KPB

Ostrava 2022 **Vojtěch Prokop**

2. zápočtový úkol

KPB

Vedoucí práce: RNDr. Eliška Ochodková, Ph.D

Vypracoval: Vojtěch Prokop

Studijní obor: IVT

OBSAH

ÚKOL Č. 1

1.1 Zadání

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
```

1.2 Použité instrumenty

- Python
    - Frekvence n-gramu
    - Chi

1.3 Řešení

Implementoval jsem pomocné funkce na zobrazení statistik v textu a pomocí nich postupně tvořil klíč, reprezentující správnou substituci. Pomocné metody vypisovaly počet n-gramu.

	Current	Ref
0	(E, 11.795)	(E, 12.1)
1	(O, 8.718)	(T, 8.94)
2	(V, 8.718)	(A, 8.55)
3	(J, 8.59)	(O, 7.47)
4	(R, 8.59)	(I, 7.33)
5	(Q, 7.949)	(N, 7.17)
6	(G, 6.026)	(S, 6.73)
7	(K, 5.897)	(R, 6.33)
8	(P, 5.256)	(H, 4.96)
9	(C, 4.103)	(L, 4.21)
10	(D, 3.462)	(D, 3.87)
11	(N, 3.077)	(C, 3.16)
12	(L, 2.821)	(U, 2.68)
13	(T, 2.051)	(M, 2.53)
14	(A, 2.051)	(F, 2.18)
15	(W, 2.051)	(G, 2.09)
16	(S, 1.923)	(P, 2.07)
17	(F, 1.795)	(W, 1.83)
18	(U, 1.282)	(Y, 1.72)
19	(B, 1.282)	(B, 1.6)
20	(Y, 0.897)	(V, 1.06)
21	(I, 0.769)	(K, 0.81)
22	(H, 0.513)	(J, 0.22)
23	(I, 0.128)	(X, 0.19)
24	(M, 0.128)	(Z, 0.11)
25	(Z, 0.128)	(Q, 0.1)

	Current	Ref
0	(RGE, 2.057)	(THE, 1.81)
1	(OJR, 1.285)	(AND, 0.73)
2	(VJC, 0.771)	(ING, 0.72)
3	(VOJ, 0.771)	(ENT, 0.42)
4	(EQK, 0.643)	(ION, 0.42)
...	...	...
566	(JOJ, 0.129)	(-, 0)
567	(OJH, 0.129)	(-, 0)
568	(JHV, 0.129)	(-, 0)
569	(QEL, 0.129)	(-, 0)
570	(ELP, 0.129)	(-, 0)

571 rows × 2 columns

Postupně jsem se pokoušel nahrazovat jednotlivé znaky, a tak jsem dospěl k dešifrování. Slovník, v kterém jsem udržoval překlady jsem postupně obohacoval o komentáře, které krátce popisují, jak jsem postupoval. V prvním kroku substituce jsem vycházel z frekvenční analýzy (trigramy). Nahrazení znaků z trigramu THE. Následně jsem podobné kroky aplikovat pro monogramy společně s statistickou metodou chí-kvadrát testu.

```
key = {
    #prvni substituce
    "R": "T",
    "G": "H",
    "E": "E",
    "O": "I",
    "J": "N",
    "V": "A",
    #tree?
    "P": "R",
    #test chi
    "Q": 'S',
    "N": "C",
    "G": "H",
    "O": "I",
    "M": "Q",
    "S": "U",
    #TE_HNI__E, R E N G J O M S E T ... T E C H N I Q U E
    #C_EAR  NDEVP,
    "D": "L",
    #LI_HT__ LIGHT?
    "A": "G",
    #_RINTS .. PRINTS? LPOJRQ
    "L": "P",
    #_APANESEPRINTS .. JAPANESE?
    #HVLVJEQELPOJRQ
    "H": "J",
    #WORGCOVAKJVD
    #_ITH_IAG_NAL
    "W": "W",
    "C": "D",
    "K": "O",
    #OJRGEQKTR
    #INTHESO_T,
    "T": "F",
    #OJRGEQKTRNDEVPDOAGRKTLPKUEJNE
    #INTHESOFTCLEARLIGHTOFPRO_ENCE
    "U": "V",
    #GEWVQTSDDY
    #HEWASFULL_,
    "Y": "Y",
    #RPVOJTPKFLVPOQ
    #TRAINFRO_PARIS
    "F": "M",
    #RRGEOFLVNRWVQFKPEQSIRDEFKPEISPOEC
    #TTHEIMPACTWASMORESU_TLEMORE_URIED
    "I": "L",
    #GKPOZKJRVD
    #HORI_ONTAL
```

Po pár těchto pokusech jsem si napsal pomocnou metodu, která vypsala řetězec v podobě, kde neznámé byly nahrazeny znakem _.

```
'INTHESOFTCLEARLIGHTOFPRO_ENCEFRANCE_INCENT_ANGOGHSAWTHECRISPS_IESOFJAPANESEWOODCUTPRINTSTHEAL_OND_LOSSO_SGNARLEDTREESANDIRISESTHATDOTTEDTHEFRENCHLANDSCAPERE_INDEDHI_OFNATURESCENE
SPAINTEDIN__OTOANDINTHELOCALSWHODRAN_INCAFESOFARLESHESAWRESONANCESWITHTHEGEISHASAND_A_U_IACTORSOFACOUNTR_HEDNE_ER_ISITEDATFIRST_ANGOGHSI_PL_COPIEDTHEWOR_SIN_OTHS_ETCHESANDOILPAINT
INGS__THETI_ETHEARTIST_O_EDTOARLESHEWASFULL_INTHETHRALLOFJAPANONTHETRAINFRO_PARISHEREPEATEDL_CHEC_EDOUTTHEWINDOWHEWROTETOHISFRIENDPAULGAUGUINTOSEEIFITWASLI_EJAPAN_ET_CHILDISHISNTI
TTHEI_PACTWAS_ORESU_TLE_ORE_URIEDINHISTECHNIQUEFORINSTANCEHESO_ETI_ESDI_IDEDTHECAN_ASUSINGDIAGONALLINESRATHERTHANUSINGHORI_ONTALPERSPECTI_EPLANESASWASTHENOR_INWESTERNPAINTINGANDHE
WOULDSTREA_HISPAINTINGSWITHDIAGONALRAINASHEHADSEENINJAPANESEPRINTS'
```

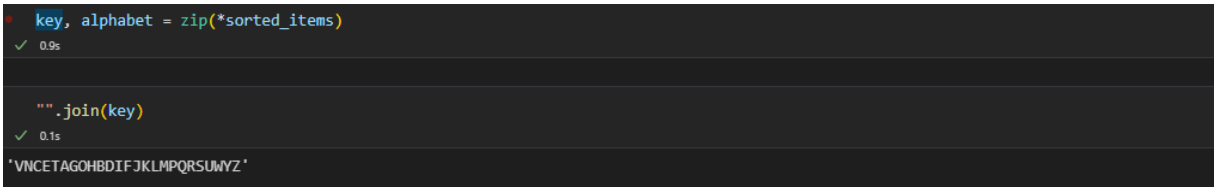
V takto zkonstruovaném řetězci jsem vždycky našel kus anglického slova, který mohl být doplněn. Z komentářů tyto slova lze pozorovat. Tree, Technique, Prints, With Diagonal, Provence, Fully, From, Horizontal..

1.4 Dešifrovaný text

INTHESOFTCLEARLIGHTOFPROVENCEFRANCEVINCENTVANGOGHSAWTHECRI
SPSKIESOFJAPANESEWOODCUTPRINTSTHEALMONDLLOSSOMSGNARLEDTREE
SANDIRISESTHATDOTTEDTHEFRENCHLANDSCAPEREMINDEDHIMOFNATURES
CENESPAINTEDINKYOTOANDINTHELOCALSWHODRANKINCAFESOFARLESHES
AWRESONANCESWITHTHEGEISHASANDKALUKIACTORSOFACOUNTRYHEDNE
VERVISITEDATFIRSTVANGOGHSIMPLYCOPIEDTHEWORKSINLOTHSKETCHESA
NDOILPAINTINGSLYTHETIMETHEARTISTMOVEDTOARLESHEWASFULLYINTHE
THRALLOFJAPANONTHETRAINFROMPARISHEREPEATEDLYCHECKEDOUTTHE
WINDOWHEWROTETOHISFRIENDPAULGAUGUINTOSEEIFITWASLIKEJAPANYET
_CHILDISHISNTITTHEIMPACTWASMORESULTLEMORELURIEDINHISTECHNIQU
EFORINSTANCEHESOMETIMESDIVIDEDTHECANVASUSINGDIAGONALLINESRA
THERTHANUSINGHORIZONTALPERSPECTIVEPLANESASWASTHENORMINWEST
ERNPAINTINGANDHEWOULDSTREAKHISPAINTINGSWITHDIAGONALRAINASHE
HADSEENINJAPANESEPRINTS

1.5 Odpovědi

Klíč = **VINCETAGOHBDFJKLMPQRSUWYZ**



ÚKOL Č. 2

1.6 Zadání

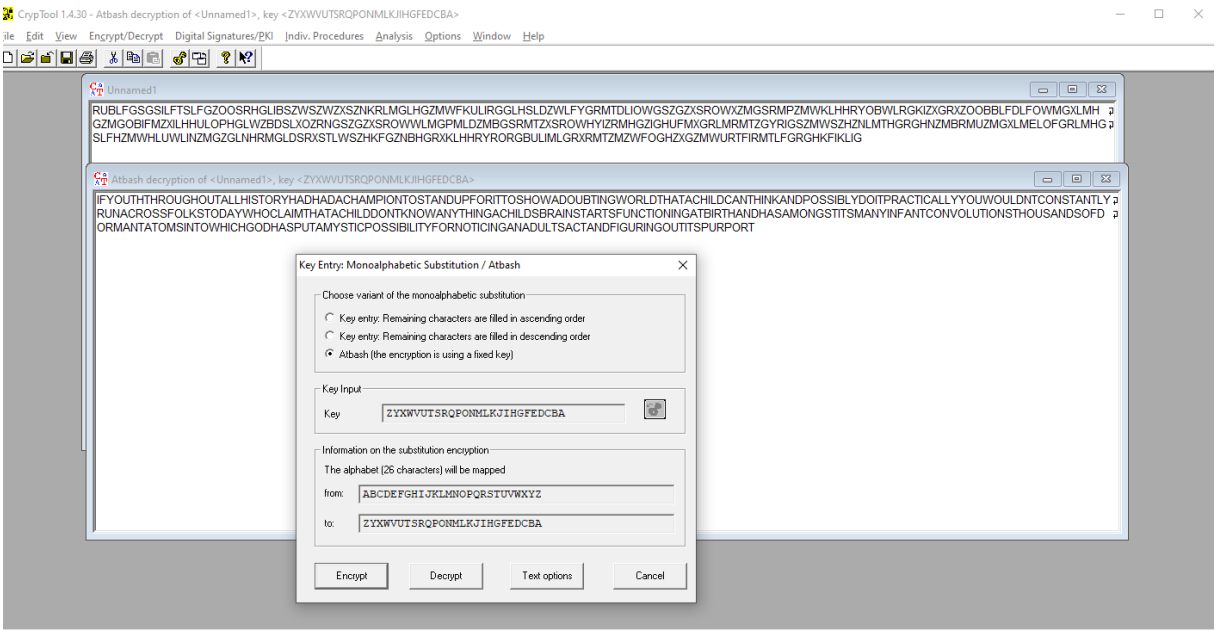
2. (3 body) Následující šifrový text opět vznikl obecnou monoalafabetickou substitucí z anglického textu, otevřená i šifrová abeceda jsou anglická abeceda bez mezery. Dešifrujte jej a kromě otevřeného textu uveďte použitý klíč (šifrovou abecedu) a postup řešení. Rozhodněte, co je neobvyklé na získaném otevřeném textu, a jaké to může mít důsledky (co to ovlivní)? Upřesněte, jaká šifra byla použita.

```
RUBLFGSGSILFTSLFGZOOSRHGLIBSZWSZWZXSZNKRLMGLHGZMWFKULIRGGLHSLDZWLFYGRMTDLIOWGSZGZXSR
OWXZMGSRMPZMWKLHHRYOBWLRGKIZXGRXZOOBBLFDLFOWMGXLMHGZMGOBIFMZXILHHULOPHGLWZBDSLXOZRNG
SZGZXSROWWLMGPMLDZMBGSRMTZXSROWHYIZRMHGZIGHUFMXGRLMRMTZGYRIGSZMWSZHZNLMTHGRGHNZMBRMU
ZMGXLMELOFGRLMHGSLFHZMWHLUWLINZMGZGLNHRMGLDSRXSTLWSZHKFGZNBHGRXKLHHRYRORGBULIMLGRXRM
TZMZWFOGHZXGZMWURTFIRMTLFGRGHKFIKLIG
```

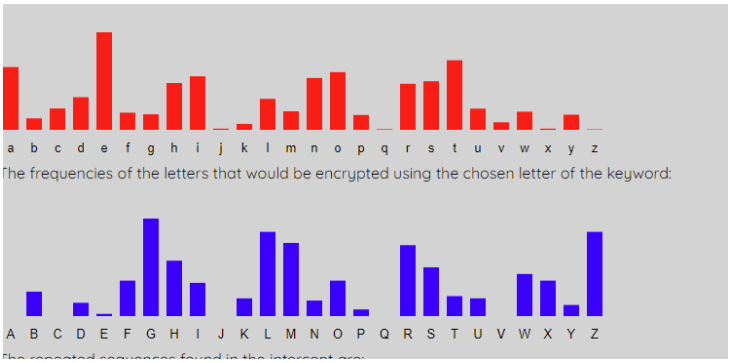
1.7 Použité instrumenty

- Python
- CryptTool
- https://crypto.interactive-maths.com/kasiski-analysis-breaking-the-code.html

1.8 Řešení



V druhém úkolu byl využit **CrypTool**, který po správném nastavení dešifroval text. Prvně byl pokus o stejný přístup jako v prvním příkladě, ale bohužel se nepovedlo moc dobře pokročit pomocí frekvenční analýzy.



1.9 Šifrovaný text

RUBLFGSGSILFTSLFGZOOSRHGLIBSZWSZWZXSZNKRLMGLHGZMWFKULIRGG
LHSLDZWLFYGRMTDLIOWGSZGZXSROWXZMGSRMPZMWKLHHRYOBWLRGKI
ZXGRXZOOBBLFDLFOWMGXLMHGZMGOBIFMZXILHHULOPHGLWZBDSLXOZR
NGSZGZXSROWWLMGPMLDZMBGSRMTZXSROWHYIZRMHGZIGHUFMXGRLMR
MTZGYRIGSZMWSZHZNLMTHGRGHNZMBRMUZMGXLMELOFGRLMHGSLFHZM
WHLUWLINZMGZGLNHRMGLDSRXSTLWSZHKFGZNBHGRXKLHHRYRORGBULI
MLGRXRMTZMZWFOGHZXGZMWURTFIRMTLFGRGHKFIKLIG

1.10 Dešifrovaný text

IF YOUTH THROUGHOUT ALL HISTORY HAD HAD A CHAMPION TO STANDUP FOR IT TO SHOW A DOUBTING WORLD THAT A CHILD CAN THINK AND POSSIBLY DO IT PRACTICALLY YOU WOULDNT CONSTANTLY RUN ACROSS FOLKS TODAY WHO CLAIM THAT A CHILD DONT KNOW ANYTHING A CHILDS BRAIN STARTS FUNCTIONING AT BIRTH AND HAS AMONGST ITS MANY INFANT CONVOLUTIONS THOUSANDS OF DORMANT ATOMS INTO WHICH GOD HAS PUT A MYSTIC POSSIBILITY FOR NOTICING AN ADULTS ACT AND FIGURING OUT ITS PURPORT

1.11 Odpovědí

- Nemá obvyklou distribuci znaků.
- Klič = **ZYXWVUTSRQPONMLKJIHGFEDCBA**

ÚKOL Č. 3

1.12 Zadání

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.

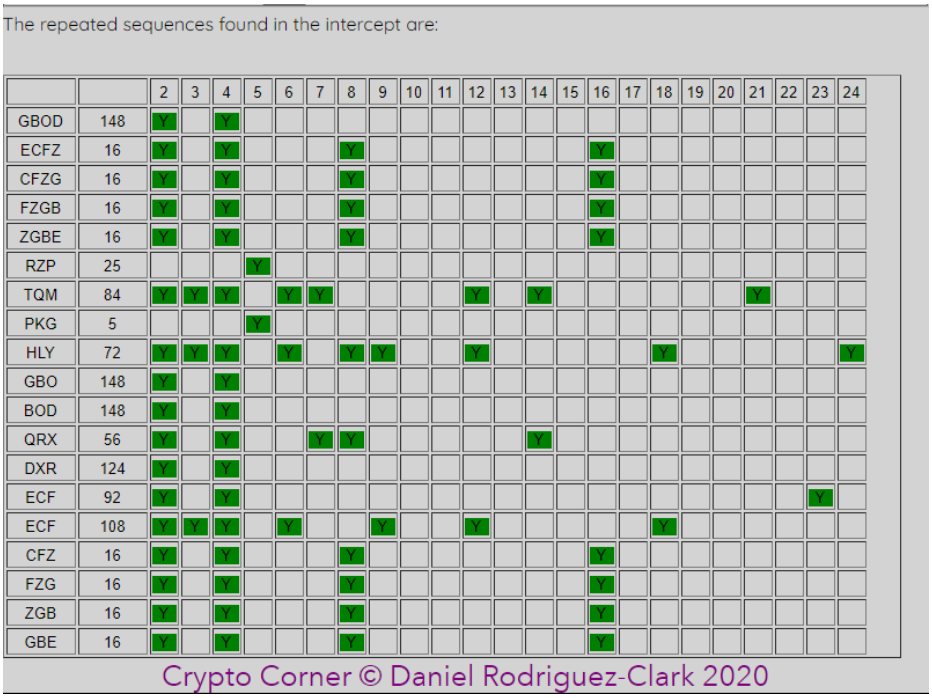
```
HMHLTBTQMUZOJWYEUHSVTCHEUOCGGBODRDTQKGVLOBROKRPFQOSDYQSDRZPQMSOWNSNRTJPQZWZQGZHLYRZP
XSRDXRTQMKSDZWDDIVTHBOMOKOYGYVPKGRLPKGDDMSQRXOYBECFQMGEHXGHKUATJNHHLYVERLCWOUKTQNSCI
UCEVZSAVGBODOAQRXGFFISDVUBMRZVDNOGLQJGYRCPZDXRORCVLWKJPUECFZGBEVNSDDORTIECFZGBEWUQSR
```

1.13 Použité instrumenty

- https://crypto.interactive-maths.com/kasiski-analysis-breaking-the-code.html
- CryptoTool

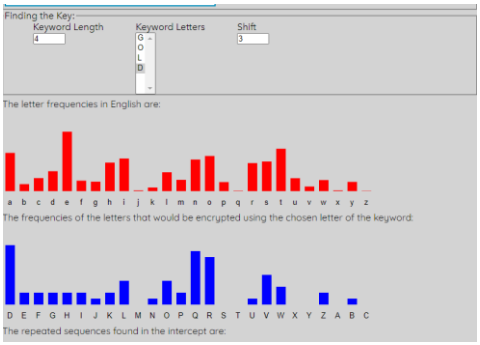
1.14 Řešení

V prvním kroku byl využit online nástroj, který pomocí Kasiského testu provedl analýzu a vizualizoval vzdálenost výskytu daného n-gramu společně s děliteli. Jelikož jsem věděl, že klíč na šifrování je velikost méně jak 6, pak jsme mohli odhadnout, že klíč bude 2 nebo 4.

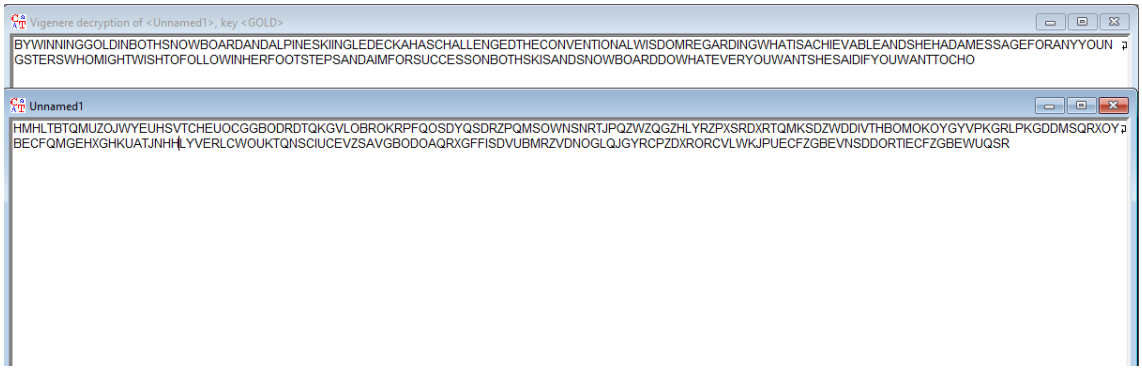


		2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
GBOD	148	Y		Y																				
ECFZ	16	Y		Y				Y								Y								
CFZG	16	Y		Y				Y								Y								
FZGB	16	Y		Y				Y								Y								
ZGBE	16	Y		Y				Y								Y								
RZP	25				Y																			
TQM	84	Y	Y	Y		Y	Y					Y		Y							Y			
PKG	5				Y																			
HLY	72	Y	Y	Y		Y		Y	Y			Y						Y						Y
GBO	148	Y		Y																				
BOD	148	Y		Y																				
QRX	56	Y		Y			Y	Y						Y										
DXR	124	Y		Y																				
ECF	92	Y		Y																			Y	
ECF	108	Y	Y	Y		Y			Y			Y						Y						
CFZ	16	Y		Y				Y								Y								
FZG	16	Y		Y				Y								Y								
ZGB	16	Y		Y				Y								Y								
GBE	16	Y		Y				Y								Y								

Po rozdělení celistvého textu na 4 sloupce jsem byl schopen provést frekvenční analýzu s mapováním na anglický text, díky kterého jsem odhadl klíč.



Po uhodnutém klíči na dešifrování jsem využil CryptoTool nástroj, dle kterého jsem si vygeneroval otevřený text. Tento text jsem obohatil o mezery.



1.14.1 Dešifrovaný text

BYWINNINGGOLDINBOTHSNOWBOARDANDALPINESKIINGLEDECKAHASCHAL
LENGEDTHECONVENTIONALWISDOMREGARDINGWHATISACHIEVABLEANDSH
EHADAMESSAGEFORANYYOUNGSTERSWHOMIGHTWISHTOFOLLOWINHERFOO
TSTEPSANDAIMFORSUCCESSONBOTHSKISANDSNOWBOARDDOWHATEVERYO
UWANTSHESAIDIFYOUWANTTOCHOOSEJUSTONETHENCHOOSEJUSTONEIWAN
TEDTOCHOOSEBOTHANDALOTOFPEOPLETOLDMETHATITSNOTPOSSIBLETOGE
TTOTHETOPINBOTHOBVIOUSLYITSNOTEASYITSAGREATTHINGTHATICANBEH
EREINBOTHSPORTSANDENJOYBOTHSPORTSHEREINTHEREPUBLICOFKOREAM
YPLANISTOSTAYWITHMYHEARTSOFORNOWITHINKIWILLDOBOTHBECAUSEIL
OVEBOTHANDILOVETODOTHISSHEADDED

1.14.2 Dešifrovaný text s mezerami

BY WINNING GOLD IN BOTH SNOWBOARD AND ALPINE SKIING LEDECKA HAS CHALLENGED THE CONVENTIONAL WISDOM REGARDING WHAT IS ACHIEVABLE AND SHE HAD A MESSAGE FOR ANY YOUNGSTERS WHO MIGHT WISH TO FOLLOW IN HER FOOTSTEPS AND AIM FOR SUCCESS ON BOTH SKIS AND SNOWBOARD DO WHATEVER YOU WANT SHE SAID IF YOU WANT TO CHOOSE JUST ONE THEN CHOOSE JUST ONE I WANTED TO CHOOSE BOTH AND A LOT OF PEOPLE TOLD ME THAT ITS NOT POSSIBLE TO GET TO THE TOP IN BOTH OBVIOUSLY ITS NOT EASY ITS A GREAT THING THAT I CAN BE HERE IN BOTH SPORTS AND ENJOY BOTH SPORTS HERE IN THE REPUBLIC OF KOREA MY PLAN IS TO STAY WITH MY HEART SO FOR NO WITH INKI WILL DO BOTH BECAUSE I LOVE BOTH AND I LOVE TO DO THIS SHEADDED

1.15 Odpovědi

- Velikost klíče jsou 4 znaky.
- Klíč na šifrování a dešifrování je GOLD.

ÚKOL Č. 4

1.16 Zadání

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`

1.17 Použité instrumenty

- https://isaaccomputerscience.org/concepts/data_encrypt_vernam?examBoard=all&stage=all
- https://cs.wikipedia.org/wiki/Vernamova_%C5%A1ifra

1.18 Řešení

Binární varianta je obzvláště citlivá na opakované použití klíče. Důvodem je následující vlastnost operace XOR: $(A \oplus X) \oplus (B \oplus X) = A \oplus B$. Když má tedy útočník v ruce dvě zprávy šifrované týmž klíčem a provede s nimi XOR, dostane XOR dvou původních zpráv a zbaví se veškeré náhodnosti, která spočívala v klíči a která dává šifře její sílu. Statistická kryptoanalýza mu pak už docela lehce umožní zprávy přečíst.

Předpokládáme, že pokud by byly klíče různé, pak bychom neměli možnost rozluštit šifrované zprávy. Respektive bychom mohli možná aplikovat přístup, kdy bychom zkoušeli různý klíč pro šifrovanou zprávu a pokud by bylo slovo ze slovníku, pak bychom si ho uložili. Přesto si ale myslím že nebudeme mít jistotu správného dešifrování. Jelikož tato operace nám bude moci vyprodukovat více správných slov z dodaného slovníku.

Předpokládejme tedy, že po provedení XOR mezi C1 a C2 dostaneme XOR mezi originálními zprávami. Na tomhle můžeme provést pokus o dešifrování.

- Provedení XOR mezi C1 a C2.
- Načtení slovníku.
- Vyfiltrování slovníku, 12 znaků dlouhé slova.
- Iterace přes všechny tyto slova, přičemž využijeme doplněk k získání znaku pro msg2_j. Pokud nezůstáváme v povolené abecedě otevřeného textu přeskakujeme a zkoušíme další slovo.
- Pokud zůstaneme v abecedě pro všech 12 znaků, pak testujeme, zda slovo existuje v definovaném slovníku.
- Pokud ano máme řešení.
- Z výsledných dvou slov získáme klíč pomocí C1 ^ msg1 a analogicky pro C2.

1.19 Odpověďi

- M1 = **Lichtenstein**
- M2 = **superimposes**
- Klíč = **plausibility**

ÚKOL Č. 5

1.20 Zadání

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

1.21 Použité instrumenty

- https://tholman.com/other/transposition/

1.22 Řešení

- Implementace metody, která vytvoří matici vzhledem k velikosti klíče.
    - Klíč definuje počet sloupců.
- Text je rozdělen na segmenty, tak aby šel vložit to matice o n sloupcích.
- Segmenty textu byly vloženy do matice.
- Sloupce byly přehazovány, tak aby bylo zajištěno bezpečnější šifrovací mechanismus.
- Implementoval jsem metodu, která vytvořila všechny možné permutace vzhledem k přehození sloupců, a tyto texty explicitně procházel a zkoušel najít text, který bude v mateřském jazyce.
- K tomuto otevřenému textu byl následně nalezena šifrovací permutace. Podobným způsobem jako u dešifrování ale převrácený postup. Uložil jsem si permutaci, která generovala text rovný s šifrovým textem.

1.23 Dešifrovaný text

LIDE VE VLACICH CD STAHUJI MOC DAT OPERATOR JE NELZEVNI NAOPAK JE O MEZI ZAKAZNICI CESKYCH DRAH SE NA SOCIALNICH SITICH PODIVUJI NAD ZVAZOVANYM OMEZENIM DAT STAHOVANYCH PŘES WIFI VE VLACICH POPISUJI ZKUSENOSTI S POMALYM A NESTABILNIM PRIPOJENIM PARADOX NE TAK BYLA POPRENA ORIGINALNI EKONOMICKA TEORIE MINISTRYNE MARTY NOVAKOVE KDY VI CESTA ZENYCH DAT ZNAMENA JEJICH ZLEVNENI CO TAM KDO STAHUJE VZDYT SIGNAL FURT PADA A JE TO POMALE TO MAM RYCHLEJSI MOBILNI POPSAL JEDEN Z DISKUTUJICICH NA FACEBOOKU UMEALE SPONTAKRKA VŽDY NEFUNKCNI ZNIDALSIKOMENTARNAADRESU WIFICDO MEZITDATAVICUZ TO SNAD ANI NEJDE NEPTA SE RECNICKY DAL SI CESTUJICI **QQ**

1.24 Odpovědi

- Šifrovací permutace - **14023**
- Dešifrovací permutace - **20341**