Ministerul Educaţiei și Cercetării al Republicii Moldova
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică și Microelectronică

Departamentul Ingineria Software și Automatică

Report

For lab Nr. 2

Course: „Cryptographic methods of information protection”

Elaborated:

Popescu Nichifor, gr. FAF-212

Verified:

Cătălin Mîţu

Chişinău - 2023

Subject: Criptanaliza cifrurilor monoalfabetice

Tasks:

1. 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.

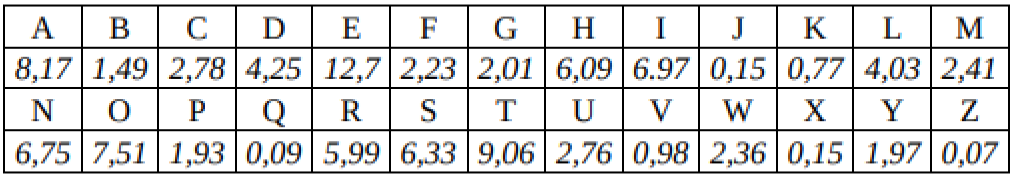
Notă: utilizați serviciul:

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

info

The weak point of mono alphabetic encryption systems is the frequency of occurrence of characters in the text. If an encrypted text is long enough and the language in which it is written is known clear text, the system can be broken by an attack based on the frequency of occurrence of letters in a language(attack by frequency analysis), this frequency being an intensively studied problem (not necessarily in cryptographic purposes) and as a result various order structures were built relative to the frequency the appearance of letters in every European language and in other languages.Usually, the longer a cipher text is, the closer the frequency of the letters used is this general order. A comparison between the two order relationships (that of the characters in the text encrypted and that of the letters from the alphabet of the current language) leads to the realization of several correspondences (letter clear text – encrypted text letter), which uniquely establishes the encryption key.

For the English language, we have the situation presented in table 1 and figure 1:



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*

Table 1 – The frequency of the letters in english alphabet

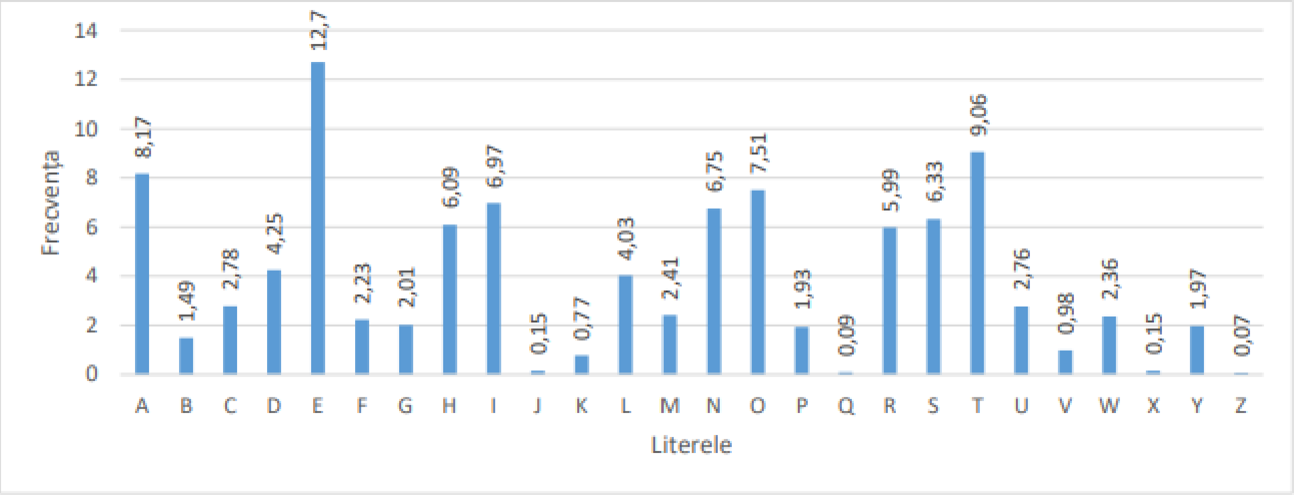
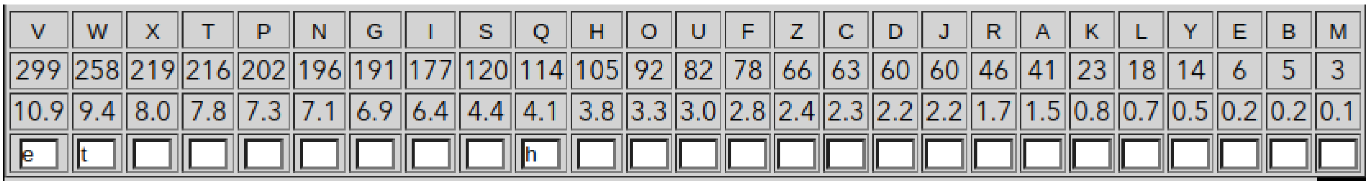


Figure 1 – The frequency of the letters in english alphabet

Results:

The first step is to find to frequency of all letters using https://crypto.interactive-maths.com :



V	W	X	T	P	N	G	I	S	Q	H	O	U	F	Z	C	D	J	R	A	K	L	Y	E	B	M
299	258	219	216	202	196	191	177	120	114	105	92	82	78	66	63	60	60	46	41	23	18	14	6	5	3
10.9	9.4	8.0	7.8	7.3	7.1	6.9	6.4	4.4	4.1	3.8	3.3	3.0	2.8	2.4	2.3	2.2	2.2	1.7	1.5	0.8	0.7	0.5	0.2	0.2	0.1
e	t								h																

Figure 2 – The frequencies of the intercept

I put the most common letters as "e" and "t" , then I found the word tQe so Q=h.Then we have got:

ODIXGJ TSS thePe FeTIP, HIFUtNSNJF RTP THBDXIXGJ T tTXGt thTt SXGJeIPeKeG tNOTF—the HNGKXHtXNG XG the ZXGOP NC ZTGF UeNUSe thTt HIFUtNSNJFXP T ASTHL TIt, T CNIZ NC NHHDStXPZ RhNPe UITHtXtXNGeI ZDPt, XG RXSSXTZ C.CIXeOZTG'P TUt UhITPe, "UeICNIHe HNZZDGe OTXSF RXth OTIL PUXIXtP tNTHHNZUSXPh hXP CeTtP NC ZeGtTS EXD-EXtPD."XG UTIt Xt XP T LXGO NC JDXSt AF TPPNHXTtXNG. CINZ the eTISF OTFP NC XtPeYXPteGHe, HIFUtNSNJF hTO PeIKeO tN NAPHDIe HIXtXHTS UNItXNGP NC RIXtXGJPOeTSXGJ RXth the UNteGt PDAEeHt NC ZTJXH—OXKXGTtXNGP, PUeSSP, HDIPeP,RhTteKeI HNGCeIIeO PDUeIGTtDITS UNReIP NG XtP PNIHeIeIP. TGNtheIXZUNItTGt CTHtNI RTP the HNGCDPXNG NC HIFUtNSNJF RXth the EeRXPhLTAATSTh.ADt, XZUNItTGt TP TSS thePe ReIe, the KXeR thTt HIFUtNSNJF XP ASTHLZTJXH XG XtPeSC PUIXGJP DStXZTteSF CINZ T PDUeICXHXTS IePeZASTGHe AetReeGHIFUtNSNJF TGO OXKXGTtXNG. eYtITHtXGJ TG XGteSSXJXASe ZePPTJe CINZHXUheIteYt PeeZeO tN Ae eYTHtSF the PTZe thXGJ TP NAtTXGXGJ LGNRSeOJeAF eYTZXGXGJ the CSXJht NC AXIOP, the SNHTtXNG NC PtTIP TGO USTGetP, theSeGJth TGO XGteIPeHtXNGP NC SXGeP XG the hTGO, the eGtITXSP NC PheeU, theUNPXtXNG NC OIeJP XG T teTHDU. XG TSS NC thePe, the RXMTIO-SXLe NUeITtNIOITRP PeGPe CINZ JINtePBDe, DGCTZXSXTI, TGO TUUTIeGtSF ZeTGXGJSePPPXJGP. he ZTLeP LGNRG the DGLGNRG.TSS thXP PtTXGeO HIFUtNSNJF PN OeeUSF RXth the OTIL hDeP NC ePNteIXPZthTt PNZe NC theZ PtXSS UeIPXPt, GNtXHeTASF HNSNIXGJ the UDASXH XZTJe NCHIFUtNSNJF. UeNUSe PtXSS thXGL HIFUtTGTSFPXP ZFPteIXNDP. ANNL OeTSeIP PtXSSSXPt HIFUtNSNJF DGOeI "NHHDSt." TGO XG 1940 the DGXteO PtTteP HNGCeIIeODUNG XtP ETUTGePe OXUSNZTtXH HIFUtTGTSFPeP the HNOeGTZe ZTJXH. XG GNGe NC the PeHIet RIXtXGJ thDP CTI RTP theIe TGF PDPtTXGeOHIFUtTGTSFPXP. NHHTPXNGTS HTPeP, FeP. ADt NC TGF PHXeGHe NC HIFUtTGTSFPXP,theIe RTP GNthXGJ. NGSF HIFUtNJITUhF eYXPteO. TGO theIeCNIe HIFUtNSNJF,RhXHh XGKNSKeP ANth HIFUtNJITUhF TGO HIFUtTGTSFPXP, hTO GNt Fet HNZe XGtN AeXGJ PNCTI TP TSS thePe HDStDIeP—XGHSDOXGJ the RePteIG —ReIe HNGHeIGeO.HIFUtNSNJF RTP ANIG TZNGJ the TITAP. theF ReIe the CXIPt tN OXPHNKeITGO RIXte ONRG the ZethNOP NC HIFUtTGTSFPXP. Th UeNUSe thTt eYUSNOeONDt NC TITAXT XG the 600P TGO CSTZeO NKeI KTPt TIeTP NC the LGNRG RNISOPRXCtSF eGJeGOeIeO NGe NC the hXJhePt HXKXSXMTtXNGP thTt hXPtNIF -hTO FetPeeG. PHXeGHe CSNReIeO. TITA ZeOXHXGe TGO ZTtheZTtXHP AeHTZe the AePtXG the RNISO—CINZ the STtteI, XG CTHt, HNZeP the RNIO "HXUheI." UITHtXHTSTItP CSNDIXPheO. TOZXGXPtITtXKe teHhGXBDeP OeKeSNUeO. the eYDAeITGtHIeTtXKe eGeIJXeP NC PDHh T HDStDIe, eYHSDOeO AF XtP IeSXJXNG CINZ

UTXGtXGJNI PHDSUtDIe, TGO XGPUXIeO AF Xt tN TG eYUSXHTtXNG NC the hNSF LNITG,UNDIeO XGtN SXteITIF UDIPDXtP. PtNIFteSSXGJ, eYeZUSXCXeO AF PheheITMTOe'PthNDPTGO TGO NGe GXJhtP, RNIO-IXOOSeP, IeADPeP, UDGP, TGTJITZP, TGOPXZXSTI JTZeP TANDGOeO; JITZZTI AeHTZe T ZTENI PtDOF. TGO XGHSDOeORTP PeHIet RIXtXGJ.TCteI eYUSTXGXGJ thTt NGe ZTF RIXte XG TG DGLGNRG STGJDTJetN NAtTXGPeHIeHF, XAG TO-ODITXhXZ, THHNIOXGJ tN BTSBTPhTGOX, JTKe PeKeG PFPteZPNC HXUheIP.thXP SXPt eGHNZUTPPeO, CNI the CXIPt tXZe XG HIFUtNJITUhF, ANthtITGPUNPXtXNG TGO PDAPtXtDtXNG HXUheIP. ZNIeNKeI, NGe PFPteZ XP the CXIPtLGNRG HXUheI eKeI tN UINKXOe ZNIe thTG NGe PDAPtXtDte CNI T USTXGteYtSetteI. IeZTILTASe TGO XZUNItTGt TP thXP XP, hNReKeI, Xt XP NKeIPhTONReO AF RhTt CNSSNRP— the CXIPteYUNPXtXNG NG HIFUtTGTSFPXP XG hXPtNIF.

thTt , therefore T= a. I saw aGO that repeats many times so I put n and d, therefore we’ve got and. I saw Xn the, therefore X=i. I saw Dnited, D=u.

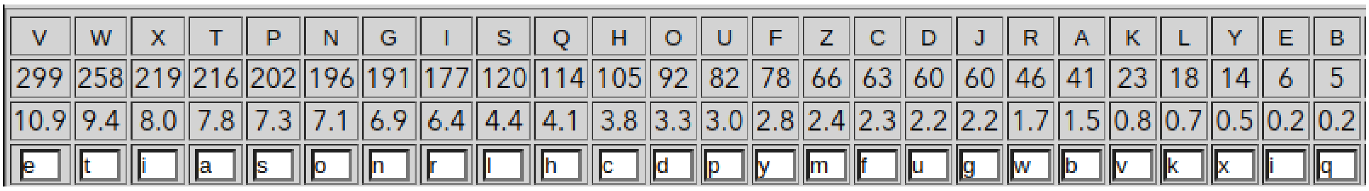
The 1st word of the text is duIinJ , i thought that it might be "during"united PtateP, P=s.

Stars and USanets, Usanets=planets.

"Zessage CrNZHipherteYt seeZed tN Ae eYaHtlF the saZe" Z=m.

supernatural pNRers, pNRers=powers.

toaHHomplish his Ceats oC mental Eiu-Eitsu = to accomplish his ? of mental Jiu-Jitsu.
crFptologF F=y.
Lnown the unLnown L=k.
Aut noticeaAly A=b.
deKeloped , administratiKe K=v.
eYemplified , eYplaining Y=x.
techniBues , grotesBue B=q.
sheheraMade but its correct scheherazade M=z.



V	W	X	T	P	N	G	I	S	Q	H	O	U	F	Z	C	D	J	R	A	K	L	Y	E	B
299	258	219	216	202	196	191	177	120	114	105	92	82	78	66	63	60	60	46	41	23	18	14	6	5
10.9	9.4	8.0	7.8	7.3	7.1	6.9	6.4	4.4	4.1	3.8	3.3	3.0	2.8	2.4	2.3	2.2	2.2	1.7	1.5	0.8	0.7	0.5	0.2	0.2
e	t	i	a	s	o	n	r	l	h	c	d	p	y	m	f	u	g	w	b	v	k	x	i	q

Figure 3 – Final substitutions

Then, the final text is:

During all these years, cryptology was acquiring a taint that lingers even today—the conviction in the minds of many people that cryptology is a black art, a form of occultism whose practitioner must, in william f.friedman's apt phrase, "perforce commune daily with dark spirits to accomplish his feats of mental jiu-jitsu."In part it is a kind of guilt by association. From the early days of its existence, cryptology had served to obscure critical portions of writings dealing with the potent subject of magic—divinations, spells, curses,whatever conferred supernatural powers on its sorcerers. Another important factor was the confusion of cryptology with the jewish. But, important as all these were, the view that cryptology is blackmagic in itself springs ultimately from a superficial resemblance between cryptology and divination. extracting an intelligible message from ciphertext seemed to be exactly the same thing as obtaining knowledge by examining the flight of birds, the location of stars and planets, the length and intersections of lines in the hand, the entrails of sheep, the position of dregs in a teacup. in all of these, the wiMard-like operator draws sense from grotesque, unfamiliar, and apparently meaningless signs. he makes known the unknown.all this stained cryptology so deeply with the dark hues of esoterism that some of them still persist, noticeably coloring the public image of cryptology. People still think cryptanalysis is mysterious. book dealers stylized cryptology under "occult." and in 1940 the United States conferred upon its japanese diplomatic cryptanalysis the codename magic. In none of the secret writing thus far was there any sustained cryptanalysis. occasional cases, yes. But of any science of cryptanalysis,there was nothing. only cryptography existed. and therefore cryptology,which involves both cryptography and cryptanalysis, had not yet come into being so far as all these cultures—including the western —were concerned.cryptology was born among the arabs. They were the first to discover and write down the methods of cryptanalysis. The people that exploded out of Arabia in the 600s and flamed over vast areas of the known world swiftly engendered one of the highest civiliZations that history -had yet seen. science flowered. Arabic medicine and mathematics became the best in the world—from the latter, in fact, comes the word "cipher." practical arts flourished. Administrative techniques developed. the exuberant creative energies of such a culture, excluded by its religion from painting or sculpture, and inspired by it to an explication of the holy koran,poured into literary pursuits. storytelling, exemplified by scheheraZade thousand and one nights, word-riddles, rebuses, puns, anagrams, and similar games abounded; grammar became a major study. and included was secret writing.after explaining that one may write in an unknown language to obtain secrecy, ibn ad-duraihim, according to handi, gave seven systems of ciphers. This list encompassed, for the first time in cryptography, both transposition and substitution ciphers. Moreover, one system is the first known cipher ever to provide more than one substitute for a plaintext letter. remarkable and important as this is, however, it is overshadowed by what follows— the first exposition on cryptanalysis in history.

Conclusion:

In conclusion, the laboratory experiment focused on deciphering a text using Frequency Analysis, a method widely employed in cryptography. Utilizing the online tool at https://crypto.interactive-maths.com significantly facilitated the decryption process, allowing for a systematic analysis of letter frequencies to unveil the hidden message. This method proved effective in breaking simple substitution ciphers and provided valuable insights into the cryptographic patterns within the encrypted text.

Despite the assistance provided by the site, it was notable that deciphering certain words posed a considerable challenge. This difficulty highlighted the complexity of linguistic variations and the nuanced patterns that can arise in encrypted messages. The experience underscores the importance of combining analytical tools with a deep understanding of language and context when engaging in cryptographic analysis. Overall, the laboratory provided valuable insights into the fascinating world of cryptography, revealing both the power and intricacies involved in deciphering messages through Frequency Analysis.

Github link: https://github.com/Nicu22/cs/tree/main