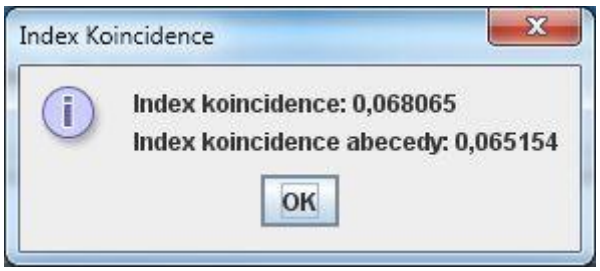
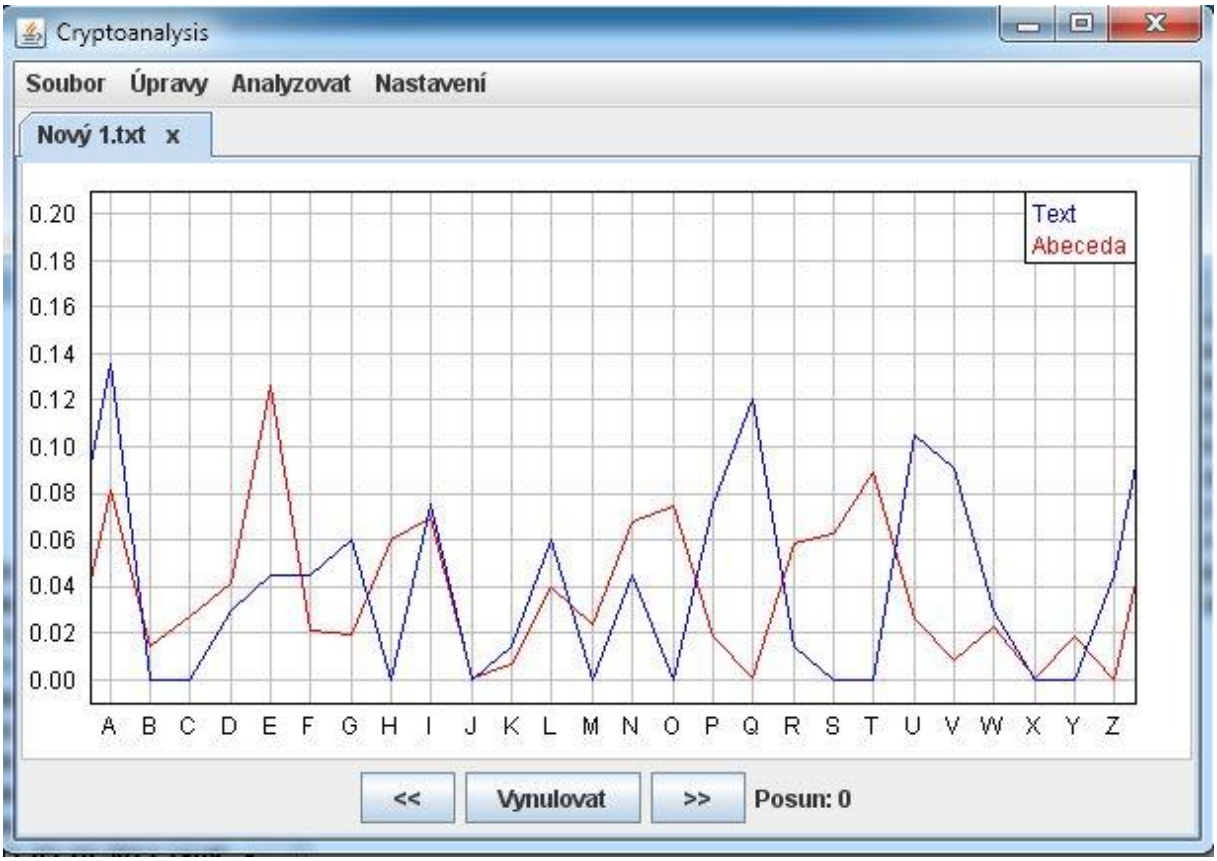
Řešení afinní šifry

QWVPAUGU PAU RQQN VFAIQZ EN LPEUQ AUVQILU KPGIP ADQ WEUL VDAILGIAF ANZ AVVFGQZ

Nejprve určíme index koincidence.



Hodnota IC nám napovídá, že se může jednat o monoalfabetickou substituci. Proveďme tedy frekvenční analýzu ŠT.



Víme, že jde o text v angličtině. Z frekvenční analýzy sice nepoznáme, jak jsou jednotlivé znaky ŠT „zamíchány“, ale můžeme odhadnout, že A a Q představují v ŠT dva velmi časté znaky. Při pohledu na ŠT zjistíme, že jednotlivá slova byla zachována v původním dělení a že několik z nich (a to i kratších) začíná znakem E. Ze znalosti angličtiny můžeme usoudit, že není pravděpodobné, aby trojpísmenná slova začínala znakem E – mnohem pravděpodobnější je, že se jedná o znak A. Předpokládejme tedy, že znak A je v daném případě šifrován opět na A (vzhledem k malému rozsahu textu nemusí nejvýraznější špička v grafu frekvenční analýzy odpovídat znaku E). Předpokládejme dále, že jako Q bude zašifrován jiný velmi často se vyskytující znak – E. Potom by v ŠT slovo „ADQ“ mohlo odpovídat původnímu slovu „ARE“. Příslušné číselné hodnoty znaků jsou: A 0, E 4, Q 16.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Setavme rovnice podle definičního vztahu: $C_i = A.P_i + B \bmod 26$

$0 = A.0 + B \bmod 26$

$16 = A.4 + B \bmod 26$

odtud snadno vyjádříme

$B = 0$

a dosadíme

$16 = 4.A \bmod 26$

Nesmíme zapomínat, že pracujeme v aritmetice mod 26. Proto neplatí A = 4, jak by se mohlo na první pohled zdát: musíme nalézt takovou hodnotu A, jejíž čtyřnásobek dá po dělení 26 zbytek 16. Tato podmínka by sice byla splněna i pro A = 4, avšak víme, že parametr A nemůže být sudé číslo, protože by k němu neexistovala multiplikativní inverze. Zkoumejme tedy násobky 26 zvětšené o požadovaný zbytek 16, zda jsou dělitelné 4:

- podmínce vyhovuje 0.26+16=16, tedy 4.4 – tuto možnost jsme však již zamítli
- 1.26+16=42 není dělitelné 4
- 2.26+16=68 odpovídá 4.17 -- tedy mohlo by platit A = 17
- Další možností je pak 94 (není dělitelné 4)
- a konečně 120 (hodnota parametru A by pak vycházela 30, což je ale číslo sudé a větší než 25)

Dále nemá smysl pokračovat. Hledaným parametrem je tedy číslo 17.

Nyní se s použitím nalezených parametrů (A = 17, B = 0) můžeme pokusit určit znaky OT podle definičního vztahu: $P_i = A^{-1}(C_i - B) \bmod 26$

Připomeňme si, že v aritmetice mod 26 je A^{-1} multiplikativní inverze parametru A (v našem případě čísla 17), tedy číslo, kterým musíme vynásobit A, abychom dostali výsledek 1 mod 26. Jak si můžeme snadno ověřit, hledaným číslem je 23. Jelikož B = 0, budeme počítat podle vztahu: $P_i = 23.C_i \bmod 26$

Postupně dosazujme číselné hodnoty jednotlivých znaků ŠT (16, 22, 21, 15, 0, 20, 6, 20 ...) a dostaneme číselné hodnoty příslušných znaků OT (4, 12, 15, 7, 0, 18, 8, 18 ...), které můžeme převést na text:

QWVPAUGU ...

EMPHASIS ...

Jak vidíme, text vypadá, že by mohl dávat smysl, tedy že jsou parametry pravděpodobně určeny správně. Pokračujme v dešifrování a obdržíme celý OT:

QWVPAUGU PAU RQQN VFAIQZ EN LPEUQ AUVQILU KPGIP ADQ WEUL VDAILGIAF ANZ AVVFGQZ

EMPHASIS HAS BEEN PLACED ON THOSE ASPECTS WHICH ARE MOST PRACTICAL AND APPLIED