

Zpracování úlohy předmětu Inovace pro informatiky Vigenérova aifra

Zadání:

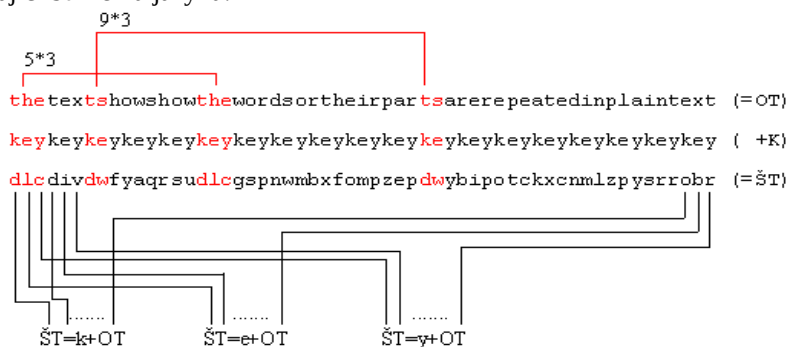
Odhalení délky klíče, odhalení klíče a deaifrování souboru aktualne.vig (Vigenerova aifra)

Vypracování:

Luatění spočívá ve dvou základních krocích.

První krokem je určení délky periodicky se opakujícího Vigenérova klíče. Vychází z jednoduchého předpokladu, že v dlouhém otevřeném se textu se najde mnoho opakujících se slov nebo jejich částí. Jestliže ovaem dojde k současnému opakování v otevřeném textu a v klíči, projeví se tento fakt i ve výskytu opakování v aifrovaném textu. Vzdálenost mezi těmito opakováními je potom násobkem délky klíče. Z několika opakování je pak možné určit délku klíče.

Druhý krok spočívá v určení písmen vlastního klíče. Mějme například klíč dlouhý 3 písmena. První písmeno v ka-dé trojici aifrovaného textu je aifrováno stejným klíčem. Zkouáme tedy různá písmena klíče, dokud nevznikne frekvence písmen odpovídající běžnému jazyku.



Pro rychlejší a jednodušší možnost rozluštění jsem si našel stánku

<http://cryptoclub.math.uic.edu/vigenere/decrypt.php>

Zde jsem zkopíroval zadaný řetězec písmen, ale pro rozluštění mě chyběla znalost délky klíče. Proto jsem se odkazem

Help me find key length na dataí aplikaci, která slouží k odhalení délky klíče. Následně jsem vybíral postupně všechny možné opakující se posloupnosti znaků v kódu. Program vypisuje pod znaky i jejich pořadové číslo, začínající 10 a končící 2100. Zadával jsem posloupnosti od těch nejdelaších po kratší. Také je důležitá četnost takové sekvence. Čím je častější, tím je pravděpodobnější, že jsme na dobré cestě. Po čase jsem došel na sekvenci znaku MMSUIZ. Z přečtených materiálů jsem věděl, že vzdálenost mezi těmito opakujícími se znaky je násobek délky klíče. Postupně jsem počítal tyto vzdálenosti tj. 144-109=35, 294-144=150, 879-294=585, 1144-879=265, 2029-1144=885. Dělitelem těchto čísel je číslo 5. Z tohoto principu jsem určil délku klíče na hodnotu 5. S tím, že jsem již znal délku klíče jsem se odkazem Return to decrypting page dostal na původní stránku projektu. Zde jsem k již zadanému textu přidal délku klíče. Pomocí frekvenční analýzy jsem zjistil četnost jednotlivých znaků. Z přednášek jsem použil posun k nejčastěji používanému písmenu českého jazyka, tedy E. Výsledek frekvenční analýzy byl tento: 1. - O, 2. - T, 3. - M, 4. - F, 5. - S. Z toho postupu mě vyvalo klíčové slovo KPIBO a po použití na aifrovaná data jsem zjistil, že to je správné klíčové slovo.

Zadaná aifrovaná zpráva ze souboru aktualne.vig

MTALCXTAQZXXAWITTDSCZHSZNKKIASUKMWMBDJFNOAMOSOAMLHBXVZJVPLBDBXDTHEECECO
KZPDCZMVBSTAMWLXTBNOSWSCUJHWMCXPRSAMMSUIZJQUTMOSBVQFNFTBSBIRPDWFDLOWM
WMMSUIZBFOCVBCCBXSCMTVUIJIZJFYZGQFOSDZDBHMOWWIWICDDBFFWXVVCFHMNASCQTHOG
AUJKEZVAIHTVOJXDPHXXPPDBDAUFOSQQFSEWVGDRJNOIWCMDVXSWVXAPDDXUJGDXKLSMXTQ
FYKGSCLJMSUIZJQUTMOSBVQFNYPJSIMMBIRPARBDRVDBDZPYXTJVRHODZGYZWVDBPDESZD
LPPXDAUWCETOSXHBXPXSKMTDYAMDBOXSOFWCCBQOWCIMSOGDTDBSXTZHSDXKLSRDZFUEAI
DBSWWVFKSCCECUJUFBDJHQFYFMEBKAIWZKSIAODXUTSYSPBRIOMDSCZWOSCETOWCKCKNKKIAS
UKMWMBDJFQSHBFSVTSUFSCGPPTTDPJKAGIZKKVFJYSJPFXNKIHOMBQFRIMEGOEWEHYEWESZHM
OSBQOWCIMSOGDKIWWNTWDVVDCCOMTHVBKHCDEJJDJRSIMABOQMKOUBWEFODSPJIHKIZYRPMC
EQIDSJJVBGERPVIFXLJHOOVFPOYLAYSZFCUDDZGMWTPJYSIWGORPOCXTHBQRGIOFWAWOWCTDP
PXDDJHOAVZQROLSTXKISXTZHWOKGSCLXTPDBDKFBDRQTHOTTFYDGQOMMDHCMVDWQFYRMO
HFXXKOSJKZPQOKMADBPDFASCQTHOGAUSFPZFUEAIDBSWWVFKSCTSYKAFAEKIEWJTBPIAWQFOS
MWGSBLJYIKWEBSBMMSUIZBFXPUKSTXKINSCAUOVDDDBIKGLCXMPJCTUVNBDSZNRGCCOCIMK
BIKQDSMXAUSOAMLHBXVZGOEZPHYKGSCLXTPRSZGQFOSVJJIBPZRBTPUSRSZAZDLNWZXINPIALP
GDPBFYFDLZGDXUUCDGMOROBDOUCMMNOSWCINDCDBKEWDWDPBVDYOWSBEYMTSFTHQFKK
MQFYKTBREIMOHYEZFRZDSMONHMQCDKZEWVJHMSDDAWMBDJBSVTSUFSCGWSFDLOWMWMMSU
IZBFXPKIHYIQAFOZWSRXTXSCZPLMOWJHFNKIWFLDGMNBSHCDVYZDVZSCMNIJYMASTBMOOFTD
MHKKALSUPALONTVFRYHBBHOZDPRHXZPZORVPGDRMADYIDRSASAFYMKWMWDPRXXKISVTSUF
KGVBBQRHMPDBDBJZCALIZGWQONAIWMBDJBSVTSUFSCGPDBDKFBDICSPSCGWMCRPMMJTTFBKT
TFYDGGQOBTSPFNCMQFYIEZKKQDSJSMQCNAMNWXXAUSBHBWOZGCNMCACUOUAMUCCEWQFF
TXPASCQNOVCMQSDXTFHORPQCNXTFZOZBSWXNHPPXDDJHOAVZQROLSTJVBQOASPJORMTYOHX
PHBTJFBOKHSCCIMBZOZTFGXTJJCWPAABOCIQXJRFCMTSBJKQCFEFGWNVVPDOWWSCWCNTUQFY
RKFGUDAOSTKMUGSEZBJNTXPRYQVPGDXVFGZAVJGJRFYAWHWMZGAOFPHFYTTBFBJTAFBOSIS
WFXKFJJHJJKIJJCWPAZDBDDZFYQCFZOZBSWXNXSOFTLPPSDUBGIGGDVVTZPGDDCDWMWLSFFXV
ASWTLFZCZGDVZAWEWXRQFYAWHWMZGDVZTTFHLNTZYVPLFBKMMYOCIESTTDJRODMOSBVQF
NOHTVBMTVFQRRMNSUKCMWZGITODZCNSXTZHWOMTZECKFBORPDSWTSWIVXXSOPBLIWMIPF
OIQDYIEWUSXRQBZTTHOOMCGUJBSQTSFSWLIWTVUIDGPTSKAMTHKAMOSBDHWWXJTCWYBITMTT
AUOVTVFRYHBBHOZBBYJTVFAYWWVJJCQLODCWWSOAMLHBPZOMUIMSSLNRJGZPTPKAGOOZGQL
ZKSKFNLNKIHOADFGFTMMSUIZBFXTDICNDVJBOHXBZYKIUJIWZBRXTJJCWPAVBKGIWYKAFAXPH
BGKSVJDBTSBNUJVFAKZLFJJXBECCIXBZSKIEOVHQNDBJMSWTUKSJTAFGZDCTHEQQPAKHGWMFP
HJRYOIIKFCQDWFGILCEHSVDYAALIMXVFAORSVRYHBBYJKFGUTNJFWNHBDKAQWCFTLSSFDKJGV
PUVJSRXFBOOHFZOCIFBOGOJSFDPSCJTVJPSDUBGKYLFBKTFQCBIDJQOOLFJIKWAPSDUBGIHBBZOG
WTHOJXPNYGVJZEVOVBXKGMNWB DAMOFHIGOBXSQFOSAFRKRMTYOWWTRBJHFBSEZPPSDINOCJKA
PSDUQFSYLFHBTAUNLGCSTSVJRBYLJLFBKCMTDVCMOWMTALSRDHBKOSVFOPOPJKIMWFYEALOU
UJGOHMAODXUOSNPWEVKSPIDKSSOTCQNDXBXXBROBCASLGCTSVWEEDOIMCLJSFJBDXTYOBCT
CESCLHOGGCMWDPMQOHSFFOECCZSRMVROAQUQSIMMBYJXPYEICULNHFAOBWIZKETBHSIBBYN
AWVVYSWLINQGTJEYHBJKOMLBOHXMBSAITHSCWWMWXVJGDGHJJYIVJVYEZPGDGMWZTBSDOIZ
AWVTSAQCHLNOTPAOCEOBFRFNHWOVBQOWCIZZDBJUZGVJIAWFDBOWRDXSCCIZFRSBISHSCISWW
PVBOWPZUWXPJVFCXSBOLNAQCVJAQFOSAFRYJMOSBVMUWMZMICBTOVZKRVJVYJZBREYWTSP
TUGWBIMNFOOQHBYKIMWXPWSPJVLQO

Deaifrovaná zpráva:

CEKONESPLNISVUJEVROPSKYZAVAZEKVEVYROBEZELENEELEKTRINYVLADAPRIVSTUPUDOEVROP
SKEUNIESLIBILAZEDOROKUZVYSIPODILELEKTRICKEENERGIEZVETRNYCHCIVODNICHELEKTRAREN
NAOSMPROCENTUZTRIROKYPREDVYPRSENIMTOHOTOTERMINUOVSEMMINISTERSTVAPRUMYSLUA
ZIVOTNIHOPROSTREDIPRIPOUSTEJIZETOBYLOPRILISOPTIMISTICKECILPROVYROBUELEKTRICKEENE
RGIEZOBNOVITELNYCHZDROJUPROROKNEBUDES VYSOKOUPRAVDEPODOBNOSTISPLNENSTOJI...atd

Zdroje:

Čerpal jsem z předávek a také z internetu:

<http://sovickacz.blog.cz/0710/vigenerova-sifra> stránka pro pochopení základního principu

<http://moon.felk.cvut.cz/~pjv/Jak/info/i416/Codus.htm> stránka pro pochopení luaticího principu

<http://cryptoclub.math.uic.edu/vigenere/decrypt.php> stránka pro pomoc při deaifrování