## Лабораторная работа N1

# Взлом моноалфавитного подстановочного шифра методом частотной атаки

Цель работы: ознакомиться на практике с использованием частотной криптоатаки при взломе подстановочных шифров.

#### Исходные данные:

Зашифрованный текст, перечень наиболее часто встречающихся букв в тексте, перечень наиболее часто используемых в русском языке букв.

#### Выходные данные:

Расшифрованный текст.

### Теоретические основы:

Моноалфавитный подстановочный шифр - шифр, в котором каждой букве исходного алфавита поставлена в соответствие одна буква шифра.

Например, возьмем слово «КУКУРУЗА». Пусть букве «К» текста соответствует буква «А» шифра, букве «У» текста соответствует буква «Б» шифра, букве «Р» текста соответствует буква «В» шифра, букве «З» текста соответствует буква «Г» шифра, букве «А» текста соответствует буква «Д» шифра. После подстановки букв шифра вместо букв исходного теста слово «КУКУРУЗА» в зашифрованном виде будет выглядеть как «АБАБВБГД».

Недостатком подобного шифрования является то, что, если какая-то буква встречается в исходном тексте чаще всего (например, буква «О» в русском алфавите), то и соответствующая ей буква шифра в зашифрованном тексте также встречается чаще всего.

В нижеприведенной таблице приведены частоты встречаемости букв в английском тексте (в процентих):

Высокая		Средняя		Низкая	
Е	12,31	L	4,03	В	1,62
Т	9,59	D	3,65	G	1,61
А	8,05	С	3,20	V	0,93
0	7,94	U	3,10	Κ	0,52
Ν	7,19	Р	2,29	Q	0,20
Ι	7,18	F	2,28	Х	0,20
S	6,59	Н	2,25	J	0,10
R	6,03	W	2,03	Z	0,09
Н	5,14	Y	1,88		

Зная частоты наиболее встречающихся букв и подсчитав, какие буквы чаще всего встречаются в шифровке, криптоаналитик может подобрать расшифровку для некоторых букв текста. Затем, анализируя короткие слова, найти еще буквы, истинные значения которых можно с высокой степенью уверенности предугадать. Например, если уже расшифрована буква «О» и в тексте есть слово «ОЫО» (подчеркнуты уже расшифрованные буквы), то, скорее всего, шифру «Ы» соответствует буква «Н» в исходном тексте («ОНО»). Чем дальше расшифровывается текст, тем легче идет процесс расшифровки.

## Методические указания:

1. Запустить на выполнение файл labw01.exe

На экране появится окно выполнения лабораторной работы (рис. 1):



Рисунок 1. Окно выполнения лабораторной работы

В левой части окна находится зашифрованный текст (буквы, выделенные красным цветом). В процессе расшифровки расшифрованные (правильно или неправильно) буквы текста меняют цвет с красного на черный.

Рисунок 2. Изменения окна лабораторной работы после расшифровки одной буквы

Чтобы указать для какой-либо буквы шифра ее истинное (расшифрованное) значение, нужно в поле «Буква в шифре» указать значение буквы, например, "б", а в поле «Заменить на» - ее истинное значение, например, "и", а затем нажать кнопку "Добавить". Результат такого действия приведен на рис. 2.

На рис. 3. Приведено окно выполнения лабораторной работы после добавления расшифровок нескольких букв.

Лабораторная работа N1: Взлом моноалфавитного подстановочного шифра	
- ф рлтмэихож тгму мтдт, тгмр маршер, - л лихиливкюрки, хгмюем мтгктрэ шмэихнюм мттолтр имж лосо.	Показать только замененные Показать закодированный текст
эрткясо мязншрэ чгнтсо. шизихнюм итсрюозяф г сякязк, титрянф хнтфятик, итчэкшюоз щэф, титии оздшюозяф ягикио тнятюкяо, тинюфэ словсо р тямржокя:	Показать частоты
- хн олткч! - нн. хн лислигрек! - р хн низпож вржои!	Буква в шифре Заменить на
- нэф юнл мшмрч! - тлипонкэ гкэрсню. - гихимвюм, - ленхнэ шизихнюм гихимвюм лимюкюдф юк тисринэр кпи. зклн шизихнюм жонз, ьти кпи смитнюмию чрткл	6 = И Ц = Н Ы = Л
р ъти щти чилиакк, лкнемк лиъктнюрк - чртлилти тлр лтизи импоьки ткзк. юм глк вк лрлс щдэ гкэрс. шизихнюм юк имп лкарти нэф лкшф, ькпи кио	я = т
читкания шизикк, этища эртклоо нищая инслитрен и тилтиу титдтер р тки лниди шкх прлен ишклткърз кио кпи низж рэр ътища эртклоо типрш, тилзк ъкпи шизихнюм тлразили ща проскоти лишлтгкиюму вржоиж. ъти зовак?	
тлкти лислигре, юк тингклпнфли итнлюмлтр, рэр глк йкэрсии хн гдлаож лтнгсо? шизихнюм щдэ итдтюди рплисии р тлкслилюм хюнэ итгкт. юм глк вк мнюму	
млтиливюмлтиж кпм чилисткл юк рльклтдгиэлф: тилиу кио им шиэр читкэмли лиимио лрлсюоти вржюж юн эракююму гихночи тэнюктк лислигре.	
эртклео тмункт тклгди. тнемг опмгил. шизихнюм ослнэ смитижткл, тклкннэ кпм эртклсо, р тит низвкю ликэнти тклгож титдтсо. клэр мюн онилтлф, кпм низф шонкт гигик шизиак низр шизихнюм. клэр вк мю типршюкт -	
юнлтотрт мьклкни шизихнюм. лтлнююдк тнлтюклд, лтлнююдк олэмгрф, юм эртклсо итснхдгнэлф нипигнлргнтилф ти-нлопиио, р эклн шизихнюм юк лтнэ лтилрти ли лгири тэкьрлтди симтнюмиоми, эртклсо читкэ гклюотилф л	
лислигреки рэр юк гихглнентилф лиглки. лклкнрюд юк импэм щдти, г щтми мюр мшн щдэр огклкюд.	
шизихнюм тлигкэ тлонюож юмьи. кпи сгнлтрлн г гдлисии лгктэми хннюрр юн	

Рисунок 3. Окно лабораторной работы после расшифровки нескольких букв



Рисунок 4. Процедура удаления ошибочно указанных расшифровок

Чтобы отменить указанную расшифровку буквы, нужно в списке расшифровок мышкой указать соответствующую пару букв и нажать кнопку «Удалить» (рис. 4).

Полоса вертикального скроллинга служит для навигации по расшифровываемому тексту.

2. Начинается частотная атака с анализа частот встречаемости букв в шифровке. Для этих целей в окне выполнения лабораторной работы предусмотрена кнопка «Показать частоты». При ее нажатии на экран выводится перечень десяти наиболее часто встречаемых букв в шифре, а также перечень букв, наиболее часто встречаемых в русском языке (рис. 5).

1	nforma	ation 🔀
	<b>i</b>	Первые 10 самых часто встречающихся букв: (скорее всего одними из первых будут "о", "е", "а", "н", "и", "т", "л") "м" = 503 "к" = 437 "p" = 315 "ц" ("н)" = 307 "Ю" = 303 "я" ("т)" = 267 "Ы" ("л)" = 262 "э" = 244 "л" = 226 "г" = 182
		[OK]

Рисунок 5. Информация о частотах встречаемости букв в шифре

Первым шагом в расшифровке текста может быть указание расшифровки для самой часто встречаемой буквы - буквы «о». Для случая, приведенного на рис. 5, указывается «о» как расшифровка буквы «м» шифра (см. рис. 6).

Рисунок 6. Первый шаг расшифровки - указание расшифровки буквы «о»

Следует помнить, что для конкретного текста частота встречаемости букв может быть несколько иной, чем в среднем для русского языка. Если в русском языке, например, буква

«т» встречается чаще, чем буква «л», то в каком-то конкретном тексте буква «л» вполне может встречаться чаще буквы «т». Поэтому слепо опираться на данные частотного анализа не следует.

3. В зашифрованном тексте осуществляется поиск коротких слов, зашифрованные буквы которых можно предсказать по уже расшифрованным буквам и частотной информации из рис. 5. На рис. 7. в верхней строчке есть фрагмент текста « ою », где «о» уже известно

Лабораторная работа N1: Взлом моноалфавитного подстановочного шифра		
Νούο κακ ππρυομρέ, με ούο ομκειών ταπάκ μεπιμοσά ακεκτάκεσοπι, πιχπιοψηματιή ποσάκιωμας δρπος, πποτεισμακερύ τε τοιμασακ ταπάκι κορό, ειδάμαπραιφιμά τ κειδικομας το ποστεισματικός το τοιμασακ ταπάκι κορό, ειδάμαπραφιμά τ καιδιόσματα το μετάτα το ποστεισματία το μουστάτα το μετάτα τη μετάτα το μετάτα το μετάτα το μετάτα μετάτα το μετάτα το μετάτα μ	Г Показать толь Г Показать зако Буква в шифре М = О	кко замененные одированный текст тоты Заменить на о Добавить Удалить

Рисунок 7. Поиск коротких слов

Лабораторная работа N1: Взлом моноалфавитного подстановочного шифра	
Лабораторная работа N1: Валом моноалфавитного подстановочного шифра мон нк тлрчонрэ, р он омкэмф тклкн цслцноб якэкгксяолц, лцхпэфндгцф тлойкымрж брлог, тлотэдгцжерч г томяояк тклкн нрб, гыбцялргцфыи г хкэкндк, хоэоядк р солрынкгдк тэцнкяд. шэрвк с ояло он лкарэ кек лцх тломбоялкяи тэкнсо о мослогрек. кк шозиак гксц нцхцн оямнфэ осяцг бклэрн, тлоэкяцф нц гдмояк акмярнкыфяр брэи нцн бцэкнисоу шкхгохноаноу тэцнкяоу. мкуьцы сомяр бклэрнц шкэкжя нц лцгнрнк, но тэкнсц мочлцнрэцыи, р сонялщинндк сотрр мяофя нц ьклноб лднск шозиарч нкикп. омялду пэцх сцбялд огрнкз бнопок. гоя мослогрек, ц гоя кпо члцнрякэм. нкмяцлкжеру, шэкмяферу, гкэрькмягкинду нкыфярзояогду лошоя м опзогцядб тлфбоопозиндб яозогрекб р бцзкнисоу, точовку нц ькэогкькысох позогоу, пэцнсоу, шкх кнрнопо гдыяотц. тохцнр нкпо голояц, ояслаядк нцыякви, но гык лцгно нкномяотндк. ц яцб нцэмак - мослогрец, тэонд бцмяклыягц ядыфь брлог, бнопо-бкопо экя нцхин омяцгэкнидк хикым нкрхгкияно тоъкбо. нк тломяо лкхндк сцбнр. нк тломяо тоаэдк сомер яцс нцхдгцкбопо нлцпойкннопо бкяцээц. шопцямяго хцсэжьцэоми нк г ыцбрч бцяклрцэцч: томэкникбо гцлгцло нк тлрнкя г позого тклктэцгряи рч г бклягдк мэряср. хикии члцнрэрым эрэрплцнядк мяцзощяср, сцхцэоми, вргдк р ндацерк. плцгжлд нц мгрийк, толцвцжерк лцхоб р омяцицгэргцжерк мклийк. ьонкындкк рияцэрр нц цпцяк рх бщяклысрч м хцболовкнядч брлог г тоэотцлыкск оя шкмсонкьномяр. ловыдти отцэог, полферч гноялкнирб мгкаб, рысомно мокнрикнндч г флерк овключе, мхопноадк р гдафноадк яцс, ьяо рч мтэкякнрк	Г Показать только замененные Показать закодированный текст Показать частоты Буква в шифре Заменить на ю   н М = О   Добавить Ю = Н Удалить
мокнрикнидч г флерк овклкзиф. ытрлцзи рх лцновнопо нклкгц. тозоыер рх сомяр сцеопо-яо вргоянопо, рхопноядк р гдяфноядк яце, ьяо рч ытэкякнрк хцголцвргцзо грикирфбр тломялцимягц г рноб рхбклкирр. толцхрякзиноу слцмояд лцеогряд, гдлкхциндк ониц г илопоу р очонферк г шкмеонкьномяи. пэциерк эрмяиф шкхдбфиндч иклкгикг. оязэрзогциндк сцбир ы икрхгкыяндч шклкпог. оакзобэфжецф созэксйрф ьонкы, го гыкб ыгокб клерсовктрр члцифецфыф нц тфярикыфяр сгцилцяндч флицч хц голояцбр. площдк эжир, сояолдб ьовно тонрбцирк тлкелцынопо, хцтэцярэр ыгорбр врхифбр хц тотдяер хцгэцикяи щярбр мослогрецбр. ик ицио шозиаопо обц,	

Рисунок 8. Результат расшифровки букв «о» и «н»

Этот фрагмент может быть скорее всего словом « он » В таблице частот (рис. 5) буква «ю» шифра стоит на 5-м месте, что примерно соответствует позиции буквы «н» русского языка (4-е место). Значит разумно попробовать поменять «ю» на «н». Результат приведен на рис. 8.



Рисунок 9. Продолжение поиска коротких понятных слов

Рис. 10. Результат расшифровки букв «о», «н» и «и»

Далее повторяется поиск коротких слов, в которых можно догадаться о значении зашифрованных букв. На рис. 9 в первой и третей строках есть отдельно стоящее «р». Скорее всего это предлог «и», что согласуется и с информацией на рис. 5. Результат замены приведен на рис. 10.

На рис. 11 в первой строке обнаруживается слово из двух известных «и» и шифрованной буквы «э» между ними. Скорее всего это буква «л», образующая слово «или» (рис. 12).





ялкяи мослогие, ик тонгклицфым отщыномяи, или гык йклисоб хц гдмаок мацгео? шолихщно щдл отдяндб иплособ и тлкслцыно хицл оягкя. но гык вк онноу ояколовномаик кпо чцицсакл ик изыклтдиция): толоу кбо но шоли чояклови вщбобо лиженоя и вижних иц лижениор голоу кбо но шоли чояклови литкысо, и яоя нолвки миклцая тклюх тотдасо, кыли онц онциямф, ис пилького я изя нолвки миклцая тклюх тотдасо, кыли онц онциямф, ис литкысо озсидигцияф пологдия тцянкад, ыялинндк сылогиф, ис литкысо озсидигцияф пологдиягцямаф то-илопебо, и экли шолихцию ик мацл ысологиекб или ик гохулицанамаф собщиновоб, и экли шолихцию ик мацл ысологиекб или ик тохулицанамаф собщиновоб, и экли шолихцию ик мацл ысологиекб или ик тохулицанамаф собщиновоб, из якли шолихцию ик мацл тосинояи кк шкх мовцлкныу, литкысо тлкникад нк болло шдяя, г щяоб они ошц щдли огклкнд, шолихцио тислика ноэм, клю сгидяили г гдыособ ыгкялоб хиции иц шклкию шлизиацексно оххлац цили щдли кликанад накелоб колондо вилиси, и такима источная и отилиция, и лиженоб отинд балиств, каое кие к шкх мовцлкныу, литкысо тлкнизад виям г гонжыми ялекоб, воюща тосинояи кк шкх мовцлкныу тилин щда циливасо сояло он иками кек лах тлажанда, коолади, и сониканф тилин щда шлакк с сало он иками кек лах тлажац и на тлячици шклаканана, иклия и кали ниб цикнисоу шкхрозанови г тлацкязу, колодак и солизиндак тилика, кили на балкнисоу шкхрозанови г тлацкязу, колодак и солизици иклакя ид лациник, но тлакиец мочалиниящем, и сонала бклаинц шклакая на лациники, но тлакиец мочалинищик, и соналацищинада сотим мофа на кълиба данок шолизич никикп, овяяду пацу сабкад отиния бколок. гоз мослогиек, д гоз клю чащинакам. икмада тафбоополиндб яологиекб	Табораторная работа N1: Взлом моноалфавитного подстановочного шифра	2
шолихидно щдл отдяндб иплособ и тяксяцыно хнцл оягкя. но гык вк онноу оказловномяяк кпо чилисяял ик изыклядгициф: толоу кбо но шоли чоякломи ыщбобо лимснояи вихниж нц лиакиноу гохночц тлцикяк мослогие. литкысо тоункя тилядб. яцоог опогол. шолихино ослцл собтижаял, тклинцл кпо литкысо, и яоя нолвки моли шолихино коли иса собтижаял, тклинцл кпо литкысо сояцадгициф нолихицо. кыли вк он тогишиня - нцияотия окляки шолихицо. кыли вк он тогишиня - нцияотия оклякия шолихицо. кыли вк он тогишиня - нциястия оклакия солициндам тиланда то-плопобо, и экли шолихицио нк мящл ытолиями мо ыгоиб тякьмыядб собтциновоб. литкысо чоякл гилиноямыф ы мослогиекб или ик гохглицециныф могыхб. ыкликинд нк болло шдая, г цяоб они ошц щдли огклкци, литымсе тлингловида вилиекб, ьяощд тосимоян кк ших мовцлкиу. литкысе тлингловида вилиекб, какши и г лихидк мяолонд. шолихицю мышф тилики иса, тиликида пиховлими г лихидк мяолонд. шолихицю мошлидыф щдло тлиплымая с ыкшк сцсож-нишони вкненно, но тилияли тацикая, шливы с ояло он лкамя кек лих тлойкымик билог, тлотидециений тилика, шливы с ояло он лкамя кек лих тлойкымик билог, толотдаликая тилика, ши билкинсозф актохновноу тиликау, и сонялыф тилика, шливы с ояло он лкамя кек лих тлойкымик билог, тлотидикая ни цоли, или билкинсозф и солиент мочлциилцым, и сонялыф тилика и илигика, ни билкинсозф истохновном инкикп. овяяду пацу собяд огиния билоки. гоя мослогиек, ц гоя клю члицияхи. никациккему, шливафему, гиликкыагкиндинди, иньфаизовогд лошоя но оплогидаб тлфбоополиндб яологиекб	ялкяи ыослогие, нк тонгклпцфыи отцыноыяи, или гык йклисоб хц гдыаож ыяцгсо?	🗌 Г Показать только замененные Г Показать закодированный текст
оли ода дана отклаца. шолихцию тлогкл ядоннож нови, кпо сгцляилц г гдмособ ыгкялоб хициии иц шялкпо шлимяцжекпо охклц цлим щдлц ылизсоб оношндб вилиекб, ьяощд тосинояи кк шкх мовцлкниу, литкысо тлкитовияцл вияи г гонжьич ялоеошцч нц жвноб шклкпо охклц, и, лцымяцганыи иц нови, тцлянклд лцхоалими г лцхндк мяолонд, шолихцио мошлцлыф щдло тлиплцыияи с ыкшк сцсож-нишони вкнеино, но тклкнобцл. мон нк тличония, и он омклыф тклкн щслцноб яклкгксяолц, лцхплфндгцф тлойкымиж билог, тлотядгцженч г томяояк тклкн ниб, гыбцялигцфыи г хклкндк, холоадк и соливнкидк тлцикяд. шливк с ояло он лкамя кек лцх тломбоялкяи тлкнсо о мослогиек. кк шолиак гксц нцхци оямнфл осяцг бкллин, тлолкяцф иц гдмояк акмяинкыфяи били ици бцлкнисоу шкхгохноаноу тлцикясу, мкувцы совям бкллинц шклкяя нц лцгнияк, но тлкнсц мочлцнилцыи, и сонялщщинных сотии мяофя иц вклноб дднск шолиамч нкнкп. омядду плцх сцбклд огинкл бнопок. гоя мослогиек, ц гоя кпо члиниялям. нкмяцлкжему, шлкмяфему, гкливкяяткинду нкыфямвояогду лашоя м оплогцядб тлфбоополиндб яологиекб	мацтес. шолихцно щдл отдяндб иплособ и тлкслцыно хнцл оягкя. но гык вк онноу сыязоловномяиж кпо чцлцсякл нк имъклтдгцлыф: толоу кбо но шоли чоякломи вщбобо лимснояи вихниж нц лиакиноу гохночц тлцнкяк ыослогие. литкысо тоункя тклгдб. яцсог опогол. шолихцно ослцл собтижякл, тклкнцл кпо литкысо, и яоя нолвкн ынклцяи тклгож тотдясо. кыли онц онцыяыф, кпо нолф шонкя гнгок шолиак ноли шолихцно. кыли вк он топишнкя - нцыяотия оьклкни шолихцно. мялциндк тцлянклд, ыялциндк омлогиф, но литкысо оясцхдгцлыф нопогцлигцаимф то-нлопобо, и экли шолихцно нк ыяцл ытолияи мо ыгоиб тлкьимядб собтциионоб. литкысо чоякл гклнояимф ы мослогиекб или нк гохглцецяимф могыкб. ыклкнинд нк бопло щдяи, г щяоб ови оши шлик оснатики.	Показать частоты Буква в шифре Заменить на з л М = О Добавить Ю = Н Удалить р = И Э = Л
тлоыбоялкяя тлкнсо о мослогиек. кк шолиак гисц нцхци оямнфл осяцг бкллин, тлолкяцф нц гдмояк акыяинкыфяи били нци бцлкнисоу шкхгохноаноу тлцнкяоу. ыкуьцы сомяи бкллинц шклкжя нц лцгнинк, но тлкнсц мочлцнилцыи, и сонялцшцнндк сотии мяофя нц ьклноб лднск шолиачч нкнкп. омялду плцх сцбклд огинкл бнопок. гоя мослогиек, ц гоя кпо чицниякли. нкыяцлкжеиу, шлкыяфеиу, гклиькыягкинду нкыфяизояогду лошоя ы оплогцядб тлфбоополиндб яологиекб	шолихцно тлогкл ялоннож нови. кпо сгцляилц г гдмособ ыгкялоб хнцнии нц шклкпо шлимяцкекпо охклц шлиы щдлц ылиасоб оношндб вилиекб, ьяощд тосинояи кк шкх мовцлкниу. литкысо тлкитовияцл виям г гонжвич ялоеошцч нц жвноб шклкпо охклц, и, лцъвяцганыи нц нови, тцлянклд лцхоалими г лцхндк ыяолонд. шолихцно ыошлцлыф щдло тлиплцыияи с ыкшк сцсож-нишони вкнеино, но тклкнобцл. мон нк тличонил, и он оыклыф тклкн щслцноб яклкгксяолц, лцхплфндгцф тлойкымиж билог, тлотлдгцжеич г томяояк тклкн ниб, гыбцялигцфым г хклкндк, холоядк и соливнкгдк тлцнкяд. шливк с ояло он лкаил кек лцх	
и бцлкнисоу, точовку нц ьклогкькысож пологоу, плцнсоу, шкх книнопо	тлоыбоялкям тлкнсо о мослогиек. кк шолиак гксц нцхци ояынфл осяцг бкллин, тлолкяцф нц гдмояк акмяинкыфям били нцн бцлкнисоу шкхгохноаноу тлцнкяоу. ыкуьцы сомям бкллинц шклкжя нц лцгнинк, но тлкнсц мочлцнилцыи, и сонялщшннндк сотим мяофя нц ьклноб лднск шолиамч икнкп. омялду плцх сцбхлд огинкл биопок. гоя мослогиек, ц гоя кпо члцниякли. нкыяцлкжему, шлкыяфему, гклиькыягкннду нкыфямзояогду лошоя м оплогцядб тлфбоополиндб яологиекб и бцлкнисоу, точовку нц ьклогкькысож пологоу, плцнсоу, шкх книнопо	

Рисунок 12. Результат расшифровки букв «о», «н», «и» и «л»

После расшифровки аналогичным образом букв «к» на «е», «ц» на «а» и «я» на «т» окно выполнения лабораторной работы приобретает следующий вид (рис. 13):



Рисунок 13. Окно выполнения лабораторной работы после расшифровки семи букв

Когда так много букв уже известно, зашифрованные буквы могут мешать для понимания слов. Для облегчения дальнейшего анализа в программе предусмотрена возможность выставления флага «Показать только замененные», при выставлении которого все зашифрованные буквы выводятся на экран в виде символов решетки (рис. 14).

Рис. 14. Использование флага «Показать только замененные»

Теперь видно, что слово «##о#о##отал» в нижней строке вполне может быть словом «пробормотал». Если теперь выключить флаг, то можно получить косвенное подтверждение

этого - на позициях двух букв «р» в этом слове в шифре также находится одинаковая буква «л» (рис. 15).

Лабораторная работа N1: Взлом моноалфавитного подстановочного шифра	
шелепог. оаелоблфжеаф соллесйиф ьонеы, го гыеб ыгоеб гелисолетии чланфеафыф на тфтинеыфти сганлатнди флнач ха голотаби.	<ul> <li>Показать только замененные</li> <li>Показать закодированный текст</li> </ul>
площде джни, сотоддб ьовно тонибание тлесламнопо, хатлатили ыгоиби вихнфби ха тотдтси хагланети щтиби мослогиеаби. не нано шолиаопо оба,	Показать частоты
ьтощи моошлахити: соллесиионеля ы лжшоу паластиси отнанот гые, толисо ща толовити чотф ща балож ич толисо. не их холотич ылитсог моланциятым имииние мосполчений, а их тоношини рессу, не	Буквав шифре Заменить на
тоннажемчыф сотилоганиж, тоьти шеыйенндч очгаьеннду личолансоу, шолихано гхбос от голнениф еее на ыеленине	М = О Добавить
тленси. сопна ве хатими соньилами, он ошбфс г слемле, могелаенно отомтоаеннду, тотелфгаму томленние милд.	ю = н р = и
тлияла халф, мелешлфнде лонд отали гних, то нешо ламтлемсаломи сламное молнйе, шолихано тохголил меше хамноти на вамос.	э = л к = е
они леаили нельати солашли на олшите г тлеч билфч от лиаенноу гохноча тланетд, ыталаф инзолбайиф не гдхдгала ногелиф, нисто не боп ысахати	ц = а я = т
тоьно, сасог ланиом неумтгиф чланителф, емли литемсо тогехет, шолихано мтомтитыф и хашелет епо, а емли топишнет - мтомтитыф и тотдтает	
ызаытиф маб. г ысазаннле пипант гдплфнел еее шолее плобохноиб, на епо аилосоу плони	
Ве лящогия, сас и савнду тленбет г ыослогиенийе. чланители шонет ханагати готлоыд, и собтижтел тобовет на нич отгетити, а шолихано	
шонет ыловати. еыли епо талтнел озишетыф, гохбовно, озишса, тобовет ебо тошенити.	
- тд бенф ылдамам? - ытломил литемсо. - отликно ылдао. гтелен!	
- сона тд оенф толотиан' не новнеаныф соеу ыбелти: - тд намтолисо г меще не огелен? нагау ф тоуно телгдб. - шалшем, - тлошолботал литемсо млоаау бенф гнибателино. емли ф	
· · · · · · · · · · · · · · · · · · ·	

Рисунок 15. Проверка гипотезы отключением флага

Если заменить теперь букву «т» на «п», «л» на «р», «ш» на «б» и «б» на «м», то окно выполнения лабораторной работы станет выглядеть так(рис. 16):

Лабораторная работа N1: Вэлом моноалфавитного подстановочного шифра	
Лабораторная работа N1: Вэлом моноалфавитного подстановочного шифра берепог. озеломлфжееф соллесйиф ьонеы, го гыем ыгоем гелисолепии чранфеефыф на пфтинеыфти сганратндч фрнач ха горотами. пробде лжни, соторди ьовно понимание пресравнопо, хаплатили ыгоими вихифми ха попдтси хагланети щтими ыосорогиеами. не нано болиаопо ома, ьтобд мообрахити: соллесйиоперд ы лжбоу паластиси отненот гые, толисо бд половити чотф бд малож ич толисо. не их холотдч ылитсог ысландгажтыф иытиннде ыосрогиенийд, а их понобндч гесеу. не поннажениыф сопироганиж, повти беыйенндч очгавеннду личорансоу, болихано гхмос от голнениф еее на ыеренине пленси. сопна ве хапими соньилами, он обмфс г сремле, ыогераенно опоытозеннду, потерфтану помление ыилд. привла харф. ыеребрфиде лонд опали гних. по небо раыплеысаломи срамное ыолийе. болихано похголил ыебе хамноти на вамос. но толисо на вамос они реаили нервати сорабли на орбите г треч милфч от лиаенноу гохноча планетд. ытараф инзормайиф не гдхдгала ногериф, нисто не моп ысахати товно, сасог раниом неуытгиф чранителф. емли липемсо погехет, болихано ыпомтитыф и хаберет епо. а емли попибнет - ыпомтитыф и попдтает ывытиф вам. г ысазаннре пипант гдплфнел еее более проможнами. на епо аиросоу прони бдл осреплен сомпижтер, нополнителинду мохп, ыохнаннду лжними ы тасоу ве лжбогиж, сас и савнду пренмет г ыосрогиенийе. чранители бонет ханагати гопроц, и сомпижтер помовет на нич отгетити. а болихано	Гоказать только замененные Показать закодированный текст Буква в шифре Заменить на б М М = О Ю = Н Ф Лобавить Ю = Н Чдалить Э = Л К = е Ц = а Я = Т Т = П Л = р Ш = б б = М
одл осреплен сомпиятер, нополнителинду мохп, ыохнаниду ляними ы тасоу ве лябогия, сас и савнду пренмет г мосрогиенийе. чранители бонет ханагати гопроыд, и сомпиятер помовет на нич отгетити. а болихано бонет вилоаати. емли епо партнер оаибетыф, гохмовно, оаибса, помовет емо побенити. - тд менф ылдаиаи? - ыпромил липемсо. - отлиьно млдао. гперен! - сона тд менф торопиаи? не новнеаиыф моеу ымерти? - тд наытолисо г мебе не огерен? нагау ф поуно пергди. - балбем, - пробормотал липемсо ылоаау менф гнимателино. емли ф	

Рисунок 16. Окно лабораторной работы после расшифровки букв «п», «р», «б» и «м».

Хорошо видно, что дальнейший анализ значительно упрощается. Например, очевидно по слову «хаплатили», что буква «х» шифра соответствует букве «з» исходного текста. На рис. 17 приведено окно программы, когда анализ уже близок к завершению (осталось совсем немного нерасшифрованных букв).

Рисунок 17. Расшифрованы почти все буквы текста

Когда же все буквы текста расшифрованы, на экран выводится информационное окно (рис. 18):



Рис. 18. Информационное окно, свидетельствующее о успешной расшифровке текста

Появление этого окна на экране свидетельствует об успешном выполнении лабораторной работы.