Tema 6 – Criptografie

Problema 1 :

Pentru a decripta un text criptat folosind cifrul lui Cezar, trebuie să determinăm mai întâi valoarea de deplasare utilizată pentru criptare. Textul criptat este folosit într-un alfabet extins, care include literele majuscule și minuscule, cifrele, și câteva caractere speciale, formând un total de 77 de caractere:

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789():; .,!?-'

Pentru a sparge cifrul Cezar, putem utiliza abordarea descrisă în seminarul 6, care implică analiza frecvențelor literelor din textul criptat comparativ cu frecvențele tipice ale literelor în limba română.

Pentru a sparge cifrul Cezar pentru textul tău, putem utiliza abordarea descrisă în seminarul 6, care implică analiza frecvențelor literelor din textul criptat comparativ cu frecvențele tipice ale literelor în limba română.

De obicei, în limba română, cele mai frecvente litere sunt "e", "a", și "i". Pentru a simplifica procesul de spargere, putem presupune că litera cea mai frecventă în textul criptat ar trebui să corespundă cu "e" (sau altă literă frecventă) în limba română.

Vom analiza frecvențele literelor în textul criptat, le vom ordona, și vom încerca să aliniem cea mai frecventă literă criptată cu "e" pentru a determina deplasarea posibilă.

Cele mai frecvente caractere din textul criptat sunt 'z', 'L', 'P', 'T', și 'f', ordonate după frecvență. Dacă presupunem că litera 'e', fiind una dintre cele mai frecvente în limba română, ar trebui să corespundă cu una dintre acestea, putem încerca să decriptăm textul aliniind aceste litere cu 'e' și să vedem dacă rezultatul este coerent.

Să încercăm să decriptăm textul folosind deplasări care aliniază 'z', 'L', 'P', 'T', și 'f' cu 'e'. Vom calcula aceste deplasări și vom afișa rezultatele: ​​

Am decriptat textul pentru cateva cazuri. Iată rezultatele pentru primele 200 de caractere din fiecare decriptare:

* github frecventa.cpp

1. Deplasarea 21 (aliniază 'z' cu 'e'):

pH)eE )J)eEeLKBF.eL-;B.)D)ge;)eJE)J.eLKBF-B.fep)eKC:B)I.eEeDE)FJ.e-DJH.)!)e KF)e?H)D)eI-eDKe!)I-I.eD-;)-H-feq);)D KjI.eP-K)e)B:)geLKBF.)e-.I.eB)eC)H!-D.)e HKCKBK-eI-eI.e;KB;)eIK:eEeJK,)ge!)D -D KjI.e; etc…

(neclar și neregulat)

1. Deplasarea 54 (aliniază 'L' cu 'e'):

Ive?shexe?s?zypti?zmgpiere'?ge?xsexi?zyptmpi-?Ie?yqfpewi?s?rsetxi?mrxvieke?hyte?lvere?wm?ry?kewmwi?rmgemvm-?JegerhyCwi?3mye?epfe'?zyptie?miwi?pe?qevkmrie?hvyqypym?wm?wi?gypge?wyf?s?xyje'?kerhmrhyCwi?g etc…

(neclar și neregulat)

1. Deplasarea 58 (aliniază 'P' cu 'e'):

Era odată o vulpe vicleană, ca toate vulpile. Ea umblase o noapte întreagă după hrană și nu găsise nicăieri. Făcându-se ziua albă, vulpea iese la marginea drumului și se culcă sub o tufă, gândindu-se ce să mai facă, ca să poată găsi ceva de mâncare. Șezând vulpea cu botul întins pe labele de dinainte, îi vine miros de pește. Atunci ea ridică puțin capul și, uitându-se la vale, în lungul drumului, zărește venind un car tras de boi. -Bun! gândi vulpea. Iaca hrana ce-o așteptam eu. Și îndată iese de sub tufă și se lungește în mijlocul drumului, ca și cum ar fi fost moartă. Carul apropiindu-se de vulpe, țăranul ce mâna boii o vede și, crezând că-i moartă cu adevărat, strigă la boi: Aho! Aho! Boii se opresc. Țăranul vine spre vulpe, se uită la ea de aproape și, văzând că nici nu suflă, zice: -Bre! da cum naiba a murit vulpea asta aici?! Ti!... ce frumoasă câtaveica am să fac nevestei mele din blana istui vulpoi! Zicând așa, apucă vulpea de după cap și, târând-o până la car, se opintește s-o arunce deasupra peștelui. Apoi strigă la boi: Haiș! Joian, cea! Bourean.

Problema 2 :

Criptarea afină pe blocuri de lungime 1 este o formă a criptării afine, unde fiecare caracter este criptat folosind o funcție matematică liniară de forma:

# c=(a×m+b)modN

unde:

c este caracterul criptat,

m este caracterul în clar,

a și b sunt cheile de criptare,

N este mărimea alfabetului.

# m=a ^−1 ×(c−b)modN

Pentru a decripta textul folosind criptarea afină pe blocuri de lungime 1, vom aplica aceeași metodă, luând în considerare cheia de criptare și funcțiile prezentate în seminarul 6.

Pasul 1: Inițializare

Definim funcțiile de modulo și invers necesare pentru decriptare.

Obținem textul criptat.

Pasul 2: Decriptare

Folosind cheia de criptare și funcțiile definite anterior, decriptăm fiecare bloc de caractere din textul criptat.

Obținem textul decriptat.

* Github p2.cpp

Problema 3 :

Pentru a decripta textul folosind criptarea afină pe blocuri de lungime 2, trebuie să avem cheile de criptare sau să determinăm aceste chei pe baza unor presupuneri sau analize a frecvențelor bigramelor (perechi de caractere). Acest tip de criptare afină se bazează pe relația matematică:

# C=(aM+b)modN

unde:

C este vectorul de caractere criptate (bigramele criptate).

M este vectorul de caractere originale (bigramele originale).

a și b sunt matrici utilizate pentru criptare.

N este numărul total de caractere posibile în alfabet.

* Github p3.cpp