Министерство образования и науки Российской Федерации
Санкт-Петербургский Политехнический Университет Петра Великого
•
Институт кибербезопасности и защиты информации.

Л А Б О Р А Т О Р Н А Я Р А Б О Т А 2

Основы частотного криптоанализа

по дисциплине «Основы информационной безопасности»

Выполнил

студент гр. 4851003/10002 Лобов Е.А

Преподаватель Зубков Е.А.

Санкт-Петербург

2022

Цель работы

Цель работы - приобретение навыков криптоанализа, ознакомление со способом дешифрования криптограмм на примере применения метода частотного криптоанализа.

1.ИСХОДНАЯ КРИПТОГРАММА

САУУЕЛЩА?ЬЦШЕ СЩАВЛЧМАМЛЕУШ (ЛДСНЕ МАУУЕЛЩАЬЦЧЕ ЭАПЩЧЙДЦАЕ, МАУУЕЛЩАЬЦШЕ ЭАПЩШ) - МВЧМЧИ ЭАПЩЧЙДЦАХ, Й СЧЛЧЩЧУ ОТХ (ГД)ЭАПЩЧЙДЦАХ А ЩДМЭАПЩЧЙДЦАХ ВЩАУЕЦХЕЛМХ ЧОАЦ А ЛЧЛ НЕ СЩАВЛЧКЩДПАЬЕМСАР СТЯЬ. ДЧ АГЧИЩЕЛЕЦАХ МЫЕУШ ДМАУУЕЛЩАЬЦЧКЧ ЭАПЩЧЙДЦАХ ЕОАЦМЛЙЕЦЦШУ
МЪЗЕМЛЙЧЙДЙЭАУ МВЧМЧИЧУ ХЙТХТЧМЖ МАУУЕЛЩАЬЦЧЕ ЭАПЩЧЙДЦАЕ. КТЯЬ ДТКЧЩАЛУД ОЧТНЕЦ МЧЫЩДЦХЛЖМХ Й МЕСЩЕЛЕ ЧИЕАУА МЛЧЩЧЦДУА. КТЯЬ ДТКЧЩАЛУД ЙШИАЩДЕЛМХ
МЛЧЩЧЦДУА ОЧ ЦДЬДТД ЧИУЕЦД МЧЧИЗЕЦАХУА.

В ЦДМЛЧХЗЕЕ ЙЩЕУХ МАУУЕЛЩАЬЦШЕ ЭАПЩШ ЩДГОЕТХЯЛМХ ЦД 2 СТДММД:

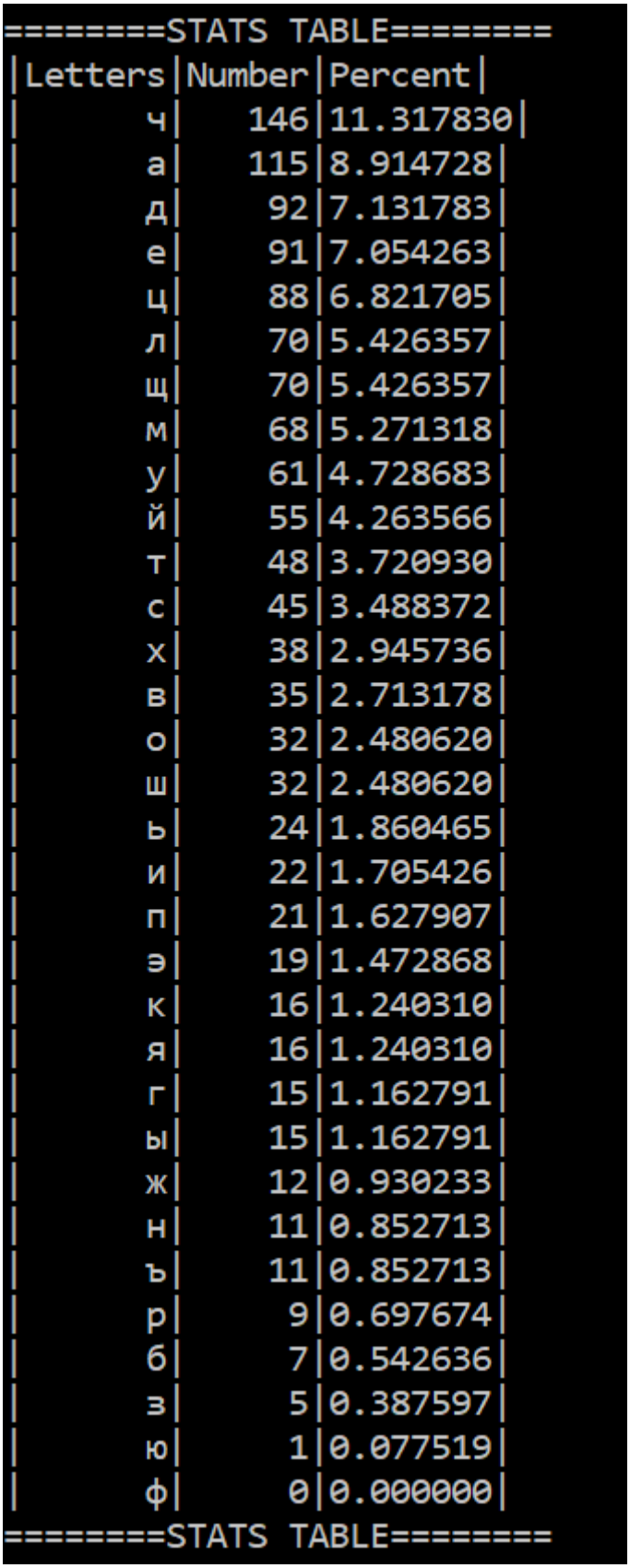
1. БТЧЬЦШЕ ЭАПЩШ. ОИЩДИДЛШЙДЯЛ АЦПЧЩУДБАЯ ИТЧСДУА ЧВЩЕОЕТёЦЦЧР ОТАЦШ (ЧИШЬЦЧ 64, 128 ИАЛ), ВЩАУЕЦХХ С ИТЧСЪ СТЯЬ Й ЪМЛДЦЧЙТЕЦЦЧУ
ВЧЩХОСЕ, СДС ВЩДЙАТЧ, ЦЕМСЧТЖСАУА БАСТДУА ВЕЩЕУЕЭАЙДЦАХ А ВЧОМЛДЦЧЙСА, ЦДГШЙДЕУШУА ЩДЪЦОДУА. РЕГЪТЖЛДЛЧУ ВЧЙЛЧЩЕЦАХ ЩДЪЦОЧЙ ХЙТХЕЛМХ
ТДЙАЦЦШР ЮППЕСЛ — ЦДЩДМЛДЯЗДХ ВЧЛЕЩХ МЧЧЛЙЕЛМЛЙАХ ИАЛЧЙ УЕНОЪ ИТЧСДУА ЧЛСЩШЛШЫ А ГДЭАПЩЧЙДЦЦШЫ ОДЦЦШЫ.

2. ПЧЛЧЬЦШЕ ЭАПЩШ, Й СЧЛЧЩШЫ ЭАПЩЧЙДЦАЕ ВЩЧЙЧОАЛМХ ЦДО СДНОШУ ИАЛЧУ ТАИЧ ИДРЛЧУ АМЫЧОЦЧКЧ (ЧЛСЩШЛЧКЧ) ЛЕСМЛД М АМВЧТЖГЧЙДЦАЕУ КДУУАЩЧЙДЦАХ.
ПЧЛЧЬЦШР ЭАПЩ УЧНЕЛ ИШЛЖ ТЕКСЧ МЧГОДЦ ЦД ЧМЦЧЙЕ ИТЧЬЦЧКЧ (ЦДВЩАУЕЩ, ГОСТ 28147-89 Й ЩЕНАУЕ КДУУАЩЧЙДЦАХ), ГДВЪЗЕЦЦЧКЧ Й МВЕБАДТЖЦЧУ ЩЕНАУЕ.
БЧТЖЭАЦМЛЙЧ МАУУЕЛЩАЬЦШЫ ЭАПЩЧЙ АМВЧТЖГЪЯЛ МТЧНЦЪЯ СЧУИАЦДБАЯ ИЧТЖЭЧКЧ СЧТАЬЕМЛЙД ВЧОМЛДЦЧЙЧС А ВЕЩЕМЛДЦЧЙЧС. МЦЧКАЕ ЛДСАЕ ЭАПЩШ АМВЧТЦХЯЛМХ Й
ЦЕМСЧТЖСЧ ВЩЧЫЧОЧЙ, АМВЧТЖГЪХ ЦД СДНОЧУ ВЩЧЫЧОЕ «СТЯЬ ВЩЧЫЧОД». МЦЧНЕМЛЙЧ «СТЯЬЕР ВЩЧЫЧОД» ОТХ ЙМЕЫ ВЩЧЫЧОЧЙ ЦДГШЙДЕЛМХ
«ЩДМВАМДЦАЕУ СТЯЬЕР». КДС ВЩДЙАТЧ, ЧЦЧ МЧГОДЕЛМХ АГ СТЯЬД ЙШВЧТЦЕЦАЕУ ЦДО ЦАУ ЦЕСАЫ ЧВЕЩДБАР, Й ЛЧУ ЬАМТЕ ВЕЩЕМЛДЦЧЙЧС А ВЧОМЛДЦЧЙЧС.

2.ЛИСТИНГ РАЗРАБОТАННОЙ ПРОГРАММЫ.

Код программы находится в дирректории source.

3.РАСПРЕДЕЛЕНИЕ ЧАСТОТ БУКВ В КРИПТОГРАММЕ



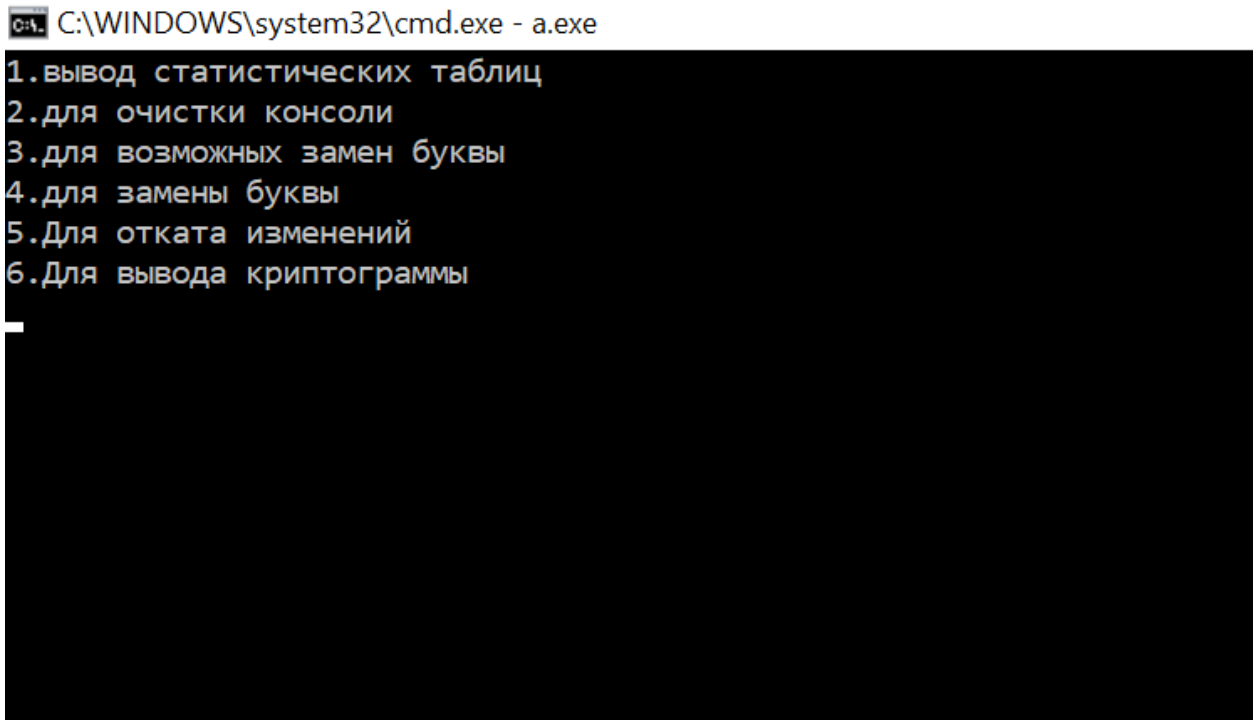
========STATS TABLE========

Letters	Number	Percent
ч	146	11.317830
а	115	8.914728
д	92	7.131783
е	91	7.054263
ц	88	6.821705
л	70	5.426357
щ	70	5.426357
м	68	5.271318
у	61	4.728683
й	55	4.263566
т	48	3.720930
с	45	3.488372
х	38	2.945736
в	35	2.713178
о	32	2.480620
ш	32	2.480620
ь	24	1.860465
и	22	1.705426
п	21	1.627907
э	19	1.472868
к	16	1.240310
я	16	1.240310
г	15	1.162791
ы	15	1.162791
ж	12	0.930233
н	11	0.852713
ъ	11	0.852713
р	9	0.697674
б	7	0.542636
з	5	0.387597
ю	1	0.077519
ф	0	0.000000

========STATS TABLE========

Таблица распределения частот букв в криптограмме

4.РЕЗУЛЬТАТЫ РАБОТЫ.



Результатом работы является консольное приложение для расшифровки криптограмм с использованием частотного криптоанализа.

Благодаря данному приложению была расшифрована исходная криптограмма. В ходе расшифровки часть букв была расшифрована исключительно благодаря частотному анализу и подстановке наиболее подходящей по частоте буквы, а часть букв была расшифрована благодаря предположениям, что слово ИАЛ на 14 строке является словом БИТ, а так же что слово ЦДВЩАУЕЩ в 24 строке является словом НАПРИМЕР. Последовательность команд, исполненных приложением во время расшифровки представлена в файле «decode_inputs.txt».

5.РЕЗУЛЬТАТЫ РАБОТЫ.

Текст расшифрованной криптограммы -

симметричные криптосистемы (также симметричное шифрование, симметричные шифры) - способ шифрования, в котором для
(за)шифрования и расшифрования применяется один и тот же криптографический ключ. до изобретения схемы асимметричного шифрования единственным
существовавшим способом являлось симметричное шифрование. ключ алгоритма должен сохраняться в секрете обеими сторонами. Ключ алгоритма выбирается
сторонами до начала обмена сообщениями.

в настоящее время симметричные шифры разделяются на 2 класса:

1. блочные шифры. дбрабатывают информацию блоками определённой длины (обычно 64, 128 бит), применяя к блоку ключ в установленном
порядке, как правило, несколькими циклами перемешивания и подстановки, называемыми раундами. йезультатом повторения раундов является
лавинный эффект — нарастающая потеря соответствия битов между блоками открытых и зашифрованных данных.

2. фоточные шифры, в которых шифрование проводится над каждым битом либо байтом исходного (открытого) текста с использованием гаммирования.
фоточный шифр может быть легко создан на основе блочного (например, гост 28147-89 в режиме гаммирования), запущенного в специальном режиме.
большинство симметричных шифров используют сложную комбинацию большого количества подстановок и перестановок. многие такие шифры исполняются в
несколько проходов, используя на каждом проходе «ключ прохода». множество «ключей прохода» для всех проходов называется
«расписанием ключей». как правило, оно создается из ключа выполнением над ним неких операций, в том числе перестановок и подстановок.

Таблица подстановок:

Буква	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п
Код	Д	И	Й	К	О	Е	Ё	Н	Г	А	Р	С	Т	У	Ц	Ч	В
Буква	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	
Код	Щ	М	Л	Г	П	Ы	Б	Ь	Э	З	-	Ш	Ж	Ю	Я	Х	

ВЫВОД

Использование частотного криптоанализа облегачет расшифровку криптограмм. Использовать только частотный криптоанализ для подстановки не представляется возможным, так как статистика, собранная по криптограмме далеко не обязательно совпадает со статистикой по языку полностью. Она совпадает лишь в некоторых основных моментах, например для самых часто встречающихся букв языка. Так же благодаря частотному криптоанализу можно составить список букв, подходящих на замену определенной букве криптограммы, ограничив тем самым возможные варианты подстановок.
Частотный криптоанализ является эффективным инструментом, но невозможно использовать только его. На данную лабораторную работу было потрачено около 8 часов.

ОТВЕТЫ НА КОНТРОЛЬНЫЕ ВОПРОСЫ.

1. Что такое шифр моноалфавитной подстановки?

В такой подстановке буква (или символ) в исходном тексте всегда изменяется на одну и ту же самую букву (или символ) в зашифрованном тексте независимо от его позиции в тексте.

2. Укажите недостстатки шифра моноалфавитной подстановки.

Главный недостаток – замена при шифровании одной буквы открытого текста на одно шифрообозначение и отсюда подверженность их частотному анализу.

3.Какова сложность дешифрации методом прямого перебора для сообщения, зашифрованного шифром моноалфавитной подстановки?

Сложность дешифрации методом прямого перебора для подобных шифров в теории равна размерности алфавита, однако на деле часто бывает достаточно всего нескольких символов для успешной дешифровки.

4.Какие условия упрощают частотный анализ?

Для упрощения частотного анализа возможна, например, поддержка программой внешнего словаря слов, или наиболее распространенных

окончаний слов, предлогов и союзов.

5.Получится ли правильно дешифрованная криптограмма, если произвести все замены в соответствии с частотами появления букв в русском языке?

Если произвести все замены в соответствии с частотами появления букв, то правильно дешифровать криптограмму не удастся, т.к. во-первых, частоты букв могут быть одинаковыми (тогда без помощи человека или словаря, программе просто не обойтись), во-вторых некоторых букв в криптограмме может просто не быть и тогда все частоты собьются.