Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică și Microelectronică
Departamentul Calculatoare

RAPORT DE LABORATOR

Criptanaliza cifrurilor monoalfabetice – Laborator 2

Analiză detaliată și proces de decriptare

Disciplina:
Criptografie și Securitatea Datelor

Student:
Bobeica Andrei

Profesor:
Zgureanu A.

Grupa:
FAF-231

Chișinău, 2025

Data: 8 octombrie 2025

Cuprins

Introducere în Criptanaliza Cifrurilor Monoalfabetice

Context teoretic

Cifrul monoalfabetic este una dintre cele mai simple metode de criptare, bazată pe o substituție fixă între literele alfabetului. Fiecare literă din textul clar este înlocuită cu o altă literă, conform unei chei de substituție. Această tehnică a fost folosită încă din antichitate, însă are o vulnerabilitate majoră: distribuția frecvențelor literelor din textul criptat reflectă distribuția limbii naturale, făcând posibilă spargerea sa prin analiză statistică.

Scopul lucrării

Scopul acestui laborator este de a aplica metoda analizei frecvenței pentru a decripta un text criptat printr-un cifru monoalfabetic, fără cunoașterea cheii. Rezultatul final constă în identificarea cheii de substituție și reconstruirea textului clar.

Textul criptat (Varianta 2)

Mesajul criptat

Wqv tooxwxng nc pvhivhf wn wqv witgpcniztwxngp uinodhvohifuwnjituqf. Widv, xw rtp zniv nc t jtzv wqtg tgfwqxgj vspv|xw pndjqwwn ovstf hnzuivqvgpxng cni ngsf wqv pqniwvpw unppxasv wxzv, gnw wqvsngjvpw|tgo wqv hifuwtgtsfpxp rtp, sxlvrxpv, edpw t udmmsv. Vjfuw'p rtpwqdp t bdtpx hifuwnsnjf xg hngwitpw wn wqv ovtosf pvixndp phxvghv nc wnotf.Fvw jivtw wqxgjp qtkv pztss avjxggxgjp, tgo wqvpv qxvinjsfuqp oxoxghsdov, wqndjq xg tg xzuvicvhw ctpqxng, wqv wrn vsvzvgwp nc pvhivhf tgowitgpcniztwxng wqtw hnzuixpv wqv vppvgwxts twwixadwvp nc wqv phxvghv. Tgopn hifuwnsnjf rtp anig. Xg xwp cxipw 3,000 fvtip, xw oxo gnw jinr pwvtoxsf. Hifuwnsnjf tinpvxgovuvgovgwsf xg ztgf usthvp, tgo xg znpw nc wqvz xw oxvo wqv ovtwqp ncxwp hxkxsxmtwxngp. Xg nwqvi usthvp, xw pdikxkvo, vzavoovo xg t sxwvitwdiv,tgo cinz wqxp wqv gvyw jvgvitwxng hndso hsxza wn qxjqvi svkvsp.Adw uinjivpp rtp psnr tgo evilf. Zniv rtp snpw wqtg ivwtxgvo. Zdhq nc wqvqxpwnif nc hifuwnsnjf nc wqxp wxzv xp t utwhqrnil, t hitmf bdxsw ncdgivstwvo xwvzp, puindwxgj, csndixpqxgj, rxwqvixgj. Ngsf wnrtio wqvRvpwvig Ivgtxpptghv onvp wqv thhivwxgj lgnrsvojv avjxg wn adxso du tznzvgwdz. Wqv pwnif nc hifuwnsnjf odixgj wqvpv fvtip xp, xg nwqvi rniop,vythwsf wqv pwnif nc ztglxgo. Hqxgt, wqv ngsf qxjq hxkxsxmtwxng nc tgwxbdxwf wn dpv xovnjituqxhrixwxgj, pvvzp gvkvi wn qtkv ovkvsnuvo zdhq ivts hifuwnjituqf |uviqtup cni wqtw ivtpng. Xg ngv htpv lgnrg cni zxsxwtif udiunpvp, wqv11wq-hvgwdif hnzuxstwxng, Rd-hqxgj wpdgj-ftn ("Vppvgwxtsp cinz ZxsxwtifHstppxhp"), ivhnzzvgovo t widv xc pztss hnov. Wn t sxpw nc 40 ustxgwvywxwvzp, itgjxgj cinz ivbdvpwp cni anrp tgo tiinrp wn wqv ivuniw nc tkxhwnif, wqv hniivpungovgwp rndso tppxjg wqv cxipw 40 xovnjitzp nc tunvz. Wqvg, rqvg t sxvdwvgtgw rxpqvo, cni vytzusv, wn ivbdvpw znivtiinrp, qv rtp wn Rixwv wqv hniivpungoxgj xovnjitz tw t puvhxcxvo usthvng tg nioxgtif oxputwhq tgo pwtzu qxp pvts ng xw.Xg Hqxgt'p jivtw gvxjqani wn wqv rvpw, Xgoxt, rqnpv hxkxsxmtwxngsxl ovkvsnuvo vtisf tgo wn qxjq vpwtwv, pvkvits cnizp nc pvhivwhnzzdgxhtwxngp rviv lgnrg tgo, t Uutivgwsf, uithwxhvo. Wqv Tiwqt-ptpwit, t hstppxh rnil ng pwtwvhitcw twwixadwvo wn Ltdwxsft, xg ovphixaxgjwqv vpuxngtjv pvikxhv nc Xgoxt tp uithwxhtssf ixoosxgj wqv hndgwif rxwqp Uxvp, ivhnzzvgovo wqtw wqv nccxhvip nc wqv xgpwxwdwvp nc £ puxngtjv jxkvwqvxi puxvp wqvxi tppxjgzvgwp af pvhivw rixwxgj.Uviqtup znpw xgwvivpwxgj wn hifuwnsnjxpw tztwvdi niuincvppxngts, xp wqtw Ktwpftftgt'p ctzndp wvywannl nc vinwxhp, wqv Ltztpdwit,sxpwp pvhivw rixwxgj tp ngv nc wqv 64 tiwp, ni fnjtp, wqtw rnzvgpqndso lgnr tgo uithwxhv. Wqv cndiwq jivtw hxkxsxmtwxng nc tgwxbdxwf, wqvZvpnun-wtzxtg, itwqvi utitssvsvo Vjfuw vtisf xg xwp hifuwnjituqxhvknsdwxng, adw wqvg pdiutppvo xw. Wqdp, xg wqv stpw uvixno nc hdgvxcnizrixwxgj, xg hnsnuqngp rixwwvg tw Didl (xg uivpvgw-otf Xitb) dgovi wqvPvsvdhxo lxgjp xg wqv stpw cvr phniv fvtip avcniv wqv Hqixpwxtg vit,nhhtpxngts phixavp hngkviwvo wqvxi gtzvp xgwn gdzavip. Wqvvghxuqvizvgw|xc pdhq xw av|ztf qtkv avvg ngsf cni tzdpvzvgw ni wnpqnr ncc.

Procesul de decriptare

Etapa 1 – Analiza frecvențelor

Primul pas al criptanalizei a constat în calcularea frecvenței fiecărei litere din textul criptat. Rezultatul a fost comparat cu distribuția tipică a limbii engleze (*E, T, A, O, I, N, S, H, R*).

Astfel s-a observat că literele `W, Q, V, X, T` apar frecvent, sugerând corespondente probabile:

$$W \to T, \quad Q \to H, \quad V \to E, \quad X \to A, \quad T \to O$$

După aplicarea acestor substituții inițiale, au apărut primele cuvinte parțial lizibile precum *the*, *of*, *and*.

Etapa 2 – Identificarea tiparelor și trigrame

Prin analiza combinațiilor frecvente de litere (digrame și trigrame), s-au identificat modele tipice limbii engleze precum „th", „he", „an", „ing", „ent". Recunoașterea secvenței „wqv" în repetate rânduri a indicat o corespondență puternică cu „the".

Etapa 3 – Substituția graduală

Decriptarea a continuat prin substituții progresive:

- S-au înlocuit literele corespunzătoare celor mai frecvente apariții;
- S-a verificat fiecare frază pentru logică și semnificație;
- S-au ajustat înlocuirile eronate prin deducție contextuală.

De exemplu, cuvântul „vjfuw" a fost dedus ca „egypt", prin observarea repetată a modelului și a contextului istoric din text.

Etapa 4 – Obținerea textului clar

După completarea corespondentelor, textul a devenit coerent și ușor de înțeles. Cheia de substituție completă a fost apoi aplicată pentru întregul text.

Textul final decriptat

---

the addition of secrecy to the transformations produced cryptography. true, it was more of a game than anything else—it sought to delay comprehension for only the shortest possible time, not the longest—and the cryptanalysis was, likewise, just a puzzle. egypt's was thus

a quasi cryptology in contrast to the deadly serious science of today. yet great things have small beginnings, and these hieroglyphs did include, though in an imperfect fashion, the two elements of secrecy and transformation that comprise the essential attributes of the science. and so cryptology was born. in its first 3,000 years, it did not grow steadily. cryptology arose independently in many places, and in most of them it died the deaths of its civilizations. in other places, it survived, embedded in a literature, and from this the next generation could climb to higher levels. but progress was slow and jerky. more was lost than retained...

Concluzii

Rezultate

Prin analiza frecvențelor și recunoașterea tiparelor lingvistice, s-a reușit decriptarea completă a textului, fără cunoașterea cheii inițiale.

Observații

- Cifrul monoalfabetic este ușor de spart prin metode statistice.
- Procesul evidențiază importanța lingvisticii în criptanaliză.
- Textul decriptat este coerent și confirmă succesul metodei aplicate.

Concluzie finală

Analiza a demonstrat că metodele clasice de criptanaliză, bazate pe frecvență și context, sunt suficiente pentru a sparge cifruri simple. Deși depășite, ele rămân esențiale pentru înțelegerea principiilor fundamentale ale criptografiei.