Титулка

ЗМІСТ

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

СЛОВАРЬ ТЕРМИНОВ

Открытый (исходный) текст — данные (не обязательно текстовые), передаваемые без использования криптографии.

Шифротекст, шифрованный (закрытый) текст — данные, полученные после применения криптосистемы.

Шифр, криптосистема — совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты.

Символ — это любой знак, в том числе буква, цифра или знак препинания.

Алфавит — конечное множество используемых для кодирования информации символов. Стандартный алфавит может быть изменён или дополнен символами. **Ключ** — параметр шифра, определяющий выбор конкретного преобразования данного текста. В современных шифрах криптографическая стойкость шифра целиком определяется секретностью ключа (принцип Керкгоффса).

Шифрование — процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает шифрованный текст.

Расшифровывание — процесс нормального применения криптографического преобразования шифрованного текста в открытый.

Асимметричный шифр, двухключевой шифр, шифр с открытым ключом — шифр, в котором используются два ключа, шифрующий и расшифровывающий. При этом, зная лишь ключ зашифровывания, нельзя расшифровать сообщение, и наоборот.

Открытый ключ — тот из двух ключей асимметричной системы, который свободно распространяется. Шифрующий для секретной переписки и расшифровывающий — для электронной подписи.

Секретный ключ, закрытый ключ — тот из двух ключей асимметричной системы, который хранится в секрете. Криптоанализ — наука, изучающая

математические методы нарушения конфиденциальности и целостности информации.

Система шифрования (шифрсистема) — это любая система, которую можно использовать для обратимого изменения текста сообщения с целью сделать его непонятным для всех, кроме адресата.

Криптостойкостью — это характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. способность противостоять криптоанализу).

Криптоаналитик — учёный, создающий и применяющий методы криптоанализа. Криптография и криптоанализ составляют криптологию, как единую науку о создании и взломе шифров (такое деление привнесено с запада, до этого в СССР и России не применялось специального деления).

Криптографическая атака — попытка криптоаналитика вызвать отклонения в атакуемой защищённой системе обмена информацией. Успешную криптографическую атаку называют взлом или вскрытие.

Дешифрование (дешифровка) — процесс извлечения открытого текста без знания криптографического ключа на основе известного шифрованного. Термин дешифрование обычно применяют по отношению к процессу криптоанализа шифротекста (криптоанализ сам по себе, вообще говоря, может заключаться и в анализе криптосистемы, а не только зашифрованного ею открытого сообщения).

Криптографическая стойкость — способность криптографического алгоритма противостоять криптоанализу.

Имитозащита — защита от навязывания ложной информации. Другими словами, текст остаётся открытым, но появляется возможность проверить, что его не изменяли ни случайно, ни намеренно. Имитозащита достигается обычно за счет включения в пакет передаваемых данных имитовставки.

Имитовставка — блок информации, применяемый для имитозащиты, зависящий от ключа и данных.

Электронная цифровая подпись(электронная подпись) — асимметричная имитовставка (ключ защиты отличается от ключа проверки). Другими словами, такая имитовставка, которую проверяющий не может подделать.

Центр сертификации — сторона, чья честность неоспорима, а открытый ключ широко известен. Электронная подпись центра сертификации подтверждает подлинность открытого ключа.

Хеш-функция — функция, которая преобразует сообщение произвольной длины в число («свёртку») фиксированной длины. Для криптографической хеш- функции (в отличие от хеш-функции общего назначения) сложно вычислить обратную и даже найти два сообщения с общей хеш-функцией.

ВВЕДЕНИЕ

Использовать можно в двух системах:

Первый вариант — это выполняются первые 8 работ и получают нужную оценку.

Второй вариант — каждое задание добавляет балы, общая сумма балов определяет итоговую оценку. (Данная система более правильна и гибка, но требует набирать балы за работу)

1 МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема: Методы защиты информации. Классификация криптосистем.

Цель: Изучить простые методы криптографической защиты информации, использовать полученные знания для сокрытия путём шифрования.

Теоретические ведомости

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость того, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных. Постепенно защита информации становится обязательной: разрабатываются всевозможные документы по защите информации; формируются рекомендации; даже проводится ФЗ о защите информации, который рассматривает проблемы и задачи защиты информации, а также решает некоторые уникальные вопросы защиты информации.

Таким образом, угроза защиты информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы.

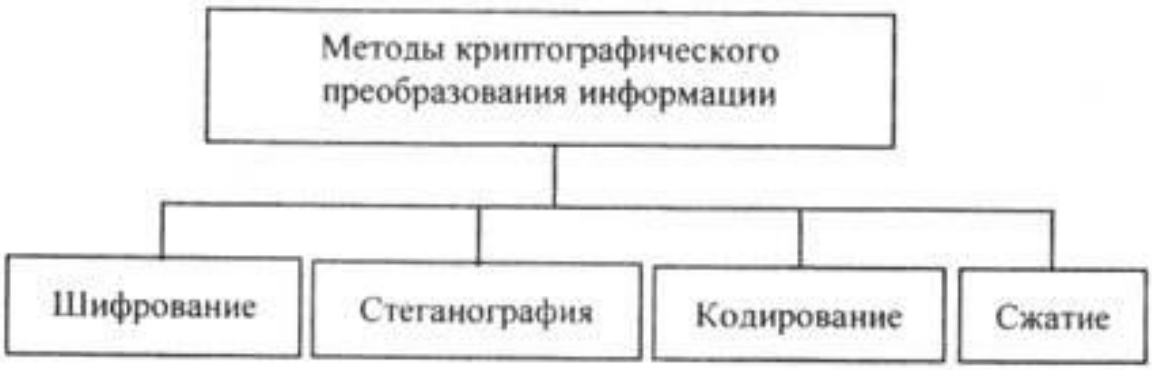

Рисунок 1.1 – Пример вставки рисунков

1 Симметричные криптосистемы

1.1 Шифры перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение «Неясное становится ещё более непонятным» записывается в таблицу из 5 строк и 7 столбцов по столбцам.

Таблица 1.1

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Ё	Е	Н	М

Для получения шифрованного сообщения текст считывается по строкам и группируется по 5 букв:

НОНСБ-НЯЕЕО-ЯОЕТЯ-СВЕЛП-НСТИЩ-ЕОЫНА-ТЕЕНМ

Несколько большей стойкостью к раскрытию обладает метод *одиночной перестановки* по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово - **ЛУНАТИК**, получим следующую таблицу:

Таблица 1.2 – Метод перестановки по ключу

Л	У	Н	А	Т	И	К
4	**7**	**5**	**1**	**6**	**2**	**3**
Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

До перестановки

→

А	И	К	Л	Н	Т	У
1	**2**	**3**	**4**	**5**	**6**	**7**
С	Н	Я	Н	Н	Б	О
Я	Е	Т	Е	О	О	Е
Е	П	Н	Я	В	Л	С
Щ	О	Ы	С	И	Е	Т
Е	Н	М	Н	Т	Е	А

После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка:

СНЯНН-БОЯЕТ-ЕООЕЕ-ПНЯВЛ-СЩОЫС-ИЕТЕН-МНТЕА

Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины её строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются алгоритмы двойных перестановок. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке порядок перестановок был обратный. Пример данного метода шифрования показан в таблице

Таблиця 1.3 – Метод перестановки по ключу

	2	**4**	**1**	**3**
4	П	Р	И	Е
1	З	Ж	А	Ю
2	-	Ш	Е	С
3	Т	О	Г	О

	1	**2**	**3**	**4**
4	И	П	Е	Р
1	А	З	Ю	Ж
2	Е	-	С	Ш
3	Г	Т	О	О

	1	2	3	4
1	А	З	Ю	Ж
2	Е	-	С	Ш
3	Г	Т	О	О
4	И	П	Е	Р

Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы. В результате перестановки получена шифровка:

АЗЮЖЕ_СШГТООИПЕР

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3х3 их 36, для 4х4 их 576, а для 5х5 их 14400.

В средние века для шифрования применялись и магические квадраты. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведённой в квадрате нумерации и затем переписать содержимое таблицы по строкам.

Таблица 1.4 – Исходный текст с идентификаторами

П	Р	И	Е	З	Ж	А	Ю	_	Ш	Е	С	Т	О	Г	О
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Таблиця 1.5 – Магический квадрат

16	3	2	13		О	И	Р	Т
5	10	11	8	→	З	Ш	Е	Ю
9	6	7	12	←	-	Ж	А	С
4	15	14	1		Е	Г	О	П

В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

Число магических квадратов очень резко возрастает с увеличением размера его сторон:

– для таблицы $3\times3\Rightarrow1$ существует только один квадрат;

– для таблицы $4\times4\Rightarrow880$;

– для таблицы $5\times5\Rightarrow250000$.

2 Шифры простой замены

2.1 Система шифрования Цезаря.

Основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на *K* букв. Известная фраза Юлия Цезаря `VENI VINI VICI` – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в `SBKF SFAF SFZF` (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретён так называемый полибианский квадрат размером 5 х 5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже её в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

3 Шифры сложной замены

3.1 Шифр Гронсфельда

Это модификация шифра Цезаря с использованием числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно так же, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

1) Пусть в качестве ключа используется группа из трех цифр – 314.
2) Тогда Сообщение СОВЕРШЕННО СЕКРЕТНО.
3) Ключ 3143143143143143143.
4) Шифровка ФПЖИСЬИОССАХИЛФИУСС.

В шифрах *многоалфавитной замены* для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит). В компьютере операция шифрования соответствует сложению кодов ASCII символов сообщения и ключа по модулю 256.

4 Гаммирование

Процесс зашифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием

открытые данные разбиваются на блоки $T(0)_i$ одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков $G(0)_i$ аналогичной длины $(c)_i = G(c)_i \oplus T(0)_i$, $\oplus$ где - побитовое сложение, $i = 1 - m$.

Процесс расшифрования сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные $T(0)_i = G(c)_i \oplus (c)_i$.

Исходное сообщение из букв русского алфавита преобразуется в числовое сообщение заменой каждой его буквы числом по следующей таблице:

Таблица 1.6 – Числовая замена букв

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

$$\Omega_{i+1} = [(A_i + C_1 - 1) \cdot mod\, 30] + 1; \qquad (0.1)$$

Исходное сообщение ОТДУШКА. Для шифрования числового сообщения используется шифрующий отрезок последовательности А1, А2, ... подходящей длины, начинающийся с $A_{100} : A_{101} \to 5$, $A_{102} \to 6$, $A_{103} \to 17$, $A_{104} \to 8$, $A_{105} \to 19$, $A_{106} \to 3$.

Исходное сообщение	О	Т	Д	У	Ш	К	А
Числовое исходное сообщение	13	17	4	18	23	9	0
Шифрующий отрезок	1	5	6	17	8	19	3
Числовое шифрованное сообщение	14	23	10	5	1	28	3
Шифрованное сообщение	П	Ш	Л	Е	Б	Ю	Г

Помним, что в выбранном алфавите 30 символов.

Задания

В соответствии с вашим вариантом из табл. 1.7 зашифровать текст используя методы криптографической защиты представленные ниже. Регистр должен быть учтён.

1) Шифры перестановки:

a) метод перестановки по ключу;
b) алгоритм двойной перестановки;
c) магические квадраты.

2) Шифры замены:

a) шифр Цезаря;
b) Аффиный шифр;
c) шифр Виженера;
d) шифра Плейфера.

3) Выполнить шифрование методом гаммирования.

Записать результаты шифрования в отчёт, сравнить методы, выбрать оптимальный для заданной фразы и аргументировать свой выбор.

Вопросы для самоконтроля

1) Криптография и её роль в обществе.
4) Объяснить цель и задачи криптографии.
5) Пояснить какие бывают криптографические методы.
6) Что такое шифрование?
7) Как происходит процесс шифровки/дешифровки сообщения?

Как наложение гаммы влияет на исходный текст?

Таблиця 1.7 **– Список фраз для шифрования**

1	6 x 6	небольшое сообщение для тестирования
2	3 x 13	В атмосфере происходит около 1800 гроз.
3	7 x 4	федеральное законодательство
4	4 x 6	Международные стандарты;
5	3 x 13	самая дорогая пицца в мире стоит $1000.
6	4 x 9	применение информационных технологий
7	3 x 12	административный уровень секретности
8	3 x 11	83% младших братьев выше старших
9	3 x 11	обеспечение доступа к информации
10	10 x 4	Индонезия расположена на 17508 островах.
11	4 x 7	у рыбы сарган зеленые кости.
12	8 x 4	язык хамелеона длиннее его тела
13	6 x 4	защищенность информации.
14	5 x 6	в озеро Байкал впадает 336 рек
15	3 x 10	гоночный болид едет по трассе.
16	8 x 3	опасность ’’открывается”
17	4 x 8	процесс обеспечения целостности
18	4 x 9	рекомендация использования терминов
19	5 x 6	обеспечивающее ее формирование
20	5 x 5	общегосударственный орган
21	8 x 4	технических средств ее передачи
22	3 x 11	ворон и ворона — два разных вида.
23	5 x 6	наибольший ущерб субъектам ИБ
24	9 x 3	информационная безопасность
25	8 x 4	ущерб при сервисном обслуживании
26	5 x 7	свойство аутентичности пользователя
27	8 x 4	данные были действия выполнены?!
28	6 x 6	законодательный уровень безопасности
29	8 x 4	из множества потенциально угроз
30	4 x 9	Защита процессов, процедур, программ

2 ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ ШИФРОВ

Тема: Исследование безопасности шифров. Применение частотного анализа для взлома шифротекста.

Цель: Изучить методы взлома криптосистем, провести частотный анализ и расшифровать текст.

Теоретические ведомости

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, то и соответствующая ей буква шифра в зашифрованном тексте также встречается чаще всего. На рисунке 2.1 приведены частоты встречаемости букв в английском тексте.

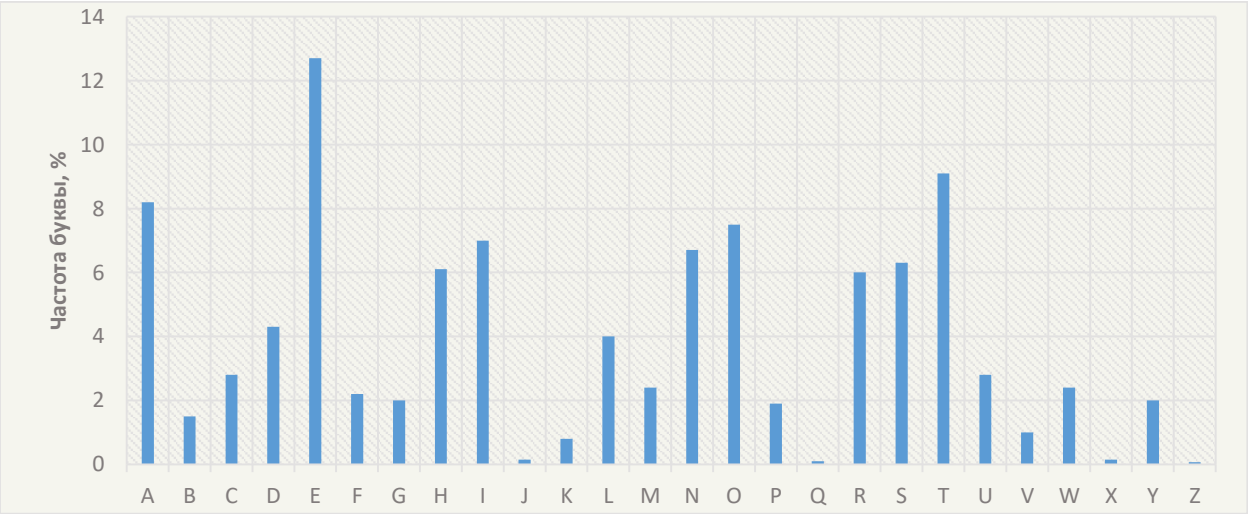

Рисунок 2.1 – Частота использования букв в Английском языке

Для примера мы взяли текст из ресурса Wikipedia[2]. Данный текст предложенный для рассмотрения принципа частотной атаки, с подробным руководством можете ознакомиться на соответствующем ресурсе.

```
LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFEMVEWHKVSTYLXZI
XLIKIIXPIJVSZEYPERRGERIMWQLMGLMXQERIWGPSRIHMXQEREKIETXM
JTPRGEVEKEITREWHEXXLEXXMZITWAWSQWXSWEXTVEPMRXRSJGSTVRIE
YVIEXCVMUIMWERGMIWXMJMGCSMWXSJOMIQXLIVIQIVIXQSVSTWHKPEG
ARCSXRWIEVSWIIBXVIZMXFSJXLIKEGAEWHEPSWYSWIWIEVXLISXLIVX
LIRGEPIRQIVIIBGIIHMWYPFLEVHEWHYPSRRFQMXLEPPXLIECCIEVEWG
ISJKTVWMRLIHYSPHXLIQIMYLXSJXLIMWRIGXQEROIVFVIZEVAEKPIEW
HXEAMWYEPPXLMWYRMWXSGSWRMHIVEXMSWMGSTPHLEVHPFKPEZINTCMI
VJSVLMRSCMWMSWVIRCIGXMWYMX
```

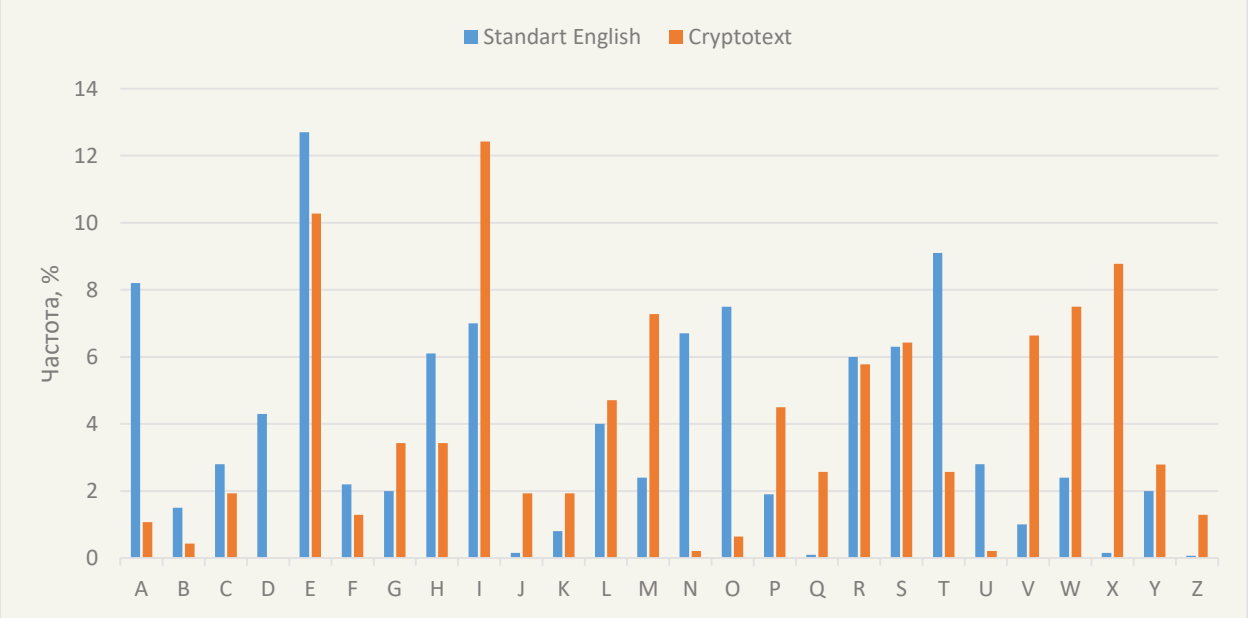

Рисунок 2.2 – Частотный анализ шифрованного текста

Как видно из графика на рис. 2.2 частоты использования символов неясны. Прямой корреляции между символами не наблюдается. Всегда нужно помнить, что частотный анализ не даёт нам полной картины. В каждом тексте соотношение символов будет различное. Так же данный вид взлома будет работать с разными показателями качества для разных языков.

На данном примере мы видим, что по частоте использования в стандарте английского языка преобладает буква **E**. В нашем зашифрованном тексте это может быть буква **I**. Так же можем предположить, что **X** является **T**. Таким образом мы можем продолжить сравнение и получить график на рис. 2.3.

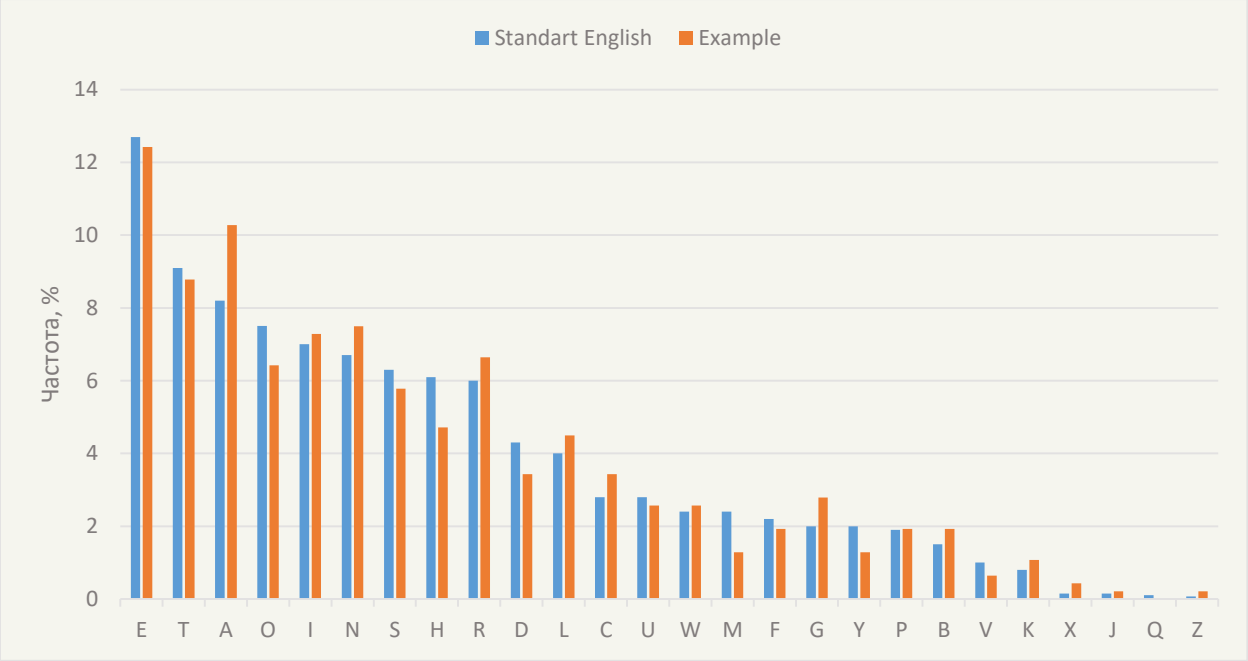

Рисунок 2.3 – Результат сравнения частот стандарта с расшифрованном текстом

```
Hereupon Legrand arose, with a grave and stately air, and
brought me the beetle from a glass case in which it was
enclosed. It was a beautiful scarabaeus, and, at that
time, unknown to naturalists—of course a great prize in
a scientific point of view. There were two round black
spots near one extremity of the back, and a long one near
the other. The scales were exceedingly hard and glossy,
with all the appearance of burnished gold. The weight of
the insect was very remarkable, and, taking all things
into consideration, I could hardly blame Jupiter for his
opinion respecting it.
```

Частотность существенно зависит, однако, не только от длины текста, но и от его характера. Например, в техническом тексте обычно редкая буква **F** может появляться гораздо чаще. Поэтому для надёжного определения средней частоты букв желательно иметь набор различных текстов[1].

Для маскировки частот появления тех или иных букв в тексте используется ***полиалфавитный шифр***. В котором шифрование очередного символа открытого текста согласно некоторому правилу.

Задания

1) Освоить теорию и принципы частотной атаки.
2) Проанализировать представленное ПО
3) Расшифровать текст и предоставить:

    a) шифрованное сообщение;
    b) перечень замен;
    c) расшифрованный текст;
    d) предоставить алгоритм дешифровки.

4) Выводы к работе

Ход работы

Вопросы для самоконтроля

3 СИММЕТРИЧНЫЕ ШИФРЫ. ЧАСТЬ 1

Тема: Тема.

Цель: Опишите цель

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

1) Отличие симметричных и асимметричный шифров.
5) Пояснить что такое исходный текст, шифр, ключ.
6) Принцип подбора ключа в симметричных криптосистемах.
7) Принцип работы симметричных шифров. Приведите примеры.

4 СИММЕТРИЧНЫЕ ШИФРЫ. ЧАСТЬ 2

Тема: Тема.

Цель: Опишите цель

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

5 ВЗЛОМ. ЧАСТЬ 2

Тема: Тема.

Цель: Опишите цель

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

6 АСИММЕТРИЧНЫЕ ШИФРЫ. ЧАСТЬ 1

Тема: Тема.

Цель: Опишите цель

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

7 АСИММЕТРИЧНЫЕ ШИФРЫ. ЧАСТЬ 2

Тема: Тема.

Цель: Опишите цель

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

8 ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ

Тема: Тема.

Цель: Опишите цель

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. НОУ «ИНТУИТ» Лекция 4: Методы криптоанализа // 03.2015 [Электронный ресурс]. URL: https://www.intuit.ru/studies/courses/600/456/lecture/10198 (дата обращения: 08.04.2018).

2. Frequency analysis // 08.01.2018 [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Frequency_analysis (дата обращения: 07.04.2018).

ДОДАТОК Б