МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Лабораторная работа №2
Криптоанализ шифров моноалфавитной замены

Студента(ки) 4 курса математического факультета
Суматохина А.С.

Преподаватель
Сидельникова Софья Юрьевна

Воронеж 2023г

Содержание

1. Исходный текст

Текст №3

ВКДЖЮТОДЧЮЫБМДЩХШЮДЖККФЭЫЧЮХШЭКУДКШФЫГТОБЮ-
ЕМШДЫШЯФОТЭОЕДЩХШЮШРБЩУОАДЩХШЮДЖККФЭЫЧЮ ЦШДЫ-
ЯФЮЭОФШЯЫФКБЮШЯКБМГКСЫЕОБОЮШДОШКЕДКРЮЕРЦШВШКЯ-
ФОТОБОДДКЮШЯФОТЭОЕДКЮШКАБЫРЕЮШ СШЮДЖККФЭЫЧЮКДДКЮ
РЮРЕОЭОШКДЫШЮЪФЫОЕШЕОЗДЮЬОРВЩХШФКБМШДКШООШФЫ-
РВФИЕЮОШКРКАОДДКШК ЯЫРДКШЯКРВКБМВЩШКДКШЬФОСЫЕК-
ШЯКБЩЬОДЮОЭШДОРЫДВЧЮКДЮФКСЫДДКЪКШТКРЕЩЯЫШВКШ-
СРОЮШЮДЖ КФЭЫЧЮЮШСШЕКЭШЬЮРБОШЯФОТЭОЕДКЮШТЫУО-
ШОРБЮШЮДЖККФЭЫЧЮЦШЗФЫДЮЕРЦШСШВКЭЯМХЕОФОШЮБЮШЯ
ФОТДЫГДЫЬОДЫШТБЦШВКЭЯМХЕОФДКЪКШЮРЯКБМГКСЫДЮЦШЩЪФ
ГИШООШВКДЖЮТОДЧЮЫБМДКРЕЮШЭКЪЩЕ ШДКРЮЕМШДОВКЭЯМ-
ХЕОФДИЮШЮШСККАЙОШДОЕОЗДЮЬОРВЮЮШЗЫФЫВЕОФШЭДКЪЮЭЦ
ЦЭШЯФЮЗКТЮЕРЦШ СИРЕЩЯЫЕМШСШВЫЬОРЕСОШЯКБМГКСЫЕОБО-
ЮШДОШКТДКЮШЫШЧОБКЪКШФЦТЫШРЮРЕОЭШЮДЖККФЭЫЧЮКД-
ДИЗ ШРОФСЮРКСШОРБЮШТБЦШТКРЕЩЯЫШВШЕЫВЮЭШРЮРЕОЭЫ-
ЭШЮРЯКБМГЩХЕРЦШЭДКЪКФЫГКСИОШЯЫФКБЮШЮБ ЮШЮДЫЦ-
ШВКДЖЮТОДЧЮЫБМДЫЦШЮДЖККФЭЫЧЮЦШЕКШДЫСОФДЦВЫШЛЕ-
ЮШТЫДДИОШАЩТЩЕШЗФЫДЮЕМРЦШДОШЕ КБМВКШСШЪКБКСО-
ШДКШЮШСШГЫЯЮРДКЮШВДЮУВОШЮБЮШДЫШБЮРЕВЫЗШАЩЭЫ-
ЪЮШВКЕКФИОШЯКБМГКСЫЕОБ МШЬЫРЕКШКРЕЫСБЦОЕШДЫШФЫ-
АКЬОЭШРЕКБОШЫШЕКШЮШЯКЯФКРЕЩШЕОФЦОЕШЮШТОБКШГТОРМ
ШДОШСШДОК ФЪЫДЮГКСЫДДКРЕЮШБХТОЮШЫШСШЮГДЫЬЫБМД-
КЮШДОЯФЮЪКТДКРЕЮШЯЫФКБМДКЮШРЗОЭИШДОСКГЭКУДКШ ЯК-
ЭДЮЕМШЭДКЪКШФЫГДИЗШЯЫФКБОЮШФОВКЭОДТЫЧЮЮШЯКШЮЗШ
ФОЪЩБЦФДКЮШЯКШСКГЭКУДКРЕЮШЬЫРЕК ЮШРЭОДОШЕКБМВК-
ШЩРЩЪЩАБЦХЕШЯКБКУОДЮОШГЫРЕЫСБЦЦШЯФЮЭОДЦЕМШДОРБ-
КУДИОШРЗОЭИШЬОФОТКС ЫДЮЦШЮБЮШСККАЙОШРЕЫФЫЕМРЦШР-
СОРЕЮШТОБКШВШТСЩЭШЕФОЭШБОЪВКШГЫЯКЭЮДЫОЭИЭШЮШ-
РЕКБМШУО ШБОЪВКШЩЪЫТИСЫОЭИЭШЯЫФКБЦЭШКЯЮРЫДДИЮ-
ШВБЫРРШЩЦГСЮЭИЗШЭОРЕШЭКУДКШДЫГСЫЕМШФЫГЭОЙОД ЮО-
ЭШВКДЖЮТОДЧЮЫБМДИЗШТЫДДИЗШСШРФОТОШЪТОШЮЭШДОШКА
ОРЯОЬОДЫШГЫЬЫРЕЩХШЮШДОШЭКУОЕШАИ ЕМШДОКАЗКТЮЭЫЦ-
ШГЫЙЮЕЫШЩЪФКГЫШУОШРКРЕКЮЕШСШЕКЭШЬЕКШЭДКЪЮОШ-
ДОШКЕВЫУЩЕРЦШЩГДЫЕМШРО ВФОЕИШВКЕКФИОШРЫЭЮШЯФКР-
ЦЕРЦШСШФЩВЮШЯКЭЮЭКШЯЫФКБОЮШЗФЫДЦЙЮЗРЦШСШГЫЯ-
ЮРДИЗШВДЮУВЫЗ ШЯКБМГКСЫЕОБОЮШСШЛЕКЕШВБЫРРШЯКЯЫ-
ТЫОЕШЯОФОТЫЬЫШВКДЖЮТОДЧЮЫБМДИЗШТЫДДИЗШСШКЕВФИ-
ЕК ЭШСЮТОШСШФЫГЪКСКФОШСШЯЮРМЭОШЯКШРОЕЮШВКЕКФЫЦ-
ШТОБЫОЕШСКГЭКУДИЭШЯОФОЗСЫЕШТЫДДИЗШТБ ЦШЫЕЫВЮШЭКЪ-
ЩЕШЮРЯКБМГКСЫЕМРЦШФЫГДИОШЕОЗДЮЬОРВЮОШРФОТРЕСЫШЯК

НЮСЫДЮООШЮБЮШЯФКР БЩНЮСЫДЮООШФЫГЪКСКФКСШЯЫРРЮ-
СДКОШЯФКРБЩНЮСЫДЮООШРОЕЮШДКШЮТОЦШКТДЫШКРЩЙОРЕ-
СЮЕМШТКРЕ ЩЯШВШТЫДДИЭШСШЕКЕШЭКЭОДЕШВКЪТЫШКДЮШ-
ДЫЮЭОДООШГЫЙЮЙОДИШРБЩУОАДЫЦШЮДЖКФЭЫЧЮЦШДЫЯФЮ
ЭОФШЯЫФКБЮШЯКБМГКСЫЕОБОЮШДОШКЕДКРЮЕРЦШВШКЯФОТО-
БОДДКЮШЯФОТЭОЕДКЮШКАБЫРЕЮШСШЮДЖКФ ЭЫЧЮКДДКЮШ-
РЮРЕОЭОШКДЫШЮЪФЫОЕШЕОЗДЮЬОРВЩХШФКБМ

1.1. Статистика для исходного текста

Статистика составлется функцией `statistics`

Всего символов: 2055
А = 14
Б = 73
В = 47
Г = 34
Д = 152
Е = 110
Ж = 14
З = 26
И = 175
К = 198
Л = 2
М = 39
Н = 3
О = 171
П = 0
Р = 98
С = 60
Т = 51
У = 16
Ф = 83
Х = 14
Ц = 40
Ч = 17
Ш = 284
Щ = 37
Э = 73
Ю = 164
Я = 60

Индекс совпадений: 0.06541867035954875

Индекс совпадений считается по формуле $\sum_{i=1}^{28} p_i^2$, где p_i - через вероятности появления i-го символа. Расчёт производит фнукция `indexOfMatches`

2. Расшифрованный текст

конфиденциальную информацию можно разделить на предметную и служебную информация например пароли пользователеи не относится к определеннои предметнои области в информационнои системе она играет техническую роль но ее раскрытие особенно опасно поскольку оно чревато получением несанкционированного доступа ко всеи информации в том числе предметнои даже если информация хранится в компьютере или предназначена для компьютерного использования угрозы ее конфиденциальности могут носить некомпьютерныи и вообще нетехническии характер многим людям приходится выступать в качестве пользователеи не однои а целого ряда систем информационных сервисов если для доступа к таким системам используются многоразовые пароли или иная конфиденциальная информация то наверняка эти данные будут храниться не только в голове но и в записнои книжке или на листках бумаги которые пользователь часто оставляет на рабочем столе а то и попросту теряет и дело здесь не в неорганизованности людеи а в изначальнои непригодности парольнои схемы невозможно помнить много разных паролеи рекомендации по их регулярнои по возможности частои смене только усугубляют положение заставляя применять несложные схемы чередования или вообще стараться свести дело к двум трем легко запоминаемым и столь же легко угадываемым паролям описанныи класс уязвимых мест можно назвать размещением конфиденциальных данных в среде где им не обеспечена зачастую и не может быть необходимая защита угроза же состоит в том что многие не откажутся узнать секреты которые сами просятся в руки помимо паролеи хранящихся в записных книжках пользователеи в этот класс попадает передача конфиденциальных данных в открытом виде в разговоре в письме по сети которая делает возможным перехват данных для атаки могут использоваться разные технические средства подслушивание или прослушивание разговоров пассивное прослушивание сети но идея одна осуществить доступ к данным в тот момент когда они наименее защищены служебная информация например пароли пользователеи не относится к определеннои предметнои области в информационнои системе она играет техническую роль

2.1. Процесс расшифровки текста

1. Составление статистики для текста
2. Замена самой частой буквы "Ш"(встретилась 284 раз) на символ пробела
3. Нахождение односимвольных и двух-символьных слов. Выявление по ним таких букв, как "И", "Н", "Е", "О".

4. Подбор остальных букв методом подбора

2.2. Статистика для расшифрованного текста

Всего символов: 2055
А = 136
Б = 14
В = 60
Г = 26
Д = 51
Е = 171
Ж = 16
З = 34
И = 195
К = 47
Л = 73
М = 73
Н = 152
О = 198
П = 60
Р = 83
С = 98
Т = 110
У = 37
Ф = 14
Х = 26
Ц = 17
Ч = 18
Ш = 3
Щ = 8
Э = 2
Ю = 14
Я = 40

Индекс совпадений: 0.065418670359548 75

3. Вывод

Вывод: текст был зашифрован с помощью метода моноалфавитной замены, так как индекс совпадения одинаков для зашифрованного и дешифрованного текста.