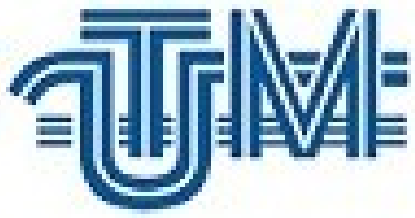


Ministry of Education, Culture and Research of the Republic of Moldova
Technical University of Moldova
Faculty of Computers, Computer Science and Microelectronics
Department of Software Engineering

Report
for laboratory work No. 2
course "Cryptoanalysis of monoalfabetical cyphers"

Done by:
Carp Dan-Octavian , gr. FAF-211
Checked by:
Cătălin MÎŢU

Chișinău – 2023

Lucrare de laborator nr. 2

Criptanaliza cifrurilor monoalfabetice

2.1. Noțiune de analiză a frecvenței apariției literelor

Punctul slab al sistemelor de criptare monoalfabetice constă în frecvenţa de apariţie a caracterelor în text. Dacă un text criptat este suficient de lung şi se cunoaşte limba în care este scris textul clar, sistemul poate fi spart printr-un atac bazat pe *frecvenţa apariţiei literelor* într-o limbă (atacul prin analiza frecvenței), această frecvență fiind o problemă studiată intens (nu neapărat în scopuri criptografice) iar în rezultat au fost construite diverse structuri de ordine relativ la frecvenţa apariţiei literelor în fiecare limbă europeană și în alte limbi.

De obicei, cu cât un text criptat este mai lung, cu atât frecvenţa literelor folosite se apropie de această ordonare generală. O comparare între cele două relaţii de ordine (cea a caracterelor din textul criptat şi cea a literelor din alfabetul limbii curente) conduce la realizarea câtorva corespondenţe (literă text clar – literă text criptat), ceea ce stabileşte în mod univoc cheia de criptare.

Pentru limba română frecvenţa literelor (exprimată în procente) este prezentată în tabelul 2.1 şi figura 2.1.

A	Ă	Â	B	C	D	E	F	G	H	I	Î	J	K	L	M
9,95	*4,06*	*0,91*	*1,07*	*5,28*	*3,45*	*11,47*	*1,18*	*0,99*	*0,47*	*9,96*	*1,40*	*0,24*	*0,11*	*4,48*	*3,10*
N	O	P	Q	R	S	Ş	T	Ţ	U	V	W	X	Y	Z	
6,47	*4,07*	*3,18*	*0,00*	*6,82*	*4,40*	*1,55*	*6,04*	*1,00*	*6,20*	*1,23*	*0,03*	*0,11*	*0,07*	0,71	

Tabelul 2.1. *Frecvenţa literelor limbii române*

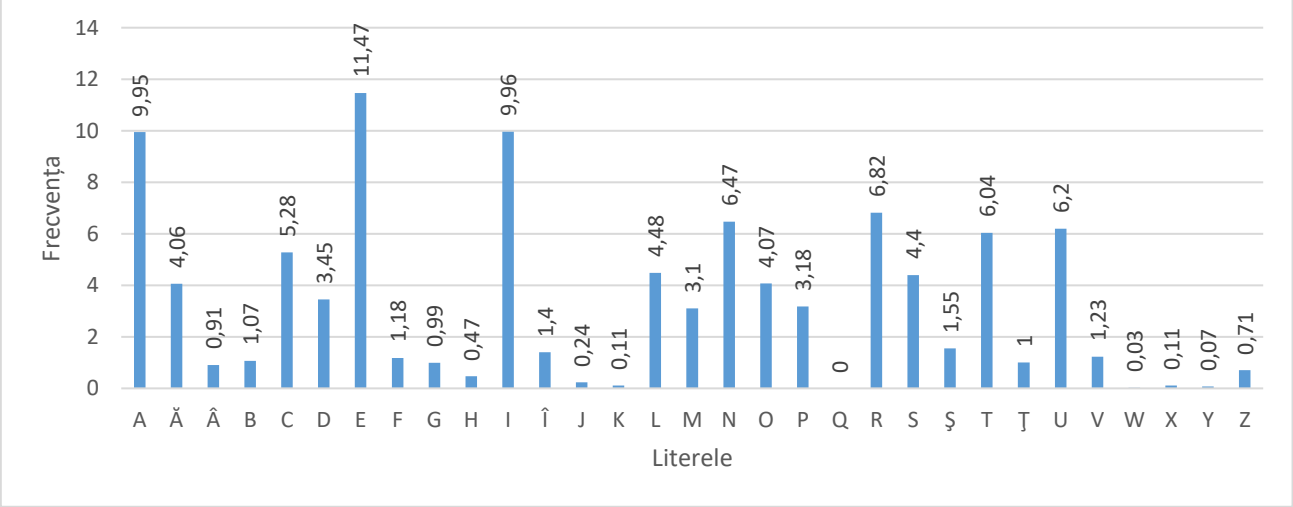


Figura 2.1. *Frecvenţa literelor limbii române*

Pentru limba engleză avem situația prezentată în tabelul 2.2 şi figura 2.2:

A	B	C	D	E	F	G	H	I	J	K	L	M
8,17	*1,49*	*2,78*	*4,25*	*12,7*	*2,23*	*2,01*	*6,09*	*6.97*	*0,15*	*0,77*	*4,03*	*2,41*
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
6,75	*7,51*	*1,93*	*0,09*	*5,99*	*6,33*	*9,06*	*2,76*	*0,98*	*2,36*	*0,15*	*1,97*	*0,07*

Tabelul 2.2. *Frecvenţa literelor limbii engleze*

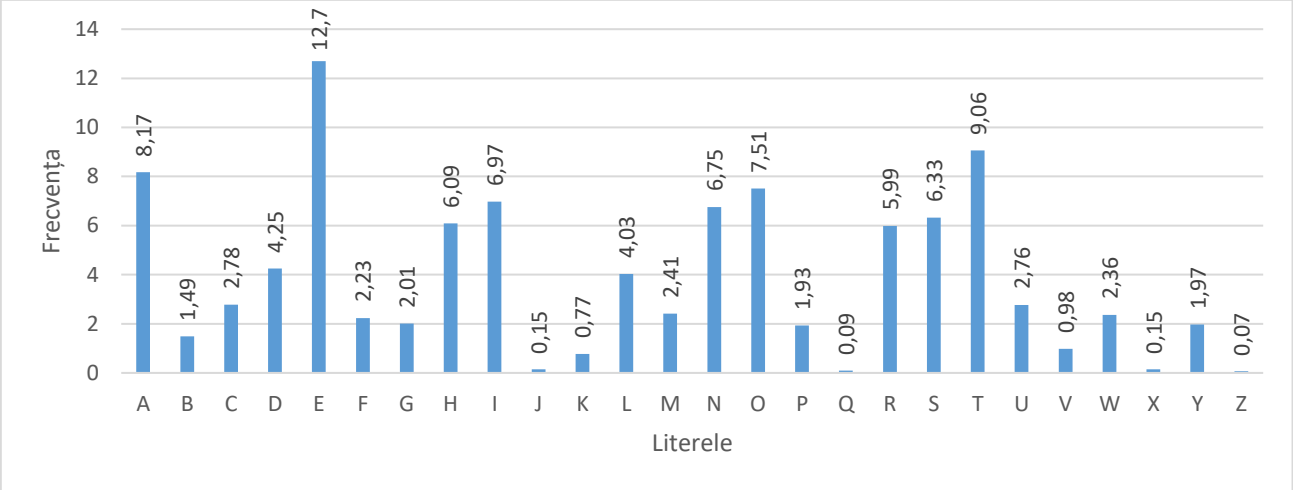


Figura 2.2. *Frecvenţa literelor limbii engleze*

2.2. Metodologia atacului prin analiza frecvențelor

Putem folosi informația despre frecvența de apariție a literelor într-o limbă pentru a încerca să spargem un cifru de substituție monoalfabetică. Acest lucru poate fi realizat deoarece, dacă spre exemplu pentru un mesaj scris în limba engleză litera „*E*”, care are cea mai mare frecvență, a fost criptată cu „*X*”, atunci fiecare „*X*” din textul criptat era un „*E*” în textul clar. Prin urmare, cea mai des întâlnită literă din textul cifrat ar trebui să fie „*X*”.

Astfel, dacă interceptăm un mesaj criptat, iar litera cea mai frecventă în el este „*P*”, putem presupune că „*P*” a fost folosit pentru a cripta „*E*”, și astfel putem înlocui toate „*P*”-urile cu „E”. Desigur, nu fiecare text are exact aceeași frecvență și, așa cum s-a văzut mai sus, „*T*” și „*A*” au și ele frecvențe înalte, așa că s-ar putea ca „*P*” să fie unul dintre acestea. Cu toate acestea, este puțin probabil să fie „*Z*”, care este rar întâlnit în limba engleză. Repetând acest proces cu următoarea cea mai frecventă literă, putem face progrese în spargerea unui mesaj.

Dacă ar fi să punem toate literele în ordine și să le înlocuim în conformitate cu tabelul frecvențelor, cel mai probabil că nu vom obține rezultatul așteptat. Criptanalistul trebuie să folosească alte „trăsături de personalitate” ale literelor pentru a sparge criptograma. Aceasta poate include

examinarea perechilor de litere (*digrafele*), cele mai frecvente fiind *TH, HE, AN, IN, ER, ON, RE, ED, ND, HA, AT, EN*. Tripletele de litere (*trigrafele*), la fel pot fi foarte utile, cele mai frecvente dintre ele în limba engleză fiind *THE, AND, THA, ENT, ION, TIO, FOR, NDE, HAS, NCE, TIS, OFT, MEN*. În plus, în limba engleză sunt doar câteva litere care apar ca duble (*SS, EE, TT, OO* și *FF* fiind cele mai frecvente). Există doar două cuvinte cu sens formate dintr-o singură literă în limba engleză: „*A*” și „*I*”.

Alte cuvinte frecvente încep să apară, de asemenea, pe măsură ce vom face unele înlocuiri. De exemplu, „*T***E*” poate apărea frecvent după efectuarea substituțiilor pentru „*T*” și „*E*”. În acest caz „*T***E*” este foarte probabil să fie „*THE*”, un cuvânt foarte frecvent în engleză.

Procesul de analiză a frecvenței folosește diverse proprietăți subtile ale limbajului și, din acest motiv, este aproape imposibil ca un computer să facă toată munca. În mod inevitabil, elementul de aport uman este necesar în acest proces pentru a lua decizii fundamentate cu privire la literele care trebuie înlocuite.

2.3. Exemplu de atac prin analiza frecvențelor

Fie că am interceptat o criptogramă ***c***, despre care cunoaștem că a fost obținută în urma utilizării uni cifru monoalfabetic peste un mesaj scris în limba engleză:

> ***c*** *= GFS WMY OG LGDVS MF SFNKYHOSU ESLLMRS, PC WS BFGW POL DMFRQMRS, PL OG CPFU M UPCCSKSFO HDMPFOSXO GC OIS LMES DMFRQMRS DGFR SFGQRI OG CPDD GFS LISSO GK LG, MFU OISF WS NGQFO OIS GNNQKKSFNSL GC SMNI DSOOSK. WS NMDD OIS EGLO CKSJQSFODY GNNQKKPFR DSOOSK OIS 'CPKLO', OIS FSXO EGLO GNNQKKPFR DSOOSK OIS 'LSNGFU' OIS CGDDGWPFR EGLO GNNQKKPFR DSOOSK OIS 'OIPKU', MFU LG GF, QFOPD WS MNNGQFO CGK MDD OIS UPCCSKSFO DSOOSKL PF OIS HDMPFOSXO LMEHDS. OISF WS DGGB MO OIS NPHISK OSXO WS WMFO OG LGDVS MFU WS MDLG NDMLLPCY POL LYEAGDL. WS CPFU OIS EGLO GNNQKKPFR LYEAGD MFU NIMFRS PO OG OIS CGKE GC OIS 'CPKLO' DSOOSK GC OIS HDMPFOSXO LMEHDS, OIS FSXO EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'LSNGFU' DSOOSK, MFU OIS CGDDGWPFR EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'OIPKU' DSOOSK, MFU LG GF, QFOPD WS MNNGQFO CGK MDD LYEAGDL GC OIS NKYHOGRKME WS WMFO OG LGDVS.*

Primul pas este să găsim frecvențele tuturor literelor care apar în criptogramă, așa cum e arătat în tabelul 2.3.

Ciphertext Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	5	2	26	42	23	51	67	8	33	1	35	39	35	29	85	30	14	17	88	0	17	3	16	6	10	0

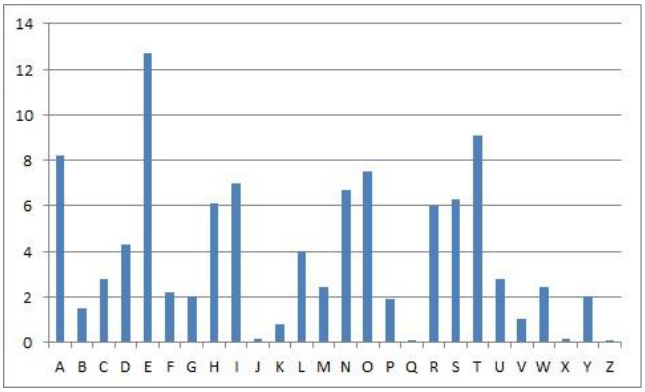
Tabelul 2.3. *Frecvența literelor în criptograma interceptată*

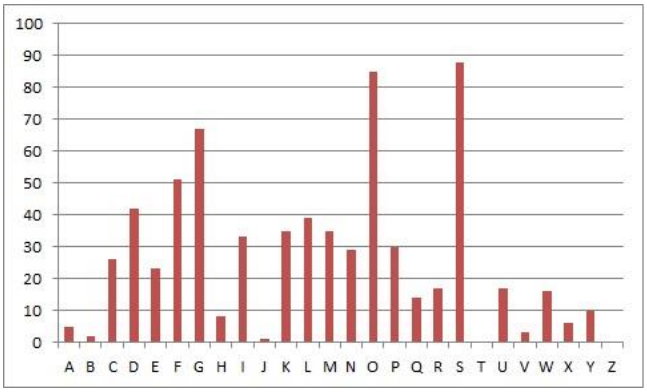
Pentru comoditate ordonăm tabelul în descreștere a frecvențelor, așa cum e arătat în tabelul 2.4.

Ciphertext Letter	S	O	G	F	D	L	K	M	I	P	N	C	E	R	U	W	Q	Y	H	X	A	V	B	J	T	Z
Frequency	88	85	67	51	42	39	35	35	33	30	29	26	23	17	17	16	14	10	8	6	5	3	2	1	0	0

Tabelul 2.4. *Frecvența literelor în criptograma interceptată*

Mai jos putem observa reprezentarea grafică a frecvenței literelor limbii engleze (figura din stânga) și a frecvenței literelor în mesajul interceptat (figura din dreapta):





Acum că avem toate frecvențele literelor din textul cifrat, putem începe să facem câteva substituții. Vedem că cea mai frecventă literă din textul cifrat este „*S*”, urmată îndeaproape de „*O*”. Din figura de mai sus și tabelele 2.2 și 2.4, putem ghici că aceste două litere reprezintă „*e*” și respectiv „*t*”, iar după efectuarea acestor substituiri obținem:

GFe WMY tG LGDVe MF eFNKYHteU EeLLMRe, PC We BFGW PtL DMFRQMRe, PL tG CPFU M UPCCeKeFt HDMPFteXt GC tIe LMEe DMFRQMRe DGFR eFGQRI tG CPDD GFe LIeet GK LG, MFU tIeF We NGQFt tIe GNNQKKeFNeL GC eMNI DetteK. We NMDD tIe EGLt CKeJQeFtDY GNNQKKPFR DetteK tIe 'CPKLt', tIe FeXt EGLt GNNQKKPFR DetteK tIe 'LeNGFU' tIe CGDDGWPFR EGLt GNNQKKPFR DetteK tIe 'tIPKU', MFU LG GF, QFtPD We MNNGQFt CGK MDD tIe UPCCeKeFt DetteKL PF tIe HDMPFteXt LMEHDe. tIeF We DGGB Mt tIe NPHIeK teXt We WMFt tG LGDVe MFU We MDLG NDMLLPCY PtL LYEAGDL. We CPFU tIe EGLt GNNQKKPFR

LYEAGD MFU NIMFRe Pt tG tIe CGKE GC tIe 'CPKLt' DetteK GC tIe HDMPFteXt LMEHDe, tIe FeXt EGLt NGEEGF LYEAGD PL NIMFReU tG tIe CGKE GC tIe 'LeNGFU' DetteK, MFU tIe CGDDGWPFR EGLt NGEEGF LYEAGD PL NIMFReU tG tIe CGKE GC tIe 'tIPKU' DetteK, MFU LG GF, QFtPD We MNNGQFt CGK MDD LYEAGDL GC tIe NKYHtGRKME We WMFt tG LGDVe.

Observăm acum că cuvântul „*tIe*” apare frecvent în pasaj. În engleză, cel mai comun cuvânt de 3 litere este „*the*” și acest lucru se potrivește cu ceea ce am făcut deja, ceea ce sugerează că „*I*” ar trebui decriptat la „*h*”.

De asemenea, uitându-ne din nou la frecvențe, vedem că următoarea literă cea mai frecventă este „*G*”, care probabil reprezintă valoarea criptată a uneia dintre literele „*a*”, „*i*” sau „*o*”. Vedem că al treilea cuvânt din pasaj este „*tG*”, iar singura dintre aceste opțiuni care are sens este „*to*”, așa că presupunem că „*G*” este „*o*” criptat.

Efectuăm și aceste substituiri și obținem:

oFe WMY to LoDVe MF eFNKYHteU EeLLMRe, PC We BFoW PtL DMFRQMRe, PL to CPFU M UPCCeKeFt HDMPFteXt oC the LMEe DMFRQMRe DoFR eFoQRh to CPDD oFe ***Lheet*** *oK Lo, MFU theF We NoQFt the oNNQKKeFNeL oC eMNh DetteK. We NMDD the EoLt CKeJQeFtDY oNNQKKPFR DetteK the 'CPKLt', the FeXt EoLt oNNQKKPFR DetteK the 'LeNoFU' the CoDDoWPFR EoLt oNNQKKPFR DetteK the 'thPKU', MFU Lo oF, QFtPD We MNNoQFt CoK MDD the UPCCeKeFt DetteKL PF the HDMPFteXt LMEHDe. theF We DooB Mt the NPHheK teXt We WMFt to LoDVe MFU We MDLo NDMLLPCY PtL LYEAoDL. We CPFU the EoLt oNNQKKPFR LYEAoD MFU NhMFRe Pt to the CoKE oC the 'CPKLt' DetteK oC the HDMPFteXt LMEHDe, the FeXt EoLt NoEEoF LYEAoD PL NhMFReU to the CoKE oC the 'LeNoFU' DetteK, MFU the CoDDoWPFR EoLt NoEEoF LYEAoD PL NhMFReU to the CoKE oC the 'thPKU' DetteK, MFU Lo oF, QFtPD We MNNoQFt CoK MDD LYEAoDL oC the NKYHtoRKME We WMFt to LoDVe.*

Primul cuvânt din criptogramă a devenit acum „*oFe*”, care atunci când este luat în considerare cu apariția lui „*F*”, ne duce la concluzia că „*F*” este imaginea lui „*n*”. Acest lucru se potrivește și cu frecvențele ambelor litere din tabele.

Observă cuvântul „*Lheet*”, care reprezintă cel mai probabil cuvântul „*sheet*”, așa că înlocuim „*L*” cu „*s*”. Din nou, frecvența acestor două litere este aproape corectă:

*one WMY to **soDVe** Mn enNKYHteU EessMRe, PC We BnoW Pts DMnRQMRe, Ps to CPnU M UPCCeKent HDMPnteXt oC the sMEe DMnRQMRe DonR enoQRh to CPDD **one sheet oK so**, MnU then We NoQnt the oNNQKKenNes oC eMNh DetteK. We NMDD the Eost CKeJQentDY oNNQKKPnR DetteK the 'CPKst', the neXt Eost oNNQKKPnR DetteK the 'seNonU' the CoDDoWPnR Eost oNNQKKPnR DetteK the 'thPKU', MnU so on, QntPD We MNNoQnt CoK MDD the UPCCeKent DetteKs Pn the HDMPnteXt sMEHDe. then We DooB Mt the NPHheK teXt We WMnt to **soDVe** MnU We MDso NDMssPCY Pts sYEAoDs. We CPnU the Eost oNNQKKPnR sYEAoD MnU NhMnRe Pt to the CoKE oC the 'CPKst' DetteK oC the HDMPnteXt sMEHDe, the neXt Eost NoEEon sYEAoD Ps NhMnReU to the CoKE oC the 'seNonU' DetteK, MnU the CoDDoWPnR Eost NoEEon sYEAoD Ps NhMnReU to the CoKE oC the 'thPKU' DetteK, MnU so on, QntPD We MNNoQnt CoK MDD sYEAoDs oC the NKYHtoRKME We WMnt to **soDVe**.*

Mai observăm cuvântul „*soDVe*”, care ar putea fi „*solve*”, implicând transformările lui „*D*” și „*V*” în „*l*” și respectiv „*v*”. De asemenea sintagma „*one sheet oK so*” ne sugerează că „*K*” este „*r*”:

*one WMY to solve Mn enNrYHteU EessMRe, PC We BnoW Pts lMnRQMRe, Ps to CPnU M UPCCerent HlMPnteXt oC the sMEe lMnRQMRe lonR **enoQRh** to CPll one sheet or so, MnU then We NoQnt the oNNQrrenNes oC eMNh letter. We NMll the Eost CreJQentlY oNNQrrPnR letter the 'CPrst', the neXt Eost oNNQrrPnR letter the 'seNonU' the ColloWPnR Eost oNNQrrPnR letter the 'thPrU', MnU so on, QntPl We MNNoQnt Cor Mll the UPCCerent letters Pn the HlMPnteXt sMEHle. then We looB Mt the NPHher teXt We WMnt to solve MnU We Mlso NlMssPCY Pts sYEAols. We CPnU the Eost oNNQrrPnR sYEAol MnU NhMnRe Pt to the CorE oC the 'CPrst' letter oC the HlMPnteXt sMEHle, the neXt Eost NoEEon sYEAol Ps NhMnReU to the CorE oC the 'seNonU' letter, MnU the ColloWPnR Eost NoEEon sYEAol Ps NhMnReU to the CorE oC the 'thPrU' letter, MnU so on, QntPl We MNNoQnt Cor Mll sYEAols oC the NrYHtoRrME We WMnt to solve.*

În pasajul obținut avem cuvântul „*enoQRh*”, care este probabil să fie „*enough*”, și astfel avem transformările „*Q*” și „*R*” în „*u*” și respectiv „*g*”.

*one WMY to solve Mn enNrYHteU **EessMge**, PC We BnoW Pts lMnguMge, Ps to CPnU M UPCCerent HlMPnteXt oC the sMEe lMnguMge long enough to CPll one sheet or so, MnU then We **Nount** the oNNurrenNes oC eMNh letter. We NMll the Eost CreJuentlY oNNurrPng letter the 'CPrst', the neXt Eost oNNurrPng letter the 'seNonU' the*

ColloWPng Eost oNNurrPng letter the 'thPrU', MnU so on, untPl We MNNount Cor Mll the UPCCerent letters Pn the HlMPnteXt sMEHle. then We looB Mt the NPHher teXt We WMnt to solve MnU We Mlso NlMssPCY Pts sYEAols. We CPnU the Eost oNNurrPng sYEAol MnU NhMnge Pt to the CorE oC the 'CPrst' letter oC the HlMPnteXt sMEHle, the neXt Eost NoEEon sYEAol Ps NhMngeU to the CorE oC the 'seNonU' letter, MnU the ColloWPng Eost NoEEon sYEAol Ps NhMngeU to the CorE oC the 'thPrU' letter, MnU so on, untPl We MNNount Cor Mll sYEAols oC the NrYHtogrME We WMnt to solve.

Avem acum cuvântul „*Nount*” care ar putea fi „*count*” și „*EessMge*” care este probabil să fie „*message*”, ceea ce ne sugerează că „*N*”, „*E*” și „*M*” sunt „*c*”, „*m*” și "*a*":

one WaY to solve an encrYHteU message, PC We BnoW Pts language, Ps to CPnU a UPCCerent HlaPnteXt oC the same language long enough to CPll one sheet or so, anU then We count the occurrences oC each letter. We call the most CreJuentlY occurrPng letter the 'CPrst', the neXt most occurrPng letter the 'seconU' the ColloWPng most occurrPng letter the 'thPrU', anU so on, untPl We account Cor all the UPCCerent letters Pn the HlaPnteXt samHle. then We looB at the cPHher teXt We Want to solve anU We also classPCY Pts sYmAols. We CPnU the most occurrPng sYmAol anU change Pt to the Corm oC the 'CPrst' letter oC the HlaPnteXt samHle, the neXt most common sYmAol Ps changeU to the Corm oC the 'seconU' letter, anU the ColloWPng most common sYmAol Ps changeU to the Corm oC the 'thPrU' letter, anU so on, untPl We account Cor all sYmAols oC the crYHtogram We Want to solve.

Cuvântul „*ocurrPng*” este în mod clar menit să citească „*occurring*”, și este probabil ca „*sYmAol*” să fie „*symbol*”. În plus, este probabil ca "W"→"w", "X"→"x", "Y"→"y" și "Z"→"z", ele având aproape aceleași frecvențe în ambele tabele, dar și dacă ne uităm la sensul cuvintelor în care aceste litere le întâlnim:

one way to solve an encryHteU message, iC we Bnow its language, is to CinU a UiCCerent Hlaintext oC the same language long enough to Cill one sheet or so, anU then we count the occurrences oC each letter. we call the most CreJuently occurring letter the 'Cirst', the next most occurring letter the 'seconU' the Collowing most occurring letter the 'thirU', anU so on, until we account Cor all the UiCCerent letters in the Hlaintext samHle. then we looB at the ciHher text we want to solve anU we also classiCy its symbols. we CinU the most occurring symbol anU change it to the Corm oC the 'Cirst' letter oC the

Hlaintext samHle, the next most common symbol is changeU to the Corm oC the 'seconU' letter, anU the Collowing most common symbol is changeU to the Corm oC the 'thirU' letter, anU so on, until we account Cor all symbols oC the cryHtogram we want to solve.

Acum, analizând cuvintele rămase nedescifrate, putem vedea că „*C*” este „*f*”, „*B*” este „*k*”, „*U*” este „*d*”, „*J*” este „*q*” și „*H*” este „*p*”. În rezultat obținem mesajul:

one way to solve an encrypted message, if we know its language, is to find a different plaintext of the same language long enough to fill one sheet or so, and then we count the occurrences of each letter. we call the most frequently occurring letter the 'first', the next most occurring letter the 'second' the following most occurring letter the 'third', and so on, until we account for all the different letters in the plaintext sample. then we look at the cipher text we want to solve and we also classify its symbols. we find the most occurring symbol and change it to the form of the 'first' letter of the plaintext sample, the next most common symbol is changed to the form of the 'second' letter, and the following most common symbol is changed to the form of the 'third' letter, and so on, until we account for all symbols of the cryptogram we want to solve.

Acesta este un extras din „*Un manuscris despre descifrarea mesajelor criptografice*”, de Al-Kindi, din jurul anului 850 AD., care este cea mai veche descriere cunoscută a procesului de analiză a frecvențelor.

De asemenea, acum putem recupera cheia folosită în criptare prin alăturarea alfabetelor textului criptat și a mesajului (tabelul 2.5). Acest lucru este util dacă avem și alte mesaje interceptate de la aceeași persoană, deoarece este probabil să folosească aceeași cheie (sau o rotație a două sau trei chei).

Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext Alphabet	M	A	N	U	S	C	R	I	P	T	B	D	E	F	G	H	J	K	L	O	Q	V	W	X	Y	Z

Tabelul 2.5. *Alfabetul reconstituit al mesajului criptat*

Sarcina. *Fie a fost interceptat un mesaj criptat despre care se cunoaște a fost obținut prin utilizarea unui cifru monoalfabetic. Aplicând atacul cu analiza frecvențelor de aflat mesajul original, dacă se presupune că el este un text scris în limba engleză. Țineți cont de faptul că au fost criptate doar literele, celelalte caractere rămânând necriptate.*
Notă: utilizați serviciul https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html
Raportul va conține descrierea procesului de spargere, exact la fel cum a fost prezentat în compartimentul **2.3** *în* **Exemplu de atac prin analiza frecvențelor**.
Fiecare student va lua varianta în conformitate cu numărul său de ordine din lista grupei.

.

V7

"OTWN tgo X rviv pwinssxgj xg wqv Pduivzv Ungwxcc'p jtiovgp tw wqv Ktwxhtgtgo rv rvgw cinz wnuxh wn wnuxh ztikvsxgj tw wqv xgjvgdxwf wqtw zvgpqnrvo xg ktixndp vgwviuixpvp, wxss Otwn jtkv vyuivppxng wn qxp rtiztozxitwxng cni wqnpv zvg rqn htg vyusnxw rqtw tiv htssvo 'hxuqvip.' "Pn rinwv Svng Atwwxpwt Tsaviwx gvti wqv avjxggxgj nc wqv pdhhxghw adwpdjjvpwxkv rnil wqtw vtigvo qxz wqv wxwsv nc Ctwqvi nc RvpwvigHifuwnsnjf. Tsaviwx rtp wqv cxipw nc t jindu nc rixwvip rqn, vsvzvgw afvsvzvgw, ovkvsnuvo t wfuv nc hxuqvi wn rqxhq znpw nc wnotf'p pfpwvzp nchifuwnjituqf avsngj. Wqv puvhxvp xp unsftsuqtavwxh pdapwxwdwxng.Xw rtp wqv tztwvdip nc hifuwnsnjf rqn hivtwvo wqv puvhxvp. Wqvuincvppxngtsp, rqn tsznpw hviwtxgsf pdiutppvo wqvz xg hifuwtgtsfwxhvyuviwxpv, hnghvgwitwvo ng wqv onrg-wn-vtiwq uinasvzp nc wqv pfpwvzpwqtw rviv wqvg xg dpv adw tiv gnr ndwotwvo. Wqv tztwvdip, dgcvwwvivo wnwqvpv ivtsxwxvp, pntivo xgwn wqv vzufivtg nc wqvnif. Wqviv rviv cndirqnpv wqndjqw wnnl rxgjp: t ctzndp tihqxwvhw, tg xgwvssvhwdts hsvixh, tgvhhsvpxtpwxhts hndiwxvi, tgo t gtwdits phxvgwxpw.Wqv tihqxwvhw rtp Tsaviwx, t ztg rqn, uviqtup avwwvi wqtg tgfngvvyhvuw Svngtion ot Kxghx, vuxwnzxmvp wqv Ivgtxpptghv xovts nc wqvdgxkvipts ztg. Anig xg 1404, wqv xssvjxwxztwv adw ctknivo png nc t ctzxsfnc ixhq Csnivgwxgv zvihqtgwp, Tsaviwx vgenfvo vywitnioxgtif xgwvssvhwdtstgo twqsvwxh tuwxwdovp. Qv utxgwvo, hnzunpvo zdpxh, tgo rtp ivjtiovotp ngv nc wqv avpw nijtgxpwp nc qxp otf. Rixwxgjp undivo cinz qxp uvg. QxpOv Iv Tvoxcxhtwnixt, wqv cxipw uixgwvo annl ng tihqxwvhwdiv, rixwwvg rqxsvJnwqxh hqdihqvp rviv pwxss avxgj adxsw, qvsuvo pqtuv wqv wqndjqwp ncwqnpv rqn adxsw pdhq dwwvisf gng-Jnwqxh pwidhwdivp tp Pw. Uvwvi'p Atpxsxhtxg Inzv. Ethna Adihlqtiow, tdwqni nc wqv hstppxh Wqv Hxkxsxmtwxng nc wqvIvgtxpptghv xg Xwtsf, pxgjsvo ndw Tsaviwx tp ngv nc wqv widsf tss-pxovozvg rqn wnrvi tankv wqvxi gdzvindp ztgf-pxovo hngwvzunitixvp. Tgotgnwqvi jivtw Ivgtxpptghv phqnsti, Enqg Pfzngop, ovhstivo wqtw "Qvuivpvgwp wqv puxixw nc wqv 15wq hvgwdif tw xwp kvif avpw."Tzngj qxp cixvgop rtp wqv ungwxcxhts pvhivwtif, Svngtion Otwn, ngv ncwqv svtigvo zvg nc qxp tjv, rqn odixgj wqtw zvznitasv pwinss xg wqvKtwxhtg jtiovgp aindjqw wqv hngkviptwxng tindgo wn hifuwnsnjf. "Fnd'kvtsrtfp avvg xgwvivpwvo xg wqvpv pvhivwp nc gtwdiv," Otwn ptxo. "Rqtw onfnd wqxgl nc wqvpv ovhxuqvivip? Qtkv fnd wixvo fndi qtgo tw xw, tp zdhqtp fnd lgnr qnr wn?"Tsaviwx pzxsvo. Qv lgvr wqtw Otwv'p odwxvp xghsdovo hxuqvip (xw rtpavcniv wqv hdixt qto t pvutitwv hxuqvi pvhivwtif). "Fnd'iv wqv qvto nc wqvutuvs pvhivwtixtw," qv wvtpvo. "Hndso xw av wqtw fnd qto wn dpv wqvpvwqxgjp t cvr wxzvp xg ztwwvip nc jivtw xzuniwtghv wn Qxp Qnsxgvpp?""Wqtw'p rqf X aindjqw xw du," Otwn ivusxvo htgoxosf. "Tgo avhtdpv ncwqv unpw X qtkv, X rtgw wn av tasv wn on xw zfpvsc rxwqndw qtkxgj wn dpvndwpxov xgwviuivwvip. Cni rqvg wqvf aixgj zv svwwvip xg hxuqvi xgwvihvuwvoaf puxvp, xw'p gn enlxgj ztwwvi. Pn usvtpvâ€”xc fnd'kv wqndjqw du tgf gvrxovtp qtkxgj wn on rxwq wqxp adpxgvpp, wvss zv tandw wqvz." Pn Tsaviwxuinzxpvo wqtw qv rndso on pnzv rnil ng xw pn wqtw Otwn rndso pvv wqtwxw rtp uincxwtasv wn qtkv tplvo qxz, tgo wqv ivpdsw rtp wqv vpptf wqtw qvrinwv xg 1466 ni vtisf 1467, rqvg qv rtp 62 ni 63.Qv xzusxvo wqtw qv wqndjqw du wqv xovt nc civbdvghf tgtsfpxp tss afqxzpvsc, adw wqv hnghvuwxng wqtw qv pvw cniwq xp cti wnn ztwdivo cni wqtw.Gvkviwqvsvpp, qxp ivztiltasf sdhxo Stwxg vpptf, wnwtsxgj tandw 25ztgdphixuw utjvp, hngpwxwdwvp wqv Rvpw'p nsovpw vywtgw wvyw nghifuwtgtsfpxp.

Realizare:

am interceptat o criptogramă c, despre care cunoaștem că a fost obținută în urma utilizării uni cifru monoalfabetic peste un mesaj scris în limba engleză:

OTWN TGO X RVIV PWINSSXGJ XG WQV PDUIVZV UNGWXCC'P JTIQVGP TW WQV KTWXHTGTGO RV RVGW CINZ
WNUXH WN WNUXH ZTIKVSXGJ TW WQV XGJVGDXWF WQTW ZVGPQNRVO XG KTIXNDP VGWVIUIXPVP, WXSS OTWN
JTKV VYUIVPPXNG WN QXP RTIZTOZXITWXNG CNI WQNPV ZVG RQN HTG VYUSNXW RQTW TIV HTSSVO 'HXUQVIP.'
''PN RINWV SVNG ATWWXPWT TSAVIWX GVTI WQV AVJXGGXGJ NC WQV PDHHXGHW ADWPDJJVPWXKV RNIL
WQTW VTIGVO QXZ WQV WXWSV NC CTWQVI NC RVPWVIGHIFUWNSNJF. TSAVIWX RTP WQV CXIPW NC T JINDU
NC RIXWVIP RQN, VSVZVGW AFVSVZVGW, OVKVSNUVO T WFUV NC HXUQVI WN RQXHQ ZNPW NC WNOTFP PFPWVZP
NCHIFUWNJITUQF AVSNGJ. WQV PUVHXVP XP UNSFTSUQTAVWXH PDAPWXWDWXNG XW RTP WQV TZTWVDIP NC
HIFUWNSNJF RQN HIVTWVO WQV PUVHXVP. WQVUINCVPPXNGTSP, RQN TSZNPW HVIWTXGSF PDIUTPPVO WQVZ XG
HIFUWTGTSFWXHVYUVIWXPV, HNGHVGWITWVO NG WQV ONRG-WN-VTIWQ UINASVZP NC WQV PFPWVZPWQTW
RVIV WQVG XG DPV ADW TIV GNR NDWOTWVO. WQV TZTWVDIP, DGCVWWVIVO WNWQVPV IVTSXWXVP, PNTIVO
XGWN WQV VZUFIVTG NC WQVNIF. WQVIV RVIV CNDIRQNPV WQNDJQW WNNL RXGJP: T CTZNDP TIHQXWVHW, TG
XGWVSSVHWDTS HSVIXH, TGVHHSVPXTPWXHTS HNDIWXVI, TGO T GTWDITS PHXVGWXPW.WQV TIHQXWVHW RTP
TSAVIWX, T ZTG RQN, UVIQTUP AVWWVI WQTG TGFNGVVYHVUW SVNGTION OT KXGHX, VUXWNZXMVP WQV
IVGTXPPTGHV XOVTS NC WQVDGXKVIPTS ZTG. ANIG XG 1404, WQV XSSVJXWXZTWV ADW CTKNIVO PNG NC T
CTZXSFNC IXHQ CSNIVGWXGV ZVIHQTGWP, TSAVIWX VGENFVO VYWITNIOXGTIF XGWVSSVHWDTSTGO TWQSVWXH
TUWXWDOVP. QV UTXGWVO, HNZUNPVO ZDPXH, TGO RTP IVJTIOVOTP NGV NC WQV AVPW NIJTGXPWP NC QXP OTF.
RIXWXGJP UNDIVO CINZ QXP UVG. QXPOV IV TVOXCXHTWNIXT, WQV CXIPW UIXGWVO ANNL NG
TIHQXWVHWDIV, RIXWWVG RQXSVJNWQXH HQDIHQVP RVIV PWXSS AVXGJ ADXSW, QVSUVO PQTUV WQV

WQNDJQWP NCWQNPV RQN ADXSW PDHQ DWWVISF GNG-JNWQXH PWIDHWDIVP TP PW. UVWVI'P ATPXSXHTXG
INZV, ETHNA ADIHLQTIOW, TDWQNI NC WQV HSTPPXH WQV HXKXSXMTWXNG NC WQVIVGTXPPTTGHV XG XWTSF,
PXGJSVO NDW TSAVIWX TP NGV NC WQV WIDSF TSS-PXOVOZVG RQN WNRVI TANKV WQVXI GDZVINDP ZTGF-PXOVO
HNGWVZUNITIXVP. TGOTGNWQVI JIVTW IVGTXPPTGHV PHQNSTI, ENQG PFZNGOP, OVHSTIVO WQTW
"QVUIVPVGWP WQV PUXIXW NC WQV 15WQ HVGWDIF TW XWP KVIF AVPW."TZNGJ QXP CIXVGOP RTP WQV
UNGWXCXHTS PVHIVWTIF, SVNGTION OTWN, NGV NCWQV SVTIGVO ZVG NC QXP TJV, RQN ODIXGJ WQTW ZVZNITASV
PWINSS XG WQVKTWXHTG JTIOVGP AINDJQW WQV HNGKVIPTWXNG TINDGO WN HIFUWNSNJF. "FND'KVTSRTFP AVVG
XGWVIVPWVO XG WQVPV PVHIVWP NC GTWDIV," OTWN PTXO. "RQTW ONFND WQXGL NC WQVPV OVHXUQVIVIP?
QTKV FND WIXVO FNDI QTGO TW XW, TP ZDHQTP FND LGNR QNR WN?"TSAVIWX PZXSVO. QV LGVR WQTW OTWV'P
ODWXVP XGHSDOVO HXUQVIP (XW RTPAVCNIV WQV HDIXT QTO T PVUTITWV HXUQVI PVHIVWTIF). "FND'IV WQV
QVTO NC WQVUTUVS PVHIVWTIXTW," QV WVTPVO. "HNDSO XW AV WQTW FND QTO WN DPV WQVPVWQXGJP T CVR
WXZVP XG ZTWWVIP NC JIVTW XZUNIWTGHV WN QXP QNSXGVPP?""WQTW'P RQF X AINDJQW XW DU," OTWN
IVUSXVO HTGOXOSF. "TGO AVHTDPV NCWQV UNPW X QTKV, X RTGW WN AV TASV WN ON XW ZFPVSC RXWQNDW
QTKXGJ WN DPVNDWPXOV XGWVIUIVWVIP. CNI RQVG WQVF AIXGJ ZV SVWWVIP XG HXUQVI XGWVIHVUWVOAF
PUXVP, XW'P GN ENLXGJ ZTWWVI. PN USVTPV—XC FND'KV WQNDJQW DU TGF GVRXOVTP QTKXGJ WN ON RXWQ
WQXP ADPXGVPP, WVSS ZV TANDW WQVZ." PN TSAVIWXUINZXPVO WQTW QV RNDSO ON PNZV RNIL NG XW PN
WQTW OTWN RNDSO PVV WQTWXW RTP UINCXWTASV WN QTKV TPLVO QXZ, TGO WQV IVPDSW RTP WQV VPPTF
WQTW QVRINWV XG 1466 NI VTISF 1467, RQVG QV RTP 62 NI 63.QV XZUSXVO WQTW QV WQNDJQW DU WQV
XOVT NC CIVBDVGHF TGTSFPXP TSS AFQXZPVSC, ADW WQV HNGHVUWXNG WQTW QV PVW CNIWQ XP CTI WNN
ZTWDIVO CNI WQTW GVKVIWQVSVPP, QXP IVZTILTASF SDHXO STWXG VPPTF, WNWTSXGJ TANDW 25ZTGDPHIXUW
UTJVP. HNGPWXWDWVP WQV RVPW'P NSQVPW VYWTGW WVYW NGHIFUWTGTSFPXP

găsim frecvențele tuturor literelor care apar în criptogramă conform aparitiei literelor in alfafetul englez

E	T	A	O	I	N	S	H	R	D	L	C	U	M	W	F	G	Y	P	B	V	K	J	X	Q	Z
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3	4.0	2.8	2.8	2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.15	0.15	0.10	0.07

V	W	T	N	X	P	I	Q	G	S	O	H	D	U	C	F	R	Z	A	J	K	L	Y	E	M	B
364	326	230	209	199	197	178	168	160	104	96	92	84	68	58	58	57	57	47	43	22	11	7	4	2	1
12.8	11.5	8.1	7.4	7.0	6.9	6.3	5.9	5.6	3.7	3.4	3.2	3.0	2.4	2.0	2.0	2.0	2.0	1.7	1.5	0.8	0.4	0.2	0.1	0.1	0.0

Incepem inlocuirea in textul criptat:

1.Am inlocuit V cu E fiind cea mai folosita litera
2. Am urmat sa inlocuiesc W cu T
3. T a fost inlocuit cu a
4. A urmat trigraful the; Q obtinand ca fiind H
5.A urmat digraful in ; afland X si G
...
Ultimele fiind cele mai putin intalnite B fiind q; M fiind S

In final am completat tabelul cu fiecare litera care a m deciptat-o:

V	W	T	N	X	P	I	Q	G	S	O	H	D	U	C	F	R	Z	A	J	K	L	Y	E	M	B
364	326	230	209	199	197	178	168	160	104	96	92	84	68	58	58	57	57	47	43	22	11	7	4	2	1
12.8	11.5	8.1	7.4	7.0	6.9	6.3	5.9	5.6	3.7	3.4	3.2	3.0	2.4	2.0	2.0	2.0	2.0	1.7	1.5	0.8	0.4	0.2	0.1	0.1	0.0
e	t	a	o	i	s	r	h	n	l	d	c	u	p	f	y	w	m	b	g	v	k	x	j	s	q

In final obtinem urmatorul text decriptat:

dato and i were strolling in the supreme pontiff's gardens at the vatican and we went from topic to topic marveling at the ingenuity that men showed in various enterprises, till dato gave expression to his warm admiration for those men who can exploit what are called 'ciphers.' "so wrote leon battista alberti near the beginning of the succinct but suggestive work that earned him the title of father of western cryptology. alberti was the first of a group of writers who, element by element, developed a type of cipher to which most of today's systems of cryptography belong. the species is polyalphabetic substitution.it was the amateurs of cryptology who created the species. the professionals, who almost certainly surpassed them in cryptanalyticexpertise, concentrated on the down-to-earth problems of the systems that were then in use but are now outdated. the amateurs, unfettered to these realities, soared into the empyrean of theory. there were four whose thought took wings: a famous architect, an intellectual cleric, an ecclesiastical courtier, and a natural scientist.the architect was alberti, a man who, perhaps better than anyone except leonardo da vinci, epitomises the renaissance ideal of theuniversal man. born in 1404, the illegitimate but favored son of a family of rich florentine merchants, alberti enjoyed extraordinary intellectual and athletic aptitudes. he painted, composed music, and was regarded as one of the best organists of his day. writings poured from his pen. hisde re aedificatoria, the first printed book on architecture, written while gothic churches were still being built, helped shape the thoughts of those who built such utterly non-gothic structures as st. peter's basilicain rome. jacob burckhardt, author of the classic the civilisation of the renaissaance in italy, singled out alberti as one of the truly all-sidedmen who tower above their numerous many-sided contemporaries. and another great renaissance scholar, john symonds, declared that "hepresents the spirit of the 15th century at its very best."among his friends was the pontifical secretary, leonardo dato, one of the learned men of his age, who during that memorable stroll in the vatican gardens brought the conversation around to cryptology. "you've always been interested in these secrets of nature," dato said. "what do you think of these decipherers? have you tried your hand at it, as much as you know how to?"alberti smiled. he knew that date's duties included ciphers (it was before the curia had a separate cipher secretary). "you're the head of the papel secretariat," he teased. "could it be that you had to use the sethings a few times in matters of great importance to his holiness?""that's why i brought it up," dato replied candidly. "and because of the post i have, i want to be able to do it myself without having to use outside interpreters. for when they bring me letters in cipher interceptedby spies, it's no joking matter. so please—if you've thought up any new ideas having to do with this business, tell me about them." so alberti promised that he would do some work on it so that dato would see that it was profitable to have asked him, and the result was the essay that he wrote in 1466 or early 1467, when he was 62 or 63.he implied that he thought up the idea of frequency analysis all by himself, but the conception that he set forth is far too matured for that. nevertheless, his remarkably lucid latin essay, totaling about 25 manuscript pages, constitutes the west's oldest extant text on cryptanalysis