Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego

Laboratorium z przedmiotu:
Wprowadzenie do Kryptologii

Sprawozdanie z ćwiczenia laboratoryjnego nr 1:

Szyfrowanie monoalfabetyczne i multiplikatywne

Prowadzący:
mgr inż. Marta Turowska

Wykonał: Radosław Relidzyński
Grupa: WCY20IY4S1
Data laboratoriów: 14.04.2021 r.

Spis treści

A. Treść zadania 2
B. Mój tekst 2
Wiadmość: 2
Zaszyfrowana wiadmomość przy pomocy szyfrowania monoalfabetycznego (key=5): 2
C. Dane pomocnicze: 2
1. Dane dotyczące częstotliwości wystąpienia liter w języku angielskim: 2
2. Dane dotyczące częstotliwości wystąpienia 2-gramów w języku angielskim: 2
3. Częstotliwość wystąpień liter w moim szyfrogramie: 3
4. Częstotliwość wystąpień 2-gramów w moim szyfrogramie: 3
5. Możliwe kroki podczas odszyfrowywania: 3
D. Kolejne zamiany 3

A. Treść zadania

1. Stworzyć tekst o długości 400-600 znaków.
2. Zaszyfrować go przy pomocy szyfrowania monoapfabetycznego lub multiplikatywnego.
3. Przy pomocy analizy częstości odszyfrować tekst.

B. Mój tekst

Wiadmość:

HELLO! MY NAME IS RADEK AND IM FROM POLAND. I LIVE IN WARSAW AND STUDY IN MILITARY UNIVERSITY OF TECHNOLOGY. IM A STUDENT OF COMPUTER SCIENCE ON THE FOURTH SEMESTER OF STUDY. THIS IS SOME TEXT WHICH I WILL ENCRYPT AND THEN DECRYPT WITH A FREQUENCY OF APPEARANCES. I WILL DO IT BY A MONOALPHABETIC CIPHER. MONOALPHABETIC CIPHER IS A METHOD OF ENCRYPTING TEXT WITH USAGE OF ARRANGEMENT OF LETTERS IN A ALPHABET. WHEN YOU WANT TO ENCRYPT A CHARACTER YOU HAVE TO CONVERT THAT LETTER TO LETTER THAT IS GIVEN STEPS FURTHER IN ALPHABET. YOU HAVE TO NOTE THE FACT THAT THE CHANGES GOES AS A CYCLE.

Zaszyfrowana wiadmomość przy pomocy szyfrowania monoalfabetycznego (key=5):

MJQQT! RD SFRJ NX WFIJP FSI NR KWTR UTQFSI. N QNAJ NS BFWXFB FSI XYZID NS RNQNYFWD ZSNAJWXNYD TK YJHMSTQTLD. NR F XYZIJSY TK HTRUZYJW XHNJSHJ TS YMJ KTZWYM XJRJXYJW TK XYZID. YMNX NX XTRJ YJCY BMNHM N BNQQ JSHWDUY FSI YMJS IJHWDUY BNYM F KWJVZJSHD TK FUUJFWFSHJX. N BNQQ IT NY GD F RTSTFQUMFGJYNH HNUMJW. RTSTFQUMFGJYNH HNUMJW NX F RJYMTI TK JSHWDUYNSL YJCY BNYM ZXFLJ TK FWWFSLJRJSY TK QJYYJWX NS F FQUMFGJY. BMJS DTZ BFSY YT JSHWDUY F HMFWFHYJW DTZ MFAJ YT HTSAJWY YMFY QJYYJW YT QJYYJW YMFY NX LNAJS XYJUX KZWYMJW NS FQUMFGJY. DTZ MFAJ YT STYJ YMJ KFHY YMFY YMJ HMFSLJX LTJX FX F HDHQJ.

C. Dane pomocnicze:

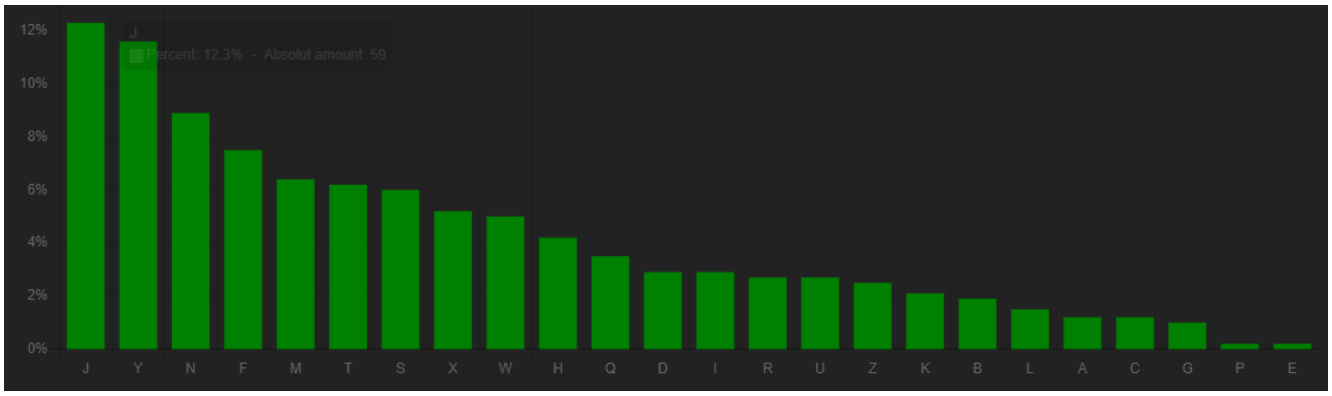
1. Dane dotyczące częstotliwości wystąpienia liter w języku angielskim:

E	T	A	O	I	N	S	R	H	L	D	C	U
12.1%	8.94%	8.55%	7.47%	7.33%	7.17%	6.73%	6.33%	4.96%	4.21%	3.87%	3.16%	2.68%
M	**F**	**G**	**P**	**W**	**Y**	**B**	**V**	**K**	**J**	**X**	**Z**	**Q**
2.53%	2.18%	2.09%	2.07%	1.83%	1.72%	1.6%	1.06%	0.81%	0.22%	0.19%	0.11%	0.1%

2. Dane dotyczące częstotliwości wystąpienia 2-gramów w języku angielskim:

TH	HE	IN	ER	AN	RE	ES	ON	ST	NT	EN	AT	ED	ND	TO
2.71%	2.33%	2.03%	1.78%	1.61%	1.41%	1.32%	1.32%	1.25%	1.17%	1.13%	1.12%	1.08%	1.07%	1.07%
OR	**EA**	**TI**	**AR**	**TE**	**NG**	**AL**	**IT**	**AS**	**IS**	**HA**	**ET**	**SE**	**OU**	**OF**
1.06%	1%	0.99%	0.98%	0.98%	0.89%	0.88%	0.88%	0.87%	0.86%	0.83%	0.76%	0.73%	0.72%	0.71%

3. Częstotliwość wystąpień liter w moim szyfrogramie:



4. Częstotliwość wystąpień 2-gramów w moim szyfrogramie:

5. Możliwe kroki podczas odszyfrowywania:

Sposób S1. Analiza częstotliwości znaków.
Sposób S2. Analiza częstotliwości 2-gramów.
Sposób S3. Własna, subiektywna analiza na podstawie znajomości słów z języka angielskiego.

D. Kolejne zamiany

Na początku wszystkie znaki będą napisane małą literą. Po dokonaniu zamiany podmienione litery będą wyróżnione poprzez zamianę ich na wielkie.

0. Stan początkowy:

hello! my name is radek and im from poland. i live in warsaw and study in military university of technology. im a student of computer science on the fourth semester of study. this is some text which i will encrypt and then decrypt with a frequency of appearances. i will do it by a monoalphabetic cipher. monoalphabetic cipher is a method of encrypting text with usage of arrangement of letters in a alphabet. when you want to encrypt a character you have to convert that letter to letter that is given steps further in alphabet. you have to note the fact that the changes goes as a cycle.

1. Zamieniam „J” na „E” (S1, najczęstszy znak):

mEqqt! rd sfrE nx wfiEp fsi nr kwtr utqfsi. n qnaE ns bfwxfb fsi xyzid ns rnqnyfwd zsnaEwxnyd tk yEhmstqtld. nr f xyziEsy tk htruzyEw xhnEshE ts ymE ktzwym xErExyEw tk xyzid. ymnx nx xtrE yEcy bmnhm n bnqq Eshwduy fsi ymEs iEhwduy bnym f kwEvzEshd tk fuuEfwfshEx. n bnqq it ny gd f rtstfqumfgEynh hnumEw. rtstfqumfgEynh hnumEw nx f rEymti tk Eshwduynsl yEcy bnym zxflE tk fwwfslErEsy tk qEyyEwx ns f fqumfgEy. bmEs dtz bfsy yt Eshwduy f hmfwfhyEw dtz mfaE yt htsaEwy ymfy qEyyEw yt qEyyEw ymfy nx lnaEs xyEux kzwymEw ns fqumfgEy. dtz mfaE yt styE ymE kfhy ymfy ymE hmfslEx ltEx fx f hdhqE.

2. Zamieniam „Y” na „T” (S1, drugi najczęstszy znak):

mEqqt! rd sfrE nx wfiEp fsi nr kwtr utqfsi. n qnaE ns bfwxfb fsi xTzid ns rnqnTfwd zsnaEwxnTd tk TEhmstqtld. nr f xTziEsT tk htruzTEw xhnEshE ts TmE ktzwTm xErExTEw tk xTzid. Tmnx nx xtrE TEcT bmnhm n bnqq EshwduT fsi TmEs iEhwduT bnTm f kwEvzEshd tk fuuEfwfshEx. n bnqq it nT gd f rtstfqumfgETnh hnumEw. rtstfqumfgETnh hnumEw nx f rETmti tk EshwduTnsl TEcT bnTm zxflE tk fwwfslErEsT tk qETTEwx ns f fqumfgET. bmEs dtz bfsT Tt EshwduT f hmfwfhTEw dtz mfaE Tt htsaEwT TmfT qETTEw Tt qETTEw TmfT nx lnaEs xTEux kzwTmEw ns fqumfgET. dtz mfaE Tt stTE TmE kfhT TmfT TmE hmfslEx ltEx fx f hdhqE.

3. Zamieniam „F” na „A” (S1, trzeci najczęstszy znak):

mEqqt! rd sArE nx wAiEp Asi nr kwtr utqAsi. n qnaE ns bAwxAb Asi xTzid ns rnqnTAwd zsnaEwxnTd tk TEhmstqtld. nr A xTziEsT tk htruzTEw xhnEshE ts TmE ktzwTm xErExTEw tk xTzid. Tmnx nx xtrE TEcT bmnhm n bnqq EshwduT Asi TmEs iEhwduT bnTm A kwEvzEshd tk AuuEAwAshEx. n bnqq it nT gd A rtstAqumAgETnh hnumEw. rtstAqumAgETnh hnumEw nx A rETmti tk EshwduTnsl TEcT bnTm zxAlE tk AwwAslErEsT tk qETTEwx ns A AqumAgET. bmEs dtz bAsT Tt EshwduT A hmAwAhTEw dtz mAaE Tt htsaEwT TmAT qETTEw Tt qETTEw TmAT nx lnaEs xTEux kzwTmEw ns AqumAgET. dtz mAaE Tt stTE TmE kAhT TmAT TmE hmAslEx ltEx Ax A hdhqE.

4. Zamieniam „T” na „O” (S1, czwarty najczęstszy znak):

mEqqO! rd sArE nx wAiEp Asi nr kwOr uOqAsi. n qnaE ns bAwxAb Asi xTzid ns rnqnTAwd zsnaEwxnTd Ok TEhmsOqOld. nr A xTziEsT Ok hOruzTEw xhnEshE Os TmE kOzwTm xErExTEw Ok xTzid. Tmnx nx xOrE TEcT bmnhm n bnqq EshwduT Asi TmEs iEhwduT bnTm A kwEvzEshd Ok AuuEAwAshEx. n bnqq iO nT gd A rOsOAqumAgETnh hnumEw. rOsOAqumAgETnh hnumEw nx A rETmOi Ok EshwduTnsl TEcT bnTm zxAlE Ok AwwAslErEsT Ok qETTEwx ns A AqumAgET. bmEs dOz bAsT TO EshwduT A hmAwAhTEw dOz mAaE TO hOsaEwT TmAT qETTEw TO qETTEw TmAT nx lnaEs xTEux kzwTmEw ns AqumAgET. dOz mAaE TO sOTE TmE kAhT TmAT TmE hmAslEx lOEx Ax A hdhqE.

5. Zamieniam „N” na „I” (S1, piąty najczęstszy znak):

mEqqO! rd sArE Ix wAiEp Asi Ir kwOr uOqAsi. I qIaE Is bAwxAb Asi xTzid Is rIqITAwd zsIaEwxITd Ok TEhmsOqOld. Ir A xTziEsT Ok hOruzTEw xhIEshE Os TmE kOzwTm xErExTEw Ok xTzid. TmIx Ix xOrE TEcT bmIhm I bIqq EshwduT Asi TmEs iEhwduT bITm A kwEvzEshd Ok AuuEAwAshEx. I bIqq iO IT gd A rOsOAqumAgETIh hIumEw. rOsOAqumAgETIh hIumEw Ix A rETmOi Ok EshwduTIsl TEcT bITm zxAlE Ok AwwAslErEsT Ok qETTEwx Is A AqumAgET. bmEs dOz bAsT TO EshwduT A hmAwAhTEw dOz mAaE TO hOsaEwT TmAT qETTEw TO qETTEw TmAT Ix lIaEs xTEux kzwTmEw Is AqumAgET. dOz mAaE TO sOTE TmE kAhT TmAT TmE hmAslEx lOEx Ax A hdhqE.

6. Zamieniam „S” na „N” (S1, szósty najczęstszy znak):

mEqqO! rd NArE Ix wAiEp ANi Ir kwOr uOqANi. I qIaE IN bAwxAb ANi xTzid IN rIqITAwd zNIaEwxITd Ok TEhmNOqOld. Ir A xTziENT Ok hOruzTEw xhIENhE ON TmE kOzwTm xErExTEw Ok xTzid. TmIx Ix xOrE TEcT bmIhm I bIqq ENhwduT ANi TmEN iEhwduT bITm A kwEvzENhd Ok AuuEAwANhEx. I bIqq iO IT gd A rONOAqumAgETIh hIumEw. rONOAqumAgETIh hIumEw Ix A rETmOi Ok ENhwduTINl TEcT bITm zxAlE Ok AwwANlErENT Ok qETTEwx IN A AqumAgET. bmEN dOz bANT TO ENhwduT A hmAwAhTEw dOz mAaE TO hONaEwT TmAT qETTEw TO qETTEw TmAT Ix lIaEN xTEux kzwTmEw IN AqumAgET. dOz mAaE TO NOTE TmE kAhT TmAT TmE hmANlEx lOEx Ax A hdhqE.

7. Zamieniam „M” na „H” (S3, pierwsze słowo to „HELLO”):

HEqqO! rd NArE Ix wAiEp ANi Ir kwOr uOqANi. I qIaE IN bAwxAb ANi xTzid IN rIqITAwd zNIaEwxITd Ok TEhHNOqOld. Ir A xTziENT Ok hOruzTEw xhIENhE ON THE kOzwTH xErExTEw Ok xTzid. THIx Ix xOrE TEcT bHIhH

I bIqq ENhwduT ANi THEN iEhwduT bITH A kwEvzENhd Ok AuuEAwANhEx. I bIqq iO IT gd A rONOAquHAgETIh hIuHEw. rONOAquHAgETIh hIuHEw Ix A rETHOi Ok ENhwduTINl TEcT bITH zxAlE Ok AwwANlErENT Ok qETTEwx IN A AquHAgET. bHEN dOz bANT TO ENhwduT A hHAwAhTEw dOz HAaE TO hONaEwT THAT qETTEw TO qETTEw THAT Ix lIaEN xTEux kzwTHEw IN AquHAgET. dOz HAaE TO NOTE THE kAhT THAT THE hHANlEx lOEx Ax A hdhqE.

8. Zamieniam „Q” na „L” (S3, pierwsze słowo to „HELLO”):

HELLO! rd NArE Ix wAiEp ANi Ir kwOr uOLANi. I LIaE IN bAwxAb ANi xTzid IN rILITAwd zNIaEwxITd Ok TEhHNOLOld. Ir A xTziENT Ok hOruzTEw xhIENhE ON THE kOzwTH xErExTEw Ok xTzid. THIx Ix xOrE TEcT bHIhH I bILL ENhwduT ANi THEN iEhwduT bITH A kwEvzENhd Ok AuuEAwANhEx. I bILL iO IT gd A rONOALuHAgETIh hIuHEw. rONOALuHAgETIh hIuHEw Ix A rETHOi Ok ENhwduTINl TEcT bITH zxAlE Ok AwwANlErENT Ok LETTEwx IN A ALuHAgET. bHEN dOz bANT TO ENhwduT A hHAwAhTEw dOz HAaE TO hONaEwT THAT LETTEw TO LETTEw THAT Ix lIaEN xTEux kzwTHEw IN ALuHAgET. dOz HAaE TO NOTE THE kAhT THAT THE hHANlEx lOEx Ax A hdhLE.

9. Zamieniam „R” na „M” (S3, trzecie słowo to „NAME”):

HELLO! Md NAME Ix wAiEp ANi IM kwOM uOLANi. I LIaE IN bAwxAb ANi xTzid IN MILITAwd zNIaEwxITd Ok TEhHNOLOld. IM A xTziENT Ok hOMuzTEw xhIENhE ON THE kOzwTH xEMExTEw Ok xTzid. THIx Ix xOME TEcT bHIhH I bILL ENhwduT ANi THEN iEhwduT bITH A kwEvzENhd Ok AuuEAwANhEx. I bILL iO IT gd A MONOALuHAgETIh hIuHEw. MONOALuHAgETIh hIuHEw Ix A METHOi Ok ENhwduTINl TEcT bITH zxAlE Ok AwwANlEMENT Ok LETTEwx IN A ALuHAgET. bHEN dOz bANT TO ENhwduT A hHAwAhTEw dOz HAaE TO hONaEwT THAT LETTEw TO LETTEw THAT Ix lIaEN xTEux kzwTHEw IN ALuHAgET. dOz HAaE TO NOTE THE kAhT THAT THE hHANlEx lOEx Ax A hdhLE.

10. Zamieniam „X” na „S” (S3, czwarte słowo to „IS”):

HELLO! Md NAME IS wAiEp ANi IM kwOM uOLANi. I LIaE IN bAwSAb ANi STzid IN MILITAwd zNIaEwSITd Ok TEhHNOLOld. IM A STziENT Ok hOMuzTEw ShIENhE ON THE kOzwTH SEMESTEw Ok STzid. THIS IS SOME TEcT bHIhH I bILL ENhwduT ANi THEN iEhwduT bITH A kwEvzENhd Ok AuuEAwANhES. I bILL iO IT gd A MONOALuHAgETIh hIuHEw. MONOALuHAgETIh hIuHEw IS A METHOi Ok ENhwduTINl TEcT bITH zSAlE Ok AwwANlEMENT Ok LETTEwS IN A ALuHAgET. bHEN dOz bANT TO ENhwduT A hHAwAhTEw dOz HAaE TO hONaEwT THAT LETTEw TO LETTEw THAT IS lIaEN STEuS kzwTHEw IN ALuHAgET. dOz HAaE TO NOTE THE kAhT THAT THE hHANlES lOES AS A hdhLE.

11. Zamieniam „D” na „Y” (S3, drugie słowo to „MY”):

HELLO! MY NAME IS wAiEp ANi IM kwOM uOLANi. I LIaE IN bAwSAb ANi STziY IN MILITAwY zNIaEwSITY Ok TEhHNOLOlY. IM A STziENT Ok hOMuzTEw ShIENhE ON THE kOzwTH SEMESTEw Ok STziY. THIS IS SOME TEcT bHIhH I bILL ENhwYuT ANi THEN iEhwYuT bITH A kwEvzENhY Ok AuuEAwANhES. I bILL iO IT gY A MONOALuHAgETIh hIuHEw. MONOALuHAgETIh hIuHEw IS A METHOi Ok ENhwYuTINl TEcT bITH zSAlE Ok AwwANlEMENT Ok LETTEwS IN A ALuHAgET. bHEN YOz bANT TO ENhwYuT A hHAwAhTEw YOz HAaE TO hONaEwT THAT LETTEw TO LETTEw THAT IS lIaEN STEuS kzwTHEw IN ALuHAgET. YOz HAaE TO NOTE THE kAhT THAT THE hHANlES lOES AS A hYhLE.

12. Zamieniam „I” na „D” (S3, szóste słowo to „AND”):

HELLO! MY NAME IS wADEp AND IM kwOM uOLAND. I LIaE IN bAwSAb AND STzDY IN MILITAwY zNIaEwSITY Ok TEhHNOLOlY. IM A STzDENT Ok hOMuzTEw ShIENhE ON THE kOzwTH SEMESTEw Ok STzDY. THIS IS SOME TEcT bHIhH I bILL ENhwYuT AND THEN DEhwYuT bITH A kwEvzENhY Ok AuuEAwANhES. I bILL DO IT gY A MONOALuHAgETIh hIuHEw. MONOALuHAgETIh hIuHEw IS A METHOD Ok ENhwYuTINl TEcT bITH zSAlE Ok

AwwANlEMENT Ok LETTEwS IN A ALuHAgET. bHEN YOz bANT TO ENhwYuT A hHAwAhTEw YOz HAaE TO hONaEwT THAT LETTEw TO LETTEw THAT IS lIaEN STEuS kzwTHEw IN ALuHAgET. YOz HAaE TO NOTE THE kAhT THAT THE hHANlES lOES AS A hYhLE.

13. Zamieniam „L” na „G” (S3, trzecie ostatnie słowo to „GOES”):

HELLO! MY NAME IS wADEp AND IM kwOM uOLAND. I LIaE IN bAwSAb AND STzDY IN MILITAwY zNIaEwSITY Ok TEhHNOLOGY. IM A STzDENT Ok hOMuzTEw ShIENhE ON THE kOzwTH SEMESTEw Ok STzDY. THIS IS SOME TEcT bHIhH I bILL ENhwYuT AND THEN DEhwYuT bITH A kwEvzENhY Ok AuuEAwANhES. I bILL DO IT gY A MONOALuHAgETIh hIuHEw. MONOALuHAgETIh hIuHEw IS A METHOD Ok ENhwYuTING TEcT bITH zSAGE Ok AwwANGEMENT Ok LETTEwS IN A ALuHAgET. bHEN YOz bANT TO ENhwYuT A hHAwAhTEw YOz HAaE TO hONaEwT THAT LETTEw TO LETTEw THAT IS GIaEN STEuS kzwTHEw IN ALuHAgET. YOz HAaE TO NOTE THE kAhT THAT THE hHANGES GOES AS A hYhLE.

14. Zamieniam „H” na „C” (S3, drugie ostatnie słowo to „CYCLE”):

HELLO! MY NAME IS wADEp AND IM kwOM uOLAND. I LIaE IN bAwSAb AND STzDY IN MILITAwY zNIaEwSITY Ok TECHNOLOGY. IM A STzDENT Ok COMuzTEw SCIENCE ON THE kOzwTH SEMESTEw Ok STzDY. THIS IS SOME TEcT bHICH I bILL ENCwYuT AND THEN DECwYuT bITH A kwEvzENCY Ok AuuEAwANCES. I bILL DO IT gY A MONOALuHAgETIC CIuHEw. MONOALuHAgETIC CIuHEw IS A METHOD Ok ENCwYuTING TEcT bITH zSAGE Ok AwwANGEMENT Ok LETTEwS IN A ALuHAgET. bHEN YOz bANT TO ENCwYuT A CHAwACTEw YOz HAaE TO CONaEwT THAT LETTEw TO LETTEw THAT IS GIaEN STEuS kzwTHEw IN ALuHAgET. YOz HAaE TO NOTE THE kACT THAT THE CHANGES GOES AS A CYCLE.

15. Zamieniam „K” na „F” (S2, regularnie powtarza się zapis „Ok”, a 2-gramem o dużej częstotliwości występowania zaczynającym się na O w języku angielskim „OF” – następny po „ON”, ale to już jest w pełni rozszyfrowane):

HELLO! MY NAME IS wADEp AND IM FwOM uOLAND. I LIaE IN bAwSAb AND STzDY IN MILITAwY zNIaEwSITY OF TECHNOLOGY. IM A STzDENT OF COMuzTEw SCIENCE ON THE FOzwTH SEMESTEw OF STzDY. THIS IS SOME TEcT bHICH I bILL ENCwYuT AND THEN DECwYuT bITH A FwEvzENCY OF AuuEAwANCES. I bILL DO IT gY A MONOALuHAgETIC CIuHEw. MONOALuHAgETIC CIuHEw IS A METHOD OF ENCwYuTING TEcT bITH zSAGE OF AwwANGEMENT OF LETTEwS IN A ALuHAgET. bHEN YOz bANT TO ENCwYuT A CHAwACTEw YOz HAaE TO CONaEwT THAT LETTEw TO LETTEw THAT IS GIaEN STEuS FzwTHEw IN ALuHAgET. YOz HAaE TO NOTE THE FACT THAT THE CHANGES GOES AS A CYCLE.

16. Zamieniam „U” na „P” (S3, w okolicy środka tekstu jest słowo „MONOALPHABETIC”):

HELLO! MY NAME IS wADEp AND IM FwOM POLAND. I LIaE IN bAwSAb AND STzDY IN MILITAwY zNIaEwSITY OF TECHNOLOGY. IM A STzDENT OF COMPzTEw SCIENCE ON THE FOzwTH SEMESTEw OF STzDY. THIS IS SOME TEcT bHICH I bILL ENCwYPT AND THEN DECwYPT bITH A FwEvzENCY OF APPEAwANCES. I bILL DO IT gY A MONOALPHAgETIC CIPHEw. MONOALPHAgETIC CIPHEw IS A METHOD OF ENCwYPTING TEcT bITH zSAGE OF AwwANGEMENT OF LETTEwS IN A ALPHAgET. bHEN YOz bANT TO ENCwYPT A CHAwACTEw YOz HAaE TO CONaEwT THAT LETTEw TO LETTEw THAT IS GIaEN STEPS FzwTHEw IN ALPHAgET. YOz HAaE TO NOTE THE FACT THAT THE CHANGES GOES AS A CYCLE.

17. Zamieniam „G” na „B” (S3, w okolicy środka tekstu jest słowo „MONOALPHABETIC”):

HELLO! MY NAME IS wADEp AND IM FwOM POLAND. I LIaE IN bAwSAb AND STzDY IN MILITAwY zNIaEwSITY OF TECHNOLOGY. IM A STzDENT OF COMPzTEw SCIENCE ON THE FOzwTH SEMESTEw OF STzDY. THIS IS SOME TEcT bHICH I bILL ENCwYPT AND THEN DECwYPT bITH A FwEvzENCY OF APPEAwANCES. I bILL DO IT BY A MONOALPHABETIC CIPHEw. MONOALPHABETIC CIPHEw IS A METHOD OF ENCwYPTING TEcT bITH zSAGE OF

AwwANGEMENT OF LETTEwS IN A ALPHABET. bHEN YOz bANT TO ENCwYPT A CHAwACTEw YOz HAaE TO CONaEwT THAT LETTEw TO LETTEw THAT IS GIaEN STEPS FzwTHEw IN ALPHABET. YOz HAaE TO NOTE THE FACT THAT THE CHANGES GOES AS A CYCLE.

18. Zamieniam „W” na „R” (S3, występuje słowo „LETTER”):

HELLO! MY NAME IS RADEp AND IM FROM POLAND. I LIaE IN bARSAb AND STzDY IN MILITARY zNIaERSITY OF TECHNOLOGY. IM A STzDENT OF COMPzTER SCIENCE ON THE FOzRTH SEMESTER OF STzDY. THIS IS SOME TEcT bHICH I bILL ENCRYPT AND THEN DECRYPT bITH A FREvzENCY OF APPEARANCES. I bILL DO IT BY A MONOALPHABETIC CIPHER. MONOALPHABETIC CIPHER IS A METHOD OF ENCRYPTING TEcT bITH zSAGE OF ARRANGEMENT OF LETTERS IN A ALPHABET. bHEN YOz bANT TO ENCRYPT A CHARACTER YOz HAaE TO CONaERT THAT LETTER TO LETTER THAT IS GIaEN STEPS FzRTHER IN ALPHABET. YOz HAaE TO NOTE THE FACT THAT THE CHANGES GOES AS A CYCLE.

19. Zamieniam „A” na „V” (S3, występuje słowo „GIVEN”):

HELLO! MY NAME IS RADEp AND IM FROM POLAND. I LIVE IN bARSAb AND STzDY IN MILITARY zNIVERSITY OF TECHNOLOGY. IM A STzDENT OF COMPzTER SCIENCE ON THE FOzRTH SEMESTER OF STzDY. THIS IS SOME TEcT bHICH I bILL ENCRYPT AND THEN DECRYPT bITH A FREvzENCY OF APPEARANCES. I bILL DO IT BY A MONOALPHABETIC CIPHER. MONOALPHABETIC CIPHER IS A METHOD OF ENCRYPTING TEcT bITH zSAGE OF ARRANGEMENT OF LETTERS IN A ALPHABET. bHEN YOz bANT TO ENCRYPT A CHARACTER YOz HAVE TO CONVERT THAT LETTER TO LETTER THAT IS GIVEN STEPS FzRTHER IN ALPHABET. YOz HAVE TO NOTE THE FACT THAT THE CHANGES GOES AS A CYCLE.

20. Zamieniam „Z” na „U” (S3, występuje słowo „YOU”):

HELLO! MY NAME IS RADEp AND IM FROM POLAND. I LIVE IN bARSAb AND STUDY IN MILITARY UNIVERSITY OF TECHNOLOGY. IM A STUDENT OF COMPUTER SCIENCE ON THE FOURTH SEMESTER OF STUDY. THIS IS SOME TEcT bHICH I bILL ENCRYPT AND THEN DECRYPT bITH A FREvUENCY OF APPEARANCES. I bILL DO IT BY A MONOALPHABETIC CIPHER. MONOALPHABETIC CIPHER IS A METHOD OF ENCRYPTING TEcT bITH USAGE OF ARRANGEMENT OF LETTERS IN A ALPHABET. bHEN YOU bANT TO ENCRYPT A CHARACTER YOU HAVE TO CONVERT THAT LETTER TO LETTER THAT IS GIVEN STEPS FURTHER IN ALPHABET. YOU HAVE TO NOTE THE FACT THAT THE CHANGES GOES AS A CYCLE.

21. Zamieniam „B” na „W” (S3, występuje słowo „WANT” oraz „WHEN”):

HELLO! MY NAME IS RADEp AND IM FROM POLAND. I LIVE IN WARSAW AND STUDY IN MILITARY UNIVERSITY OF TECHNOLOGY. IM A STUDENT OF COMPUTER SCIENCE ON THE FOURTH SEMESTER OF STUDY. THIS IS SOME TEcT WHICH I WILL ENCRYPT AND THEN DECRYPT WITH A FREvUENCY OF APPEARANCES. I WILL DO IT BY A MONOALPHABETIC CIPHER. MONOALPHABETIC CIPHER IS A METHOD OF ENCRYPTING TEcT WITH USAGE OF ARRANGEMENT OF LETTERS IN A ALPHABET. WHEN YOU WANT TO ENCRYPT A CHARACTER YOU HAVE TO CONVERT THAT LETTER TO LETTER THAT IS GIVEN STEPS FURTHER IN ALPHABET. YOU HAVE TO NOTE THE FACT THAT THE CHANGES GOES AS A CYCLE.

22. Zamieniam „V” na „Q” (S3, występuje słowo „FREQUENCY”):

HELLO! MY NAME IS RADEp AND IM FROM POLAND. I LIVE IN WARSAW AND STUDY IN MILITARY UNIVERSITY OF TECHNOLOGY. IM A STUDENT OF COMPUTER SCIENCE ON THE FOURTH SEMESTER OF STUDY. THIS IS SOME TEcT WHICH I WILL ENCRYPT AND THEN DECRYPT WITH A FREQUENCY OF APPEARANCES. I WILL DO IT BY A MONOALPHABETIC CIPHER. MONOALPHABETIC CIPHER IS A METHOD OF ENCRYPTING TEcT WITH USAGE OF ARRANGEMENT OF LETTERS IN A ALPHABET. WHEN YOU WANT TO ENCRYPT A CHARACTER YOU HAVE TO

CONVERT THAT LETTER TO LETTER THAT IS GIVEN STEPS FURTHER IN ALPHABET. YOU HAVE TO NOTE THE FACT THAT THE CHANGES GOES AS A CYCLE.

23. Zamieniam „C” na „X” (S3, występuje słowo „TEXT”):

HELLO! MY NAME IS RADEp AND IM FROM POLAND. I LIVE IN WARSAW AND STUDY IN MILITARY UNIVERSITY OF TECHNOLOGY. IM A STUDENT OF COMPUTER SCIENCE ON THE FOURTH SEMESTER OF STUDY. THIS IS SOME TEXT WHICH I WILL ENCRYPT AND THEN DECRYPT WITH A FREQUENCY OF APPEARANCES. I WILL DO IT BY A MONOALPHABETIC CIPHER. MONOALPHABETIC CIPHER IS A METHOD OF ENCRYPTING TEXT WITH USAGE OF ARRANGEMENT OF LETTERS IN A ALPHABET. WHEN YOU WANT TO ENCRYPT A CHARACTER YOU HAVE TO CONVERT THAT LETTER TO LETTER THAT IS GIVEN STEPS FURTHER IN ALPHABET. YOU HAVE TO NOTE THE FACT THAT THE CHANGES GOES AS A CYCLE.

24. Zamieniam „P” na „K” (S3, występuje słowo „RADEK”):

HELLO! MY NAME IS RADEK AND IM FROM POLAND. I LIVE IN WARSAW AND STUDY IN MILITARY UNIVERSITY OF TECHNOLOGY. IM A STUDENT OF COMPUTER SCIENCE ON THE FOURTH SEMESTER OF STUDY. THIS IS SOME TEXT WHICH I WILL ENCRYPT AND THEN DECRYPT WITH A FREQUENCY OF APPEARANCES. I WILL DO IT BY A MONOALPHABETIC CIPHER. MONOALPHABETIC CIPHER IS A METHOD OF ENCRYPTING TEXT WITH USAGE OF ARRANGEMENT OF LETTERS IN A ALPHABET. WHEN YOU WANT TO ENCRYPT A CHARACTER YOU HAVE TO CONVERT THAT LETTER TO LETTER THAT IS GIVEN STEPS FURTHER IN ALPHABET. YOU HAVE TO NOTE THE FACT THAT THE CHANGES GOES AS A CYCLE.

E. Podsumowanie

Zadanie udało się wykonać, końcowy efekt odszyfrowywania zwraca dokładnie tą samą wiadomość, jak ta, która była na wejściu do szyfratora. Rozszyfrowywanie miało w sobie dwa główne etapy, które można między sobą rozróżnić. Pierwszy z nich opierał się bardziej o intuicję i informacje o częstotliwościach wystąpień. Na podstawie tego można było odszyfrować pierwsze znaki. W drugim etapie już większą rolę odgrywała znajomość słów z języka angielskiego. Na podstawie odszyfrowanych znaków można było ocenić, jakie słowo pasuje w dane miejsce, co dawało kolejne znaki do odszyfrowania.