crittoanalisi di un cifrario a sostituzione

Dobbiamo decrittare il testo

```
QANGH TGMYJ 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
GQGXG 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 QQPUY 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 YIHAJ DABBY VUJAK TYSUN GJJAK NYXHX XYAVG
```

analisi delle frequenze

frequenze dei caratteri % in italiano

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

analisi delle frequenze

frequenze dei caratteri % nel nostro testo

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

proviamo A=e

QeNGH TGMYJ 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
GQGXG 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 GGDDe 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 SoOaH nSeOD JiQeD eBBoV
aQaXa SXaVi IHeJJ iQPeV inMer noSiO eXXon oneJJ eSXHF
eenei QaOin eXXiD eraQQ enVer eiJFH oQoeD erriS QaJVa
reJeS XanBe nonSo QoOea nVaSS eOaiJ FaXXo KJieQ PeHnL
eJKio rnoIH eSXoD eBBoV iJeKn oQaDi XoneJ JaLoX XeKaV
iHnMe QQPio FaJeK naOei JIHaJ eaMeM anoOe OaSXr anXon
ioSen onQPe XHXXi JoQPi aOaMa noOae SXroQ iJieK iaDer
MiaVe JJaDH nXaVe JSHon aSoQP eeraS eODre JHSXr aeDao
naBBa QoOeH naQiJ ieKia OaXHr aaDDe naOae SXroQ iJieK
iaeLL eMiSX oIHeJ DeBBo ViJeK noSir aJJeK roXHX XoeVa

```
QeraH naMoJ XaHnr eVira nnoSH LiXoi OieiD iQQoJ iJeXX
orino raKaB BiaMe XeSLa KJiaX oQera HnaMo JXaHn DeBBo
ViJeK nonon eraHn JeKno ViJHS SoOaH nSeOD JiQeD eBBoV
aQaXa SXaVi IHeJJ iQPeV inMer noSiO eXXon oneJJ eSXHF
eenei QaOin eXXiD eraQQ enVer eiJFH oQoeD erriS QaJVa
reJeS XanBe nonSo QoOea nVaSS eOaiJ FaXXo KJieQ PeHnL
eJKio rnoIH eSXoD eBBoV iJeKn oQaDi XoneJ JaLoX XeKaV
iHnMe QQPio FaJeK naOei JIHaJ eaMeM anoOe OaSXr anXon
ioSen onQPe XHXXi JoQPi aOaMa noOae SXroQ iJieK iaDer
MiaVe JJaDH nXaVe JSHon aSoQP eeraS eODre JHSXr aeDao
naBBa QoOeH naQiJ ieKia OaXHr aaDDe naOae SXroQ iJieK
iaeLL eMiSX oIHeJ DeBBo ViJeK noSir aJJeK roXHX XoeVa
```

X=t

```
QeraH naMoJ taHnr eVira nnoSH Litoi OieiD iQQoJ iJett
orino raKaB BiaMe teSLa KJiat oQera HnaMo JtaHn DeBBo
ViJeK nonon eraHn JeKno ViJHS SoOaH nSeOD JiQeD eBBoV
aQata StaVi IHeJJ iQPeV inMer noSim etton oneJJ eStHF
eenei QaOin ettiD eraQQ enVer eiJFH oQoeD erriS QaJVa
reJeS tanBe nonSo QoOea nVaSS eOaiJ Fatto KJieQ PeHnL
eJKio rnoIH eStoD eBBoV iJeKn oQaDi toneJ JaLot teKaV
iHnMe QQPio FaJeK naOei JIHaJ eaMeM anoOe maStr anton
ioSen onQPe tHtti JoQPi aOaMa noOae StroQ iJieK iaDer
MiaVe JJaDH ntaVe JSHon aSoQP eeraS eODre JHStr aeDao
naBBa QoOeH naQiJ ieKia OatHr aaDDe naOae StroQ iJieK
iaeLL eMiSt oIHeJ DeBBo ViJeK noSir aJJeK rotHt toeVa



                                  aMeM anoOe OaStr anton
ioSen onQPe tHtti JoQPi aOaMa noOae StroQ iJieK iaDer
```

M=v, S=s, O=m.....

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
```