

## Cvičení č. 5 - 18.3.2024

- Termín odevzdání je 5.4.2024 do 9:00, na cvičení je možné pracovat i příští týden.
  - Na řešení není možno spolupracovat s ostatními studenty.
  - Řešení budete odevzdávat do LMS. Odevzdejte jeden archivní soubor s řešením, pojmenujte ho svým loginem + "5cv KPB", do předmětu emailové zprávy napište "5. cvičení KPB". Součástí archivu bude jednak dokumentace v pdf formátu popisující postup Vašeho řešení, a případně zdrojové kódy s vašimi aplikacemi. Neposílejte exe, dll, py soubory apod., neprojde to školní poštou (použijte nějaké úložiště).
  - K vyřešení můžete používat jakékoli studijní materiály a nástroje (např. Cryptool, různé online aplikace např. <http://www.practicalcryptography.com/cryptanalysis/> nebo vlastní implementace (odevzdat)), odkazy na „cizí nástroje“ musí být v dokumentaci.
- Následující šifrový text vznikl obecnou monoalafabetickou substitucí z anglického textu, otevřená i šifrová abeceda jsou anglická abeceda bez mezery. Dešifrujte jej a kromě otevřeného textu uveďte použitý klíč (tj. šifrovou abecedu) a postup řešení.  
APSECETEADEJSFDDDELJTFeQEJTPFAQEJLDYUSEDEZFIEJVapekuqqftupesyaqmfTSQSKFJNAJTFNSNPFA  
SFTSEKJEJTEIFJSPFQMKJQFAJIKVFPADDTYRFPQFTUPESYNFPFAPFQKHFBFYWAYQAEEQUQFIEJQFTUPESYA  
IAJTFISNPFAISFTSEKJAJKHADYIFSFTSEKJAAEEIFJSECEFQUJUQUADMASSFPJQEJIETASEJLMKSFJSEAD  
SNPFASQRFNAVEKPADAJADYSETQHKJESKPQUQFPQPAJIFSWKPBFRNAVEKPCPKPQUQMTEKUQATSEVESEFQQELJA  
SUPFDFQQIFSFTSEKJPFTKLJEZFQJFWAJIUBJKWJSNPFAQRQAFIKJHADETEKUQRFNAVEKPJFSWKBMPKSFT  
SEKJEJSPUQEJKJIFSFTSEKJAJIMPVFVJSEKJAEOUETBDYIFSFTSQAJIPFQMKJIQSKJFSWKBPEJSPUQEJKQCEP  
FWADDKMSHEZASEKJAJADYZFQJFSWKBPSACCETSKKMSEHEZFCCEPFWADDPUDFQAJIEIFJSECYVUDJFPAREDE  
SEFQFJIMKEJSQFTUPESYFJNAJTFHFJSFJIMKEJSMPKSFTSEKJAEIPEVFJAJSEVEPUQAJIAJSEHADWAPFIFSF  
TSAJIMPVFVJSHADWAPFEJCFTSEKJQZFPKIAYSNPFASIFSFTSEKJEIFJSECEFQUJBJKWJSNPFAQRYHKJESKP  
EJLFJIMKEJSRFNAVEKPUQFPAUSNFJSETASEKJAJIATTFQQQFTUPESYREKHFSPTAUSNFJSETASEKJAEFJARD  
FQQFTUPFATTFQQQFQJLREKHFSPETQRFNAVEKPRAFIAUSNFJSETASEKJAJADYZFQQUQFPRFNAVEKPMASSFPJQ  
CKPUJAUSNPKPEZFIATTFQQIFSFTSEKJQFTUPESYKMFPASEKJQKMSHEZASEKJQEFHFJNAJTFHFJSAEAUSKHAS  
FQQEFHMDASCKPHQSNPFASAJADYQEADQFPMPEKPESEZASEKJAJIEJTEIFJSPFQMKJQFTNASRKSQAJIVEPSUA  
DAQQEQSAJSQAEAEIQQFTUPESYAJADYQSQEJPFADSEHFEJTEIFJSEIFJSECETASEKJAJIHESELASEKJMNEQNE  
JLAJICPAUIMPFVJSEKJFHADQFTUPESYAEAJADYZFQFHAEDTKJSFJSAJIQFJIFPRFNAVEKPSKIFSFSTMNEQ  
NEJLAJIHADETEKUQFHAEDQSPAjqatSEKJHKJESKPEJLCDALQQUQMTEKUQCEJAJTEADSPAjqatSEKJQAJICP  
AUIEJIETASKPVUDJFPAREDESYHAJALFHJSAUSKHASFIQTAJJIEJLAEUSKHASFQVUDJFPAREDESYQT AJJEJ  
LAJIAQQFQQHFJSPEQBAQQFQQHFJSAEVADUASFQVUDJFPAREDESYQFVFPESYAJIEHMATSCKPMPEKPESEZFIP  
FHFIEASEKJQFTUPESYauskhasekjaJIKPTNFQSPASEKJEJTEIFJSPFQMKJQFAUSKHASEKJAEIPEVFJWKB  
KWQAUSKHASFPQMKJQFQSKTKHHKJQFTUPESYEJTEIFJSQKPTNFQSPASEKJAETKKPIEJASFQQFTUPESYMPKTF  
QQFQCKPTKHMDFXSNPFAASPQMKJQFQMPFIETSEVFAJADYQECKPSNPFAQSNSPFASEJSFDDDELJTFAEAJADYZF  
QSNPFASEJSFDDDELJTFCFFIJSKMPFIETSFHPLEJLSNPFAJSQAJIVUDJFPAREDESEFQMNQYETADQFTUPESYFJ  
NAJTFHFJSQUPVFEDDAJTFAEWKWPFFIVEIFKAJADYSETQEIJSECEFQQUQMTEKUQATSEVESEFQCKPEHMPKVF  
IMNYQETADQFTUPESYTKHMDEAJTFAJIPFMKPSEJLAUSKHASEKJAUIESAJITKHMDEAJTFAEAQQEQSQEJAUSKHA  
SEJLTKHMDEAJTFNTFBQAJILFJFPASEJLPFMKPSQSKHFFSPFLUDASEKJQQFTUPFKCSWAPFIFVFDKMHFJSQ  
MMKPSQSASETAJIIYAHETTKIFAJADYQEQAEEAJADYZFQTKIFCKPQFTUPESYVUDJFPAREDESEFQIUEPJLIFVFD  
KMHFJSTKJSEJUKUQHKJESKPEJLUMIASFQAJISPAEJEJLAPFFQQFJSEADSKQSAYANFAIKCFVKDVEJLSNPFA
  - Následující šifrový text opět vznikl monoalafabetickou substitucí z anglického textu, otevřená i šifrová abeceda jsou anglická abeceda bez mezery. Dešifrujte jej a kromě otevřeného textu uveďte použitý klíč (šifrovou abecedu) a postup řešení. Jaká šifra (šifrovací algoritmus) byla použita? Rozhodněte, co je neobvyklé na získaném otevřeném textu, a jaké to může mít důsledky (co to ovlivní)?  
GSRHRHZMFMFHZOKZIZTIZKSRZNXFIRLFHZHGLQFHGSLDJFRXPOBBLFXZMURMWLFGDSZGRHLMFHZOZYL  
GRGRGOLLPHHLIWRMZIBZMWKOZRMGSZGBLFDLFOWGSRMPMLGSRMTDZHDILMTDRGSRGRMUZXGMLGSRMTRHDIL

MTDRGSRGRGRHSRTSOBFMFHFZOGSLFTSHGFWRGZMWGSRMPZYLFGRGYFGBLFHGRONZBMLGURMWZMBGSRMTLW  
WRUBLFDLIPZGRGZYRGBLFNRTSGURMWLFGGIBGLWLHLDRGSLFGZMBXLZSRMTZOGSLFTSRGRHSRTSOBXLNLM  
RMNLHGKZIZTIZKSHZGIRZOZGXXLNKORHSRMTFXSZMXXLFMGLUDIRGRMTRHMLGGSGWRUURXF0GBLFDLFO  
WDZMGGLPMLDGSZGGSRHGZHPNRTSGLXXFKBNLHGLUBLFIYIZRMULISLFIHRUMLGULIZHSLIGWFIZGRLMZMWZH  
BLFTLGSILEFTSGSRHZXXLFMGRGXLNKLHGRGLMDR000LLPZGBKRXZORMZDZBLIGDLSRHRHHLULIRZNHGIFTT  
ORMTGLZGGZRMDLIWHGSZGDLF0WRNKZIGDSZGRDZMGLHZBZMWRMLRMTLNRNHOHMLGULZMWB  
IWHGSZGRNFHGRHNRHLDRTGLLFIXLWMWRGRMLMGSGZGYRMWGRHHLOFGRLMMLGDROORMTGLTLLMZWLMDRGS  
GSRHHFKKLHRTMOBHR00BZMZYHFIWKZIZTIZKSROOLKGGLKFGZS0ZGGSRHKLRMGSZERMTHSLSMKIZXGRZ  
OOBGSZGRGRHMLGRNKIZXGRXZ0GLZGGZRMZKIZTIZKSDRGSLFIHBNYLOLUSRTSG

3. Následující šifrový text vznikl Vigenerovou šifrou z anglického textu pomocí klíče o délce nejvýše 8 znaků. Kromě získaného otevřeného textu uveďte použitý klíč a postup řešení. Přípustná abeceda je anglická abeceda bez mezery. Použijte index koincidence i Kasiského test (oba!). Pro určení posunu ukažte využití Chí-kvadrát testu.

IAKMIIMSSVLIMSLBEEJEKMMMELOAMTLSKOJXHWKIJYRJXGKMOFHJAISMLGYVIKMJFVMSGCTLRALXZENKXEJ  
XEJBWRGEDDXFIETAHRFJTZXIXMUEILFJLAYIFZEJWIRXHSGHRZEJRMDTOJMEEXTAFIFJTZXCVERETRPROFVLI  
MSLBEEWADLSYEVWTLPPIVTCRXTZBWKMMLSZXIKTTFTUDTVKMMWMSKVANXPVSHXRUAIALAJIMEFWWRDXTQZ  
PYOXWVILGMWFJSQFFFPSGYRVALAYIRXESLVVEKIITMADECVKGKVLZGKKYPFAEJLEEHRSUFZXSLAIJISQFFF  
PSYHFRGKLHEEGIWGXGEWSXIEDAMMFRSOAMTLCWEISVALXHWIRLBZXYJXFZVTZTRUREOZVFATZJKIRLAIC  
SNYPMEXEJFSEXHKMLVHALXWFJESLVVCZTRXIFJHQPIAJMSPIAJUYKMTMLYRPLQYECPSKHQVXIEFXVWWXRK  
LEWGHFJMSKGYENVMLVINVHJRTRAEMAEKMIIRCZKMJXISGMKCESLXVVSMDHRCIKMLVJIJLXJYNVTCRJTWKXY  
IFAKWKJUDEQFSNGYWGIVFZAYMCZLXRVTKRDERUAXYIESLXVNVNGKXYSDGQGYYRUAIJAHAVLLWESWMWJEJXRK  
GADXRUERTZVESDBKYXLQWMWJEJXRKAQHJTELUNPRXIFZIRWTWKEEHUKNECPYUXPVFRSMIVESLXVRPILMPV  
IAJEMVVOJEEKIRLAINIECUIWSRWXEJXEJBWTLDXHYSLQPIVOTZXJZVSLWEPSFZHPPAEWDMJTADFWLRDSRAY  
MCZBWKLEKNRUEYTXJFVEWTWKIRETRPGHJBWKMAFLGPETKEKITZBWRWTZXHRCZTXAISMLIEXEJXHAIRMLEC  
IMSGHGIOHEIKLRWPHFANTKEEGHWLJISMHTPDXRWXWFRTZXFEDLHAVPCGFIYMMXHYIHAQLPRXEJBWDEUFWCK  
LUJLHRCWZBGYQAJDWKLEDTWKWHUIIIAHGNVWUKTXVFRWTHRRDVKEEOWAGINMTZAMJXWWEZVHVKVMGPEKMLV  
JODESNMNYWEPMSYHSUJRAWPAHAVLWSAZRZJIUTRKJOJVLIIMSLBEEWAKMLVHAQMLRXJWLYJAAKIYKXOVXEK  
LOFMLVGRGLWDENQVLIIMSLBEEWBWEMVZELAEKNEKNWNESCPCIDSGHSYRAXHZRALHQSSNLAIWVIVTCRRDLAEK  
KOVKEZWEVAMDJRGFXYIDWTHFRZXWLRDSRWFIAKMIIWUFWEPMSSVICIBJTXZSNGYXYIRWLYIVEUMMFROXCIJ  
YS

4. Je známo, že opětovné použití téhož klíče u Vernamovy šifry (One-time Pad) může být nebezpečné. V této úloze jsou všechny znaky reprezentovány jako 8 bitů v obvyklém US-ASCII kódování (například 'A' je 0x41). Nechť  $M = (m_1, m_2, \dots, m_n)$  je otevřený text, který se skládá ze sekvence  $n$  bajtů. Nechť  $K = (k_1, k_2, \dots, k_n)$  je klíč skládající se opět z  $n$  bajtů. A jak je obvyklé,  $n$  bajtová sekvence  $C = (c_1, c_2, \dots, c_n)$  je šifrový text získaný „xor-ováním“ každého bajtu otevřeného textu s odpovídajícím bajtem klíče  $c_i = m_i \oplus k_i$ , pro  $i = 1, 2, \dots, n$ . Pokud budeme mít více než jeden otevřený text, budeme tyto označovat jako  $M_1, M_2, \dots, M_k$  a bajty OT jako  $M_j$  jako  $m_{ji}$ , a to  $M_j = (m_{j1}, \dots, m_{jn})$ ; analogické označení použijeme pro odpovídající šifrové texty.

Mějme dva 12-znakové šifrové texty  $C_1, C_2$  obdržené Vernamovou šifrou. Rozhodněte, zda byly zašifrovány stejným klíčem nebo klíči různými. Pokud jsou klíče různé, vysvětlete proč nemohou být stejné. Pokud jsou klíče stejné, pak dešifrujte šifrové texty. Součástí řešení budou oba otevřené texty  $M_1, M_2$ , správné klíče/klíč a postup Vašeho řešení. **Otevřenými texty je vždy SMYSLUPNÉ celé anglické slovo o 12 znacích ze slovníku uvedeného v souboru dic.txt.** Otevřená abeceda je anglická abeceda bez mezery, obsahuje jen alfabetické znaky (malé i velké). **Šifrová abeceda je 128 znaků ASCII tabulky.**

$C_1 = 22\ 02\ 0f\ 1c\ 0b\ 1a\ 1e\ 0f\ 1d\ 08\ 18\ 16$

$C_2 = 2c\ 11\ 1c\ 06\ 14\ 1b\ 07\ 00\ 00\ 12\ 1a\ 00$

5. Vyluštěte tento šifrový text (jednoduchá transpozice (Columnar transposition)), nalezněte oba klíče (obě permutace - šifrovací, dešifrovací). Otevřený text byl v češtině, přípustná abeceda je anglická abeceda bez mezery. Uveďte postup řešení.

IVCTIARJLNKEKCRNICIDIVAMISVHWEIPIEIANBMOMDTLRRAKIEMTMNOYSNAMEZETOUDGUDTAMCSIOJZUCAB  
UETANKNSENEFMDIOAJPRCLSCVCDUCPOENPOZNEHSONIPUDOMEAHYEIAPUUSOMTNINRNBOAIIIAINTAKCZHN  
ACVCKAVSLPJOTREOIAESJHCKAORDUIAOADWDIAZANNSNDJCQLEISJDERZIAMAIISDECITOJZVONTOCVCOJST  
MAAIPIAEYPONEMTESEYKDEEDAJHNODHZIFAEMOYJBPLNKINEULNKYNZLMRRIOTVTDEEEIAEIDLHAMTAEEAJZ  
AIYAAAHCINANEMTAPIVCIZNSLEIPJPOAAEILOCIRAOVVTYTEJLNASJYNRAOLAHILPEDITIFOMSAVECIINASI  
EACSNDTEKSTIEACHOOTNVOEIZCCHSLSHVAZYDANRFLHSKOPYSLREAXKPGNNKRNYRVEIACZNIEIMTETATAP  
EMLMNSDIUCAOEPKZFNDKTAUCZTUNIEACYIUQ