KSI 2012/2013
Úloha 4-1: Římská

Jan Horáček
Gymnázium, Brno, Vídeňská 47; jan.horacek@seznam.cz

24. března 2013

1 Řešení

1.1 1. část

Řešení jsem získal posunutím celého textu o 11 písmen v Caesarově abecedě.

GRATULUJEM TI PRAVE SA TI PODARILO DE
SIFROVAT TEXT ZASIFROVANY PODLA CEA
AROVEJ SIFRY S POSUNUTIM O JEDENAST
PISMEN TATO SIFRA BOLA POUZIVANA GAI
OM JULIOM CEASAROM V DOBACH RIMSKEJ R
ISE TERAZ SA POSUNIEME V NASEJ HISTOR
ICKEJ PUTI SIFRAMI TROCHU DALEJ TERA
Z TA CAKA ALBERTIHO SIFRA PODLA POLYH
ISTORA LEONA BATTIS TU ALBERTIHO KLU
C K DESIFROVANIU JE FI TEDA SKRATKA OD
FAKULTA INFORMATIKY PREDTYM AKO SA A
LE PUSTIS DO ALBERTIHO SIFRY NEZABUD
NI DESIFROVAT AJ ZVYSOK TEXTU CEASAR
OVOUSIFROU

1.2 2. část

Podle nápovědy v 1. části jsem získal řešení Albertiho šifry zapomocí klíče "FI" a následného posunutí v Caesarově abecedě o 11 znaků. (Takže vlastně zapomocí klíče "QT")

PRAVE SI DESIFROVAL ALBERTIHO SIFRU
A CAKA TA JEDNA Z NAJTAZSICH SUBSTITU
CNYCH SIFIER V POSLEDNEJ CASTI TA CAK
A VIGENEROVA SIFRA ABY SI TO ALE NEMAL
AZ TAKE TAZKE PREZRADIM TI ZE DO SIFRY
SA MI OMYLOM PODARILO ZANIEST CHYBU P
RI FREKVENCNEJ ANALIZE I JU URCITE VS

IMNES VIAC TI UZ NEPREZRADIM ZELAM TI
VELA STASTIA A PEVNE NERVY A NEZABUDN
I OPAT ZVYSOK SIFRY DESIFROVAT ALBER
TIHO SIFROU

1.3 3. část

3. část se mi bohužel nepodařilo dešifrovat.

Mé úvahy vedly přes řešení zapomocí zjištění opakujících se frází a zapomocí frekvenční analýzy, která je podle mě jediným způsobem, kterým lze Vigenèrovu šifru vyřešit. Bohužel, tento postup se ukázal býti neúspěšným, neboť, jak již řešení 2. částí napovídá, klíčem nebude "normální"slovo, nýbrž nějaká obskurnost. Proto nelze zjistit klíč pomocí frekvenční analýzy.

Reference

[1] Wikipedia *Vigenèrova šifra*
http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

[2] Marian Klang *Vigenèrova šifra - dešifrování bez znalosti klíče*
https://akela.mendelu.cz/ foltynek/KAS/historie/vigenere2.php