Vigenereova šifra (anglický text bez medzier)

NOWBA KVYLV KHVZL OPTJD ZWYWY HNSXT
VUSQM JZYWR WHJAS HASYH NSXTV USQYJ
JAGAA SKVDW RTLUV SNIYL AFKLE SSKOP
EKABB GVLVC IIYLJ SWGVA ZFATT VMFOT
JMGFP WFZWK DDNPK VPDYV DRPWV TLVAU
ZYKHE HKVJI ECKOW APWVU WLPXJ AGFAH
ZKWHD TILAB LTIZG BPWVA ZWNSZ ZLCLT
ITAHP WVTLC HXMLM BZTIA ZSEGF DFZWL
JKJOS XENSH NXSBL SWCUL KHWQC PKVEC
XDAHD XEPLO JDCPY ONRYF OVERY DAZHZ
VLHWP UIPWB ZAPAG MKJSL UOQHV ZMQDP
XVNSN CDLFH XTZUY QNTRA WRXNK OWDNX
EJWYJ DNZLV WIZAU OJCFA KHWCU DAHDD
LAZWO UIPWB ZHYPH OJSZU LSNTJ ASBZS
FLKWP JKTGG PIFZM DLDIA ZWIPE KLVAG
VMGFA WVDZC SDLSV YATGH UWPNR JUIOI
FTWRP DWYWS ZDDDA ZHWFS VWPBF YWSWH
ZSQPU IYLES WCJVX WPHFD FQEIZ GWBOI
YHFWJ PEFGH DTIDS M

Kasiskiho metóda

NOWBA KVYLV KHVZL OPTJD ZWYWY HNSXT
VUSQM JZYWR WHJAS HASYH NSXTV USQYJ
JAGAA SKVDW RTLUV SNIYL AFKLE SSKOP
EKABB GVLVC IIYLJ SWGVA ZFATT VMFOT
JMGFP WFZWK DDNPK VPDYV DRPWV TLVAU
ZYKHE HKVJI ECKOW APWVU WLPXJ AGFAH
ZKWHD TILAB LTIZG BPWVA ZWNSZ ZLCLT
ITAHP WVTLC HXMLM BZTIA ZSEGF DFZWL
JKJOS XENSH NXSBL SWCUL KHWQC PKVEC
XDAHD XEPLO JDCPY ONRYF OVERY DAZHZ
VLHWP UIPWB ZAPAG MKJSL UOQHV ZMQDP
XVNSN CDLFH XTZUY QNTRA WRXNK OWDNX
EJWYJ DNZLV WIZAU OJCFA KHWCU DAHDD
LAZWO UIPWB ZHYPH OJSZU LSNTJ ASBZS
FLKWP JKTGG PIFZM DLDIA ZWIPE KLVAG
VMGFA WVDZC SDLSV YATGH UWPNR JUIOI
FTWRP DWYWS ZDDDA ZHWFS VWPBF YWSWH
ZSQPU IYLES WCJVX WPHFD FQEIZ GWBOI
YHFWJ PEFGH DTIDS M

WYW	465
GFA	276
PWV	30
AZW	240

n = 6

Index koincidencie (zisťovanie dĺžky kľúča)

n	I_c	
1	0,0434	
2	0,0476	
3	0,0540	!
4	0,0478	
5	0,0441	
6	**0,0689**	←
7	0,0402	
8	0,0483	
9	0,0529	
10	0,0480	
11	0,0428	
12	0,0681	!

Vzájomný index koincidencie (zisťovanie offsetov)

offset vzhľadom na prvý znak kľúča

	1	2	3	4	5
0	0,0393	0,0382	0,0330	0,0309	0,0254
1	0,0459	**0,0731**	0,0417	0,0471	0,0345
2	0,0451	0,0456	0,0354	0,0416	0,0361
3	0,0349	0,0306	0,0424	0,0270	0,0327
4	0,0362	0,0326	0,0313	0,0438	0,0417
5	0,0516	0,0391	0,0293	**0,0636**	0,0326
6	0,0383	0,0283	0,0401	0,0414	0,0229
7	0,0319	0,0376	0,0345	0,0290	0,0317
8	0,0384	0,0362	0,0406	0,0319	0,0449
9	0,0281	0,0290	0,0460	0,0402	0,0438
10	0,0327	0,0271	0,0399	0,0382	0,0472
11	0,0346	0,0393	0,0251	0,0347	0,0443
12	0,0425	0,0452	0,0493	0,0323	0,0358
13	0,0364	0,0499	0,0459	0,0331	0,0406
14	0,0281	0,0445	0,0331	0,0390	0,0489
15	0,0393	0,0353	0,0251	0,0365	0,0351
16	**0,0666**	0,0456	0,0363	0,0476	0,0263
17	0,0432	0,0471	0,0408	0,0517	0,0291
18	0,0273	0,0354	0,0393	0,0464	0,0325
19	0,0279	0,0268	0,0506	0,0317	0,0314
20	0,0486	0,0313	0,0372	0,0520	0,0526
21	0,0468	0,0326	0,0265	0,0372	0,0422
22	0,0367	0,0314	0,0408	0,0271	0,0227
23	0,0311	0,0517	**0,0680**	0,0270	0,0423
24	0,0350	0,0405	0,0394	0,0366	**0,0771**

Zistenie posunu prvého znaku

offset kľúča: 0, 16, 1, 23, 5, 24

A	NYVEVMVIKYFJVJKRKVJN
B	MXUDULUHJXEIUIJQJUIM
C	LWTCTKTGIWDHTHIPITHL
D	KVSBSJSFHVCGSGHOHSGK
E	JURARIREGUBFRFGNGRFJ
F	ITQZQHQDFTAEQEFMFQEI
G	HSPYPGPCESZDPDELEPDH
H	GROXOFOBDRYCOCDKDOCG
I	FQNWNENACQXBNBCJCNBF
J	EPMVMDMZBPWAMABIBMAE
K	DOLULCLYAOVZLZAHALZD
L	CNKTKBKXZNUYKYZGZKYC
M	BMJSJAJWYMTXJXYFYJXB
N	ALIRIZIVXLSWIWXEXIWA
O	ZKHQHYHUWKRVHVWDWHVZ
P	YJGPGXGTVJQUGUVCVGUY
Q	XIFOFWFSUIPTFTUBUFTX
R	**WHENEVERTHOSESTATESW**
S	VGDMDUDQSGNRDRSZSDRV
T	UFCLCTCPRFMQCQRYRCQU
U	TEBKBSBOQELPBPQXQBPT
V	SDAJARANPDKOAOPWPAOS
W	RCZIZQZMOCJNZNOVOZNR
X	QBYHYPYLNBIMYMNUNYMQ
Y	PAXGXOXKMAHLXLMTMXLP
Z	OZWFWNWJLZGKWKLSLWKO

kľúč: RHSOWP

Dešifrovaný text

Whenever those states which have been acquired as stated have been accustomed to live under their own laws and in freedom, there are three courses for those who wish to hold them: the first is to ruin them, the next is to reside there in person, the third is to permit them to live under their own laws, drawing a tribute, and establishing within it an oligarchy which will keep it friendly to you, Because such a government, being created by the prince, knows that it cannot stand without his friendship and interest, and does it utmost to support him; and therefore he who would keep a city accustomed to freedom will hold it more easily by the means of its own citizens than in any other way,

Nicolo Machiavelli: *The Prince*