJeKT YQGDU XYTeJ JGLYX XeKGV
UHTMe QQPUY FGJeK TGOeU JIHGJ eGMeM GTYOe OGSXN GTXYT
UYSeT YTQPe XHXXU JYQPU GOGMG TYOGe SXNYQ UJUeK UGDeN
MUGVe JJGDH TXGVe JSHYT GSYQP eeNGS eODNe JHSXN GeDGY
TGBBG QYOeH TGQUJ UeKUG OGXHN GGDe TGOGe SXNYQ UJUeK
UGeLL eMUSX YIHeJ DeBBY VUJeK TYSUN GJJeK NYXHX XYeVG

Digrammi frequenti in italiano (nell'ordine):

er, es, on, re, el, en, de, di, si, ti, la, al

Nel nostro testo:

AN (9), YT (9), AJ (6), VU (5).

(le nostre vocali sono probabilmente G, U, Y)

G=a, N=r, ?? Y=o, T=n, U=i ??.

QeraH naMoJ XaHnr eVira nnoSH LiXoi OieiD iQQoJ iJeXX
orino raKaB BiaMe XeSLa KJiaX oQera HnaMo JXaHn DeBBo
ViJeK nonon eraHn JeKno ViJHS So0aH nSeOD JiQeD eBBoV
aQaXa SXaVi IHeJJ iQPeV inMer noSiO eXXon oneJJ eSXHF
eenei Qa0in eXXiD eraQQ enVer eiJFH oQoeD erris QaJVa
reJeS XanBe nonSo Qo0ea nVaSS e0aiJ FaXXo KJieQ PeHnL
eJKio rnoIH eSXoD eBBoV iJeKn oQaDi XoneJ JaLoX XeKaV
iHnMe QQPio FaJeK na0ei JIHaj eaMeM ano0e 0aSXR anXon
ioSen onQPe XHXXi JoQPi a0aMa no0ae SXroQ iJieK iaDer
MiaVe JJaDH nXaVe JSHon aSoQP eeraS eODre JHSXr aeDao
naBBa Qo0eH naQiJ ieKia 0aXhr aaDDe na0ae SXroQ iJieK
iaeLL eMiSX oIHeJ DeBBo ViJeK noSir aJJeK roXHX XoeVa

O=m

QeraH naMoJ XaHnr eVira nnoSH LiXoi mieid iQQoJ iJeXX
orino raKaB BiaMe XeSLa KJiaX oQera HnaMo JXaHn DeBBo
ViJeK nonon eraHn JeKno ViJHS SomaH nSemD JiQeD eBBoV
aQaXa SXaVi IHeJJ iQPeV inMer noSim eXXon oneJJ eSXHF
eenei Qamin eXXiD eraQQ enVer eiJFH oQoeD erris QaJVa
reJeS XanBe nonSo Qomea nVaSS emaiJ FaXXo KJieQ PeHnL
eJKio rnoIH eSXoD eBBoV iJeKn oQaDi XoneJ JaLoX XeKaV
iHnMe QQPio FaJeK namei JIHaj eaMeM anome maSXR anXon
ioSen onQPe XHXXi JoQPi amaMa nomae SXroQ iJieK iaDer
MiaVe JJaDH nXaVe JSHon aSoQP eeraS emDre JHSXr aeDao
naBBa QomeH naQiJ ieKia maXhr aadDe namae SXroQ iJieK
iaeLL eMiSX oIHeJ DeBBo ViJeK noSir aJJeK roXHX XoeVa

aMeM anome maSxr anXon
ioSen onQPe XHXXi JoQPi amaMa nomae SXroQ iJieK iaDer

$M=v, S=s, X=t$

la sostituzione è

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
G L Q V A F K P U - - J O T Y D I N S X H M - - - B

il testo in chiaro è:

cerau navol taunr edira nnosu bitoi mieip iccol ilett
orino ragaz ziave tesba gliat ocera unavo ltaun pezzo
dileg nonon eraun legno dilus somau nsemp licep ezzod
acata stadi quell iched inver nosim etton onell estuf
eenei camin ettip eracc ender eilfu ocoep erris calda
reles tanze nonso comea ndass email fatto gliec heunb
elgio rnoqu estop ezzod ilegn ocapi tonel labot tegad
iunve cchio faleg namei lqual eavev anome mastr anton
iosen onche tutti lochi amava nomae stroc ilieg iaper
viade llapu ntade lsuon asoch eeras empre lustr aepao
nazza comeu nacil iegia matur aappe namae stroc ilieg
iaebb evist oquel pezzo dileg nosir alleg rotut toeda