2. zápočtový úkol z KPB - zadáno dne 23.3.2022

Informace:

- **Termín odevzdání je 6.4.2022 do 23:59**.
- Na řešení není možno spolupracovat s ostatními studenty.
- Řešení budete odevzdávat pouze elektronicky. Zašlete jeden archivní soubor s řešením na můj email, pojmenujte ho svým loginem (loginy), do předmětu emailové zprávy napište "2. zápočet KPB". Součástí archivu bude jednak dokumentace v pdf formátu popisující postup Vašeho řešení, a dále zdrojové kódy s vašimi aplikacemi, pokud jste je ještě neodevzdávali v rámci 1. úkolu. Neposílejte exe, dll soubory apod., neprojde to školní poštou.
- K vyřešení můžete používat jakékoliv studijní materiály a nástroje (např. Cryptool nebo web `http://www.practicalcryptography.com/cryptanalysis/`), odkazy na ně musí být v dokumentaci. Použijte pokud možno také vlastní implementace ze cvičení. Pokud pro nějakou část potřebných kroků použijete jiný software, uveďte ho v dokumentaci (např. jeho URL adresu).

1. (2 body) 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 (šifrovou abecedu) a postup řešení. Využijte Chí-kvadrát test. Můžete také využít frekvence monogramů, bigramů, atd. z `http://www.practicalcryptography.com/cryptanalysis/letter-frequencies-various-languages/`.

   ```
   OJRGEQKTRNDEVPDOAGRKTLPKUEJNETPVJNEUOJNEJRUVJAKAGQVWRGENPOQLQBOEQKTHVLVJEQEWKKCNSRLP
   OJRQRGEVDFKJCIDKQQKFQAJVPDECRPEEQVJCOPOQEQRGVRCKRRECRGETPEJNGDVJCQNVLEPEFOJCECGOFKTJ
   VRSPEQNEJEQLVOJRECOJBYKRKVJCOJRGEDKNVDQWGKCPVJBOJNVTEQKTVPDEQGEQVWPEQKJVJNEQWORGRGEA
   EOQGVQVJCBVISBOVNRKPQKTVNKSJRPYGECJEUEPUOQORECVRTOPQRUVJAKAGQOFLDYNKLOECRGEWKPBQOJIK
   RGQBERNGEQVJCKODLVOJROJAQIYRGEROFERGEVPROQRFKUECRKVPDEQGEWVQTSDDYOJRGERGPVDDKTHVLVJK
   JRGERPVOJTPKFLVPOQGEPELEVRECDYNGENBECKSRRGEWOJCKWGEWPKRERKGOQTPOEJCLVSDAVSASOJRKQEEO
   TORWVQDOBEHVLVJYER!NGODCOQGOQJRORRGEOFLVNRWVQFKPEQSIRDEFKPEISPOECOJGOQRENGJOMSETKPOJ
   QRVJNEGEQKFEROFEQCOUOCECRGENVJUVQSQOJACOVAKJVDDOJEQPVRGEPRGVJSQOJAGKPOZKJRVDLEPQLENR
   OUELDVJEQVQWVQRGEJKPFOJWEQREPJLVOJROJAVJCGEWKSDCQRPEVBGOQLVOJROJAQWORGCOVAKJVDPVOJVQ
   GEGVCQEEJOJHVLVJEQELPOJRQ
   ```

2. (3 body) Následující šifrový text opět 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 (šifrovou abecedu) a postup řešení. Rozhodněte, co je neobvyklé na získaném otevřeném textu, a jaké to může mít důsledky (co to ovlivní)? Upřesněte, jaká šifra byla použita.

   ```
   RUBLFGSGSILFTSLFGZOOSRHGLIBSZWSZWZXSZNKRLMGLHGZMWFKULIRGGLHSLDZWLFYGRMTDLIOWGSZGZXSR
   OWXZMGSRMPZMWKLHHRYOBWLRGKIZXGRXZOOBBLFDLFOWMGXLMHGZMGOBIFMZXILHHULOPHGLWZBDSLXOZRNG
   SZGZXSROWWLMGPMLDZMBGSRMTZXSROWHYIZRMHGZIGHUFMXGRLMRMTZGYRIGSZMWSZHZNLMTHGRGHNZMBRMU
   ZMGXLMELOFGRLMHGSLFHZMWHLUWLINZMGZGLNHRMGLDSRXSTLWSZHKFGZNBHGRXKLHHRYRORGBULIMLGRXRM
   TZMZWFOGHZXGZMWURTFIRMTLFGRGHKFIKLIG
   ```

3. (2 body) Následující šifrový text vznikl Vigenerovou šifrou pomocí klíče o délce nejvýše 6 znaků. Kromě získaného otevřeného textu uveďte klíč použitý jak pro dešifrování tak pro šifrování a postup řešení. Přípustná abeceda je anglická abeceda bez mezery. Použijte index koincicence a/nebo Kasiského test.

   ```
   HMHLTBTQMUZOJWYEUHSVTCHEUOCGGBODRDTQKGVLOBROKRPFQOSDYQSDRZPQMSOWNSNRTJPQZWZQGZHLYRZP
   XSRDXRTQMKSDZWDDIVTHBOMOKOYGYVPKGRLPKGDDMSQRXOYBECFQMGEHXGHKUATJNHHLYVERLCWOUKTQNSCI
   UCEVZSAVGBODOAQRXGFFISDVUBMRZVDNOGLQJGYRCPZDXRORCVLWKJPUECFZGBEVNSDDORTIECFZGBEWUQSR
   ```

UGPMAGERTSEKKBNKUCDHPIDWUBPLCOYWKRERIVZRYSMRZVLQJOWRZCQSKCAOKHZOJAPWNOELZGYRZDZVYWMO
KHZJKHERZVPWUDTQHCEKUPGLUIDOEWEVTCEHGGJLZGLJXSLWZVTQMHSDZWNDTPPKKFPLTPZWNGARXHDDTRPQ
PCJEUHSVVCCWYVPUKWYWNSCHVIMOOQZIQCCHGAJSROYLYHZVZOJZOHSPEVPDXHDRLCCQUKTWNWYNOKTORRZE
UHSEKQLXYSTOUJPEUHSDTRTOUJPWURZWNWDVNSLGJSO

4. (3 body) 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 $M = (m_1, m_2, ..., m_n)$ je otevřený text, který se skládá ze sekvence n bajtů. Nechť $K = (k_1, k_2, ..., k_n)$ je klíč skládající se opět z n bajtů. A jak je obvyklé, n bajtová sekvence $C = (c_1, c_2, ..., c_n)$ je šifrový text získaný „*xor*-ováním“ každého bajtu otevřeného textu s odpovídajícím bajtem klíče $c_i = m_i \oplus k_i$, pro $i = 1, 2, ..., n$. Pokud budeme mít více než jeden otevřený text, budeme tyto označovat jako $M_1, M_2, ..., M_k$ a bajty OT jako M_j jako m_{ji}, a to $M_j = (m_{j1}, ..., m_{jn})$; 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 SMYSLUPLNÉ 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.

   $C_1 =$ `3c 05 02 1d 07 0c 0c 1a 18 0c 1d 17`
   $C_2 =$ `03 19 11 10 01 00 0f 19 03 1a 11 0a`

5. (2 body) 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.

   IVCTIARJLNKEKCKRNICIDIVAMISVHWEIPIEIANBMOMDTLRRAKIEMTMNOYSNAMEZETOUDGUDTAMCSIOJZUCAB
   UETANKNSENEFMDIOAJPRCLSCVCDUCPOENPOZNEHSONIPUDOMEAHYEIAPUUSOMTNINRNBOAIIOAIINTAKCZHN
   ACVCKAVSLPJOTREOIAESJHCKAORDUIAOADWDIAZANNSNDCJQLEISJDERZIAMAISDECITOJZVONTOCSVCOJST
   MAAIPIAEYPONEMTESEYKDEEDAJHNODHZIFAEMOYJBPLNKINEULNKYNZLMRRIOTVTDEEEIAEIDLHAMTAEEAJZ
   AIYAAAHCINANEMTAPIVCIZNSLEIPJPOAAEILOCOIRAOVVTYTEJLNASJYNRAOLAHILPEDTIFOMSAVECIINASI
   EACSNDTEKSTIEACHOOTNVOEIZCCHSLSHVAZYZDANRFLHSKOPYSLREAXKPNGNNKRNYRVEIACZNIEIMTETATAP
   EMLMNSDIUCAOEPKZFNDKTAUCZTUNIEACYIUQ