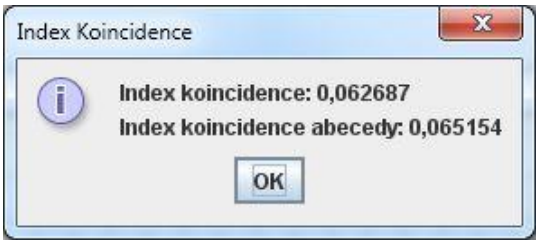
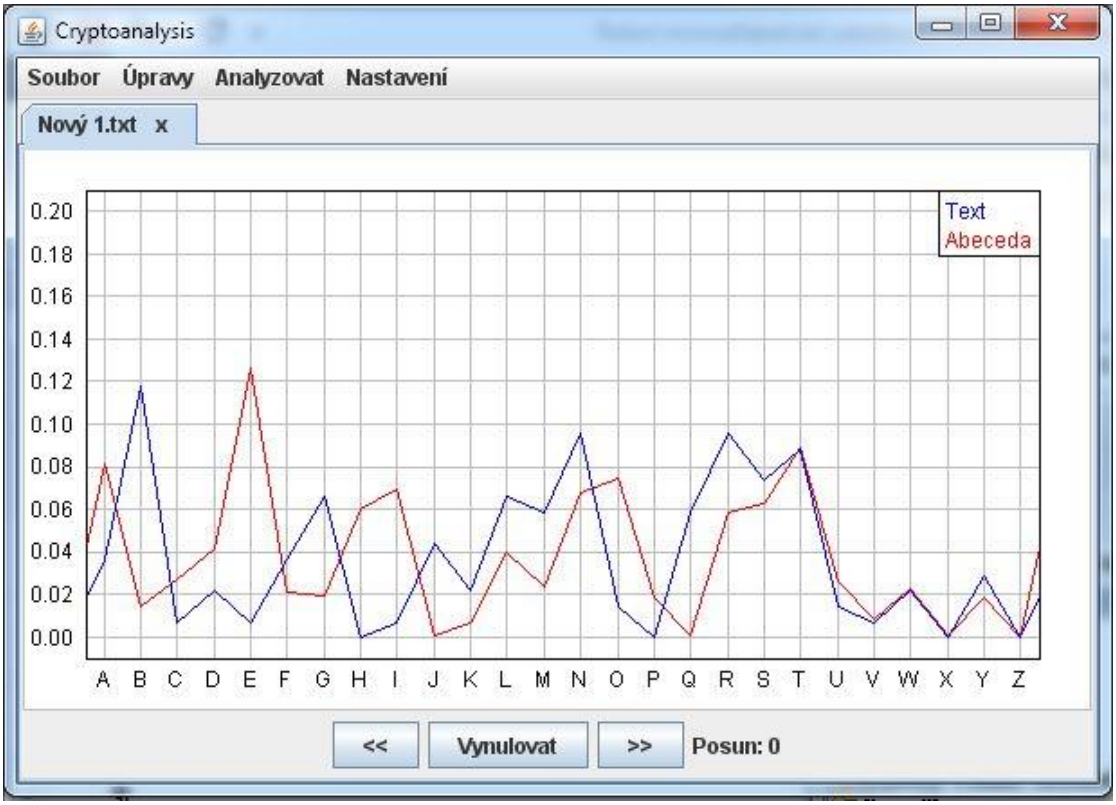
Řešení monoalfabetické substituce s heslem

```
RYENQ SNRUQ GTYGL RJUAN SRMLT QMJJG LDOFY SGRBJ BRRNS STMTF NFBQA WBQNB
SWNJJ BSOQM TNRTG LDBDB GLSTF BQKTF BTKBY RMKNV GBLNT WMQIB RRNSS ABTBB
LARMA NGLCN RTGML
```

Nejprve určíme index koincidence.



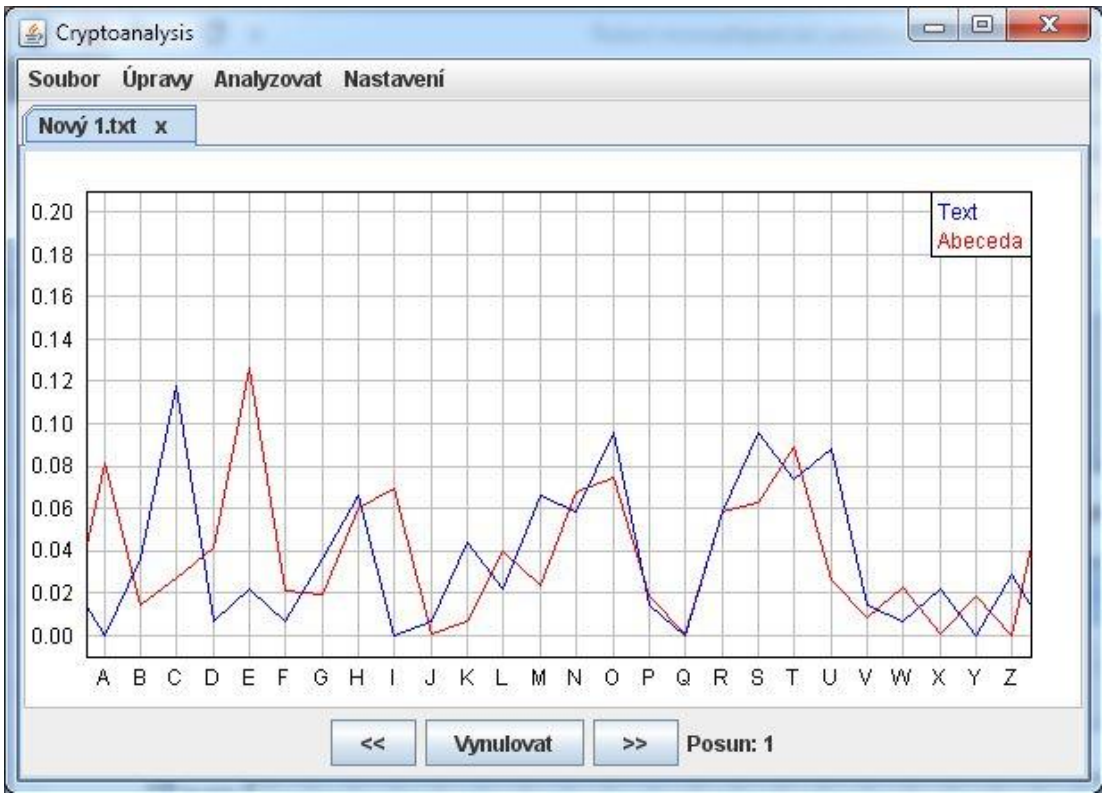
Hodnota IC ukazuje, že se může jednat o monoalfabetickou substituci. Nyní proveďme frekvenční analýzu.



Víme, že jde o text v angličtině. Z frekvenční analýzy sice nepoznáme, jaké heslo bylo použito, nicméně vidíme poměrně jasně, že grafy se velmi dobře shodují počínaje písmenem T (možná dokonce S). To nám naznačuje, že v použitém hesle bude písmenem s nejvyšší hodnotou pravděpodobně S či R.

Dále bychom se mohli pokusit odhadnout, jakými znaky jsou substituována nejčastější písmena ve zbývající části grafu. Zdá se, že v CT by například znak B mohl odpovídat písmenu E v PT. Tento předpoklad si později ověříme (mějme na paměti, že vzorek textu je poměrně krátký).

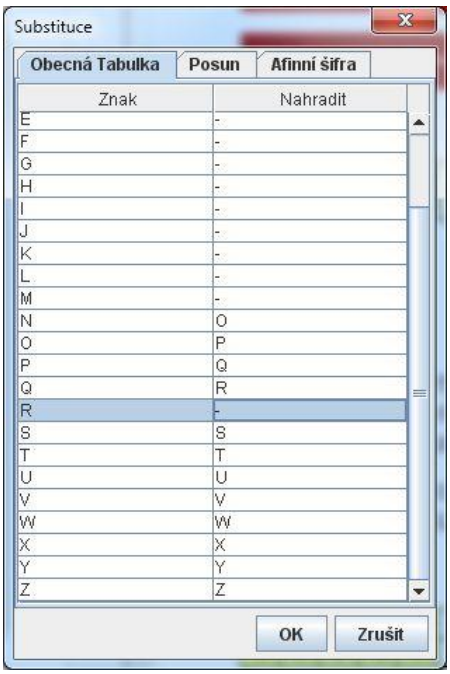
Nyní zkusme provést posun o 1 znak a pozorujme, jak vypadá shoda grafů v dalším úseku.



Opět vidíme poměrně dobrou shodu, tentokrát v úseku mezi písmeny Q a N (záměrně vynecháváme R, které je horkým kandidátem na jedno z písmen hesla). Vytvořme si částečnou převodní tabulku podle dosavadních předpokladů (první řádek odpovídá PT, druhý řádek CT). Postupujeme odzadu, kde předpokládáme identické přiřazení; je-li R skutečně písmenem hesla s nejvyšší hodnotou, bude se ve druhém řádku nacházet na některé z prvních pozic – proto je vynecháme a pokračujeme písmenem Q až po písmeno N.

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
														N	O	P	Q	S	T	U	V	W	X	Y	Z

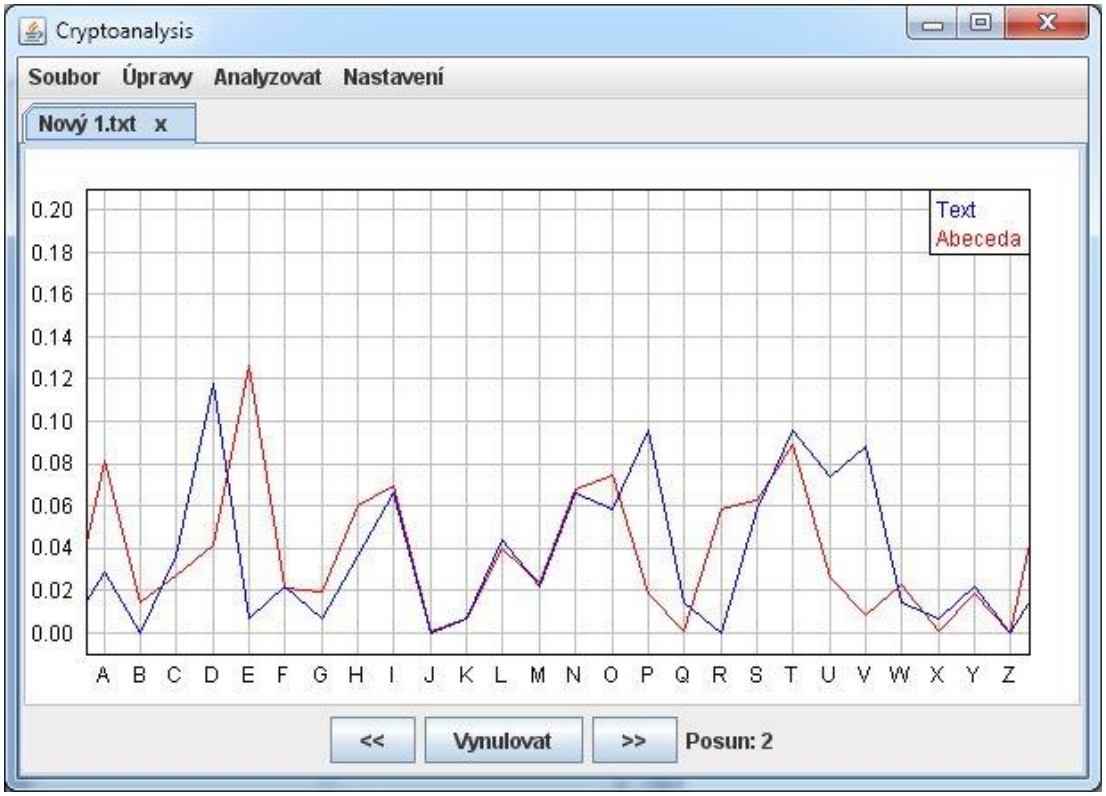
Zkusme využít nástroj pro substituci podle obecné tabulky, kam doplníme pouze uvedená písmena.



Dostaneme tak text:

```
-Y-ORSO-UR-TY----U-OS---TR------P-YS-------OSST-T-O--R-W-RO-SWO---SPR-TO-
T--------ST--R-T--T--Y---OV---OTW-R----OSS--T-------O---O-T---
```

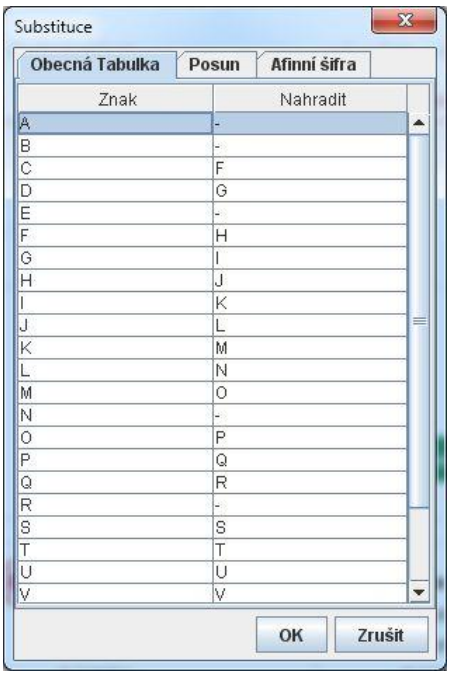
To nám příliš nepomohlo. Vypadá to, že písmeno O se objevuje příliš často a v neobvyklých kombinacích. Co když je tedy písmeno N dalším znakem hesla a v CT mu odpovídá jiný znak? Zkusme opět posunout graf frekvenční analýzy o jednu pozici.



Shoda je téměř dokonalá až po písmeno E – zde by tedy mohl být další znak hesla. Pokud tomu tak je, může mít heslo nanejvýš 5 znaků (a 3 z nich se nacházejí poblíž počátku abecedy). Upravme tabulku podle těchto předpokladů:

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
					C	D	F	G	H	I	J	K	L	M	O	P	Q	S	T	U	V	W	X	Y	Z

Opět využijeme substituci podle obecné tabulky:



Výsledkem nyní bude:

```
-Y--RS--URITYIN-LU--S-ONTROLLINGPHYSI--L----SSTOTH-H-R-W-R--SW-LL-SPROT--
TING-G-INSTH-RMTH-TM-Y-OM-VI-N-TWORK----SS--T--N--O--INF--TION
```

To už vypadá nadějně. Nejdelší souvislý segment můžeme s největší pravděpodobností doplnit na slova „CONTROLLING PHYSICAL“, a o řádek níže by mohlo být slovo „NETWORK“. Porovnáním s CT dostaneme dvojice (CT–PT): R–C, B–A a N–E. Zkusme zopakovat substituci s touto (téměř kompletní) tabulkou:

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
B		R		N	C	D	F	G	H	I	J	K	L	M	O	P	Q	S	T	U	V	W	X	Y	Z

Dostaneme text:

```
CY-ERSECURITYINCLU-ESCONTROLLINGPHYSICALACCESSTOTHEHAR-WAREASWELLASPROTEC
TINGAGAINSTHARMTHATMAYCOMEVIANETWORKACCESS-ATAAN-CO-EINFECTION
```

Je zřejmé, že poslední chybějící dvojice (CT–PT) jsou E–B a A–D. (Vidíme, že výše zmíněný předpoklad týkající se dvojice B–E byl chybný.) Úplná substituční tabulka tedy vypadá takto (žlutě jsou vyznačena písmena tvořící heslo, která jsou současně hranicemi dílčí shody mezi grafy frekvenční analýzy po provedení příslušných posunů):

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
B	E	R	A	N	C	D	F	G	H	I	J	K	L	M	O	P	Q	S	T	U	V	W	X	Y	Z

Otevřený text tedy zní:

```
CYBERSECURITYINCLUDESCONTROLLINGPHYSICALACCESSTOTHEHARDWAREASWELLASPROTEC
TINGAGAINSTHARMTHATMAYCOMEVIANETWORKACCESSDATAANDCODEINFECTION
```

neboli

```
CYBERSECURITY INCLUDES CONTROLLING PHYSICAL ACCESS TO THE HARDWARE AS
WELL AS PROTECTING AGAINST HARM THAT MAY COME VIA NETWORK ACCESS DATA AND
CODE INFECTION
```