Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Кемеровский государственный университет»
Кузбасский гуманитарно-педагогический институт

Факультет информатики, математики и экономики
Кафедра математики, физики и математического моделирования

Ю.С. Гаврилова

МАТЕМАТИЧЕСКИЕ МЕТОДЫ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Основные понятия и история криптографии

методические рекомендации по выполнению аудиторной и внеаудиторной самостоятельной работы по дисциплине
для обучающихся по направлениям подготовки
01.03.02 Прикладная математика и информатика,
02.03.03 Математическое обеспечение и администрирование информационных систем

Новокузнецк

2022

УДК [378.147.88: 004.432.2](072)
ББК 74.484(2Рос-4Кем)я73+32.973-018.6я73
Г 12

Гаврилова Ю.С.

Математические методы и программное обеспечение защиты информации. Основные понятия и история криптографии: методические рекомендации по выполнению аудиторной и внеаудиторной самостоятельной работы по дисциплине для студентов факультета информатики, математики и экономики, обучающихся по направлениям подготовки 01.03.02 Прикладная математика и информатика и 02.03.03 Математическое обеспечение и администрирование информационных систем / Ю.С. Гаврилова. – Новокузнецк : КГПИ ФГБОУ ВО «КемГУ», 2022. – 44 с.

Рекомендовано на заседании
кафедры математики, физики и
математического моделирования
Протокол № 5 от 15.12.2022
Заведующий каф. МФММ

/ Е.В. Решетникова

Утверждено методической комиссией
факультета информатики, математики и
экономики
Протокол № 5 от 15.12.2022
Председатель методической комиссии
ФИМЭ

/ И.А. Жибинова

УДК [378.147.88: 004.432.2](072)
ББК 74.484(2Рос-4Кем)я73+32.973-018.6я73
Г 12

Содержание

ПРЕДИСЛОВИЕ

Настоящие методические рекомендации адресованы студентам, получающим квалификацию бакалавр по направлениям подготовки: 01.03.02 Прикладная математика и информатика и 02.03.03 Математическое обеспечение и администрирование информационных систем и направлены на оказание помощи студентам в подготовке к выполнению лабораторных работ и индивидуальных заданий, прохождению тестирования по теме.

Криптография – один из основных разделов защиты информации, обязательный для изучения студентами IT-направлений. Данные методические материалы содержат основные понятия криптографии, примеры шифрования сообщений разными шифрами и последующего расшифровывания, а также пример применения одного из методов криптоанализа – частотного анализа.

Данные методические материалы позволят студенту закрепить теоретический материал; подготовиться к лабораторным занятиям, прохождению тестирования и выполнению индивидуальных заданий по соответствующей теме.

Методические рекомендации могут оказаться полезными при выполнении проектных работ, прохождении учебных и производственных практик, написании курсовых и выпускных квалификационных работ.

1Теоретические сведения

Защита данных с помощью шифрования считается одним из наиболее надежных способов решения проблемы безопасности. Изучением вопросов шифрования данных занимается наука – **криптология**, включающая криптографию и криптоанализ.

Криптография изучает методы и алгоритмы шифрования данных (правила построения и использования шифров), направленные на то, чтобы сделать эти данные бесполезными для противника. Методы криптографии также используются для подтверждения подлинности источника данных и контроля целостности данных. Криптография всегда являлась обязательным элементом безопасных информационных систем, однако особое значение криптографические методы получили с развитием распределенных открытых сетей, в которых нельзя обеспечить физическую защиту каналов связи.

Криптоанализ – это наука о раскрытии исходного текста зашифрованного сообщения без доступа к ключу.

С теоретической точки зрения четкого различия между кодами и шифрами не существует, но в современной практике различие между ними, как правило, является достаточно четким. **Коды** оперируют лингвистическими элементами, разделяя закрываемый текст на такие смысловые элементы, как слова и слоги. В **шифре** всегда различают два элемента: алгоритм и ключ. Алгоритм позволяет использовать сравнительно короткий ключ для шифрования сколь угодно длинного текста.

Шифр – это совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом криптографического преобразования.

Основной характеристикой шифра является **криптостойкость**, которая определяет его стойкость к раскрытию методами криптоанализа. Обычно эта характеристика определяется интервалом времени, необходимым для раскрытия шифра.

Ключ – это конкретное (секретное или открытое) состояние некоторых

параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Гаммирование – процесс наложения по определенному закону гаммы шифра на открытые данные. Под гаммой шифра понимается псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму, для шифрования открытых данных и расшифровывания зашифрованных данных.

Имиттозащита – это защита системы шифрованной связи от навязывания ложных данных.

Имитовставка – это блок из m бит, который вырабатывается по определенному правилу из открытых данных с использованием ключа и затем добавляется к зашифрованным данным для обеспечения их имитозащиты.

К шифрам, используемым для криптографической защиты информации, предъявляется ряд требований:

- достаточная криптостойкость (надежность закрытия данных);
- простота процедур шифрования и расшифрования;
- незначительная избыточность информации за счет шифрования;
- нечувствительность к небольшим ошибкам шифрования и др.

Криптографическое закрытие информации имеет многовековую историю развития и применения.

Можно выделить следующие три периода развития криптографии:

1. Первый период – эра донаучной криптологии, являющейся ремеслом узкого круга искусных умельцев.

2. Началом второго периода можно считать 1949 г., когда появилась работа К. Шеннона «Теория связи в секретных системах», в которой проведено фундаментальное научное исследование шифров и важнейших вопросов их стойкости. Благодаря этому труду криптология оформилась как прикладная математическая дисциплина.

3. Начало третьему периоду было положено появлением в 1976 г. работы У. Диффи и М. Хеллмана «Новые направления в криптографии», где

показано, что секретная связь возможна без предварительной передачи секретного ключа. Так началось и продолжается до настоящего времени бурное развитие наряду с обычной классической криптографией и криптографиис открытым ключом.

Все традиционные криптографические системы можно подразделить на:

1. Шифры перестановки:

1.1. Шифр перестановки «скитала» (цилиндр + намотанная кожа).

1.2. Шифрующие таблицы (запись цифр алфавита в матрицу).

1.3. Применение магических квадратов.

2. Шифры простой замены:

2.1. Полибианский квадрат.

2.2. Система шифрования Цезаря (сдвиг текста на определенное число позиций).

2.3. Аффинная система подстановок Цезаря.

2.4. Система Цезаря с ключевым словом.

2.5. Шифрующие таблицы Трисемуса.

2.6. Биграммный шифр Плейфейра.

2.7. Криптосистема Хилла.

2.8. Система омофонов.

3. Шифры сложной замены:

3.1. Шифр Гронсфельда.

3.2. Система шифрования Виженера.

3.3. Шифр «двойной квадрат» Уитстона.

3.4. Одноразовая система шифрования.

3.5. Шифрование методом Вернама.

3.6. Роторные машины.

4. Шифрование методом гаммирования.

5. Шифрование, основанное на аналитических преобразованиях шифруемых данных

Шифрование перестановкой заключается в том, что символы шифруемого

текста переставляются по определенному правилу в пределах некоторого блока этого текста. При достаточной длине блока, в пределах которого осуществляется перестановка, и сложном неповторяющемся порядке перестановки можно достигнуть приемлемой для простых практических приложений стойкости шифра.

Шифрование заменой (подстановкой) заключается в том, что символы шифруемого текста заменяются символами того же самого (простая замена), также одно или нескольких других алфавитов (сложная замена) в соответствии с заранее обусловленной схемой замены.

Шифрование гаммированием заключается в том, что символы шифруемого текста складываются с символами некоторой случайной последовательности, именуемой гаммой шифра. Стойкость шифрования определяется в основном длиной (периодом) неповторяющейся части гаммы шифра. Данный способ является одним из основных для шифрования информации в автоматизированных системах.

Шифрование аналитическим преобразованием заключается в том, что шифруемый текст преобразуется по некоторому аналитическому правилу (формуле). Например, можно использовать правило умножения вектора на матрицу, причем умножаемая матрица является ключом шифра, а символами умножаемого вектора последовательно служат символы шифруемого текста. Другим примером может служить использование так называемых однонаправленных функций для построения криптосистем с открытым ключом.

Простейшие перестановочные шифры

С древних времен для сокрытия смысла записанного сообщения люди использовали различные хитрости. Например, удаляли пробелы и писали слова только большими (только малыми) буквами:

Это лекция по основным понятиям и истории криптографии → ЭТОЛЕКЦИЯПООСНОВНЫМПОНЯТИЯМИИСТОРИИКРИПТОГРАФИИ

Следующим шагом усложнения является разбиение зашифрованного текста на блоки:

ЭТОЛЕКЦИЯПОО СНОВ НЫМП ОНЯТ ИЯМИ ИСТО РИИК РИПТ ОГРА ФИИ

Эффективным способом шифрования является запись слов в обратном порядке: ОТЭ ЯИЦКЕЛ ОП МЫНВОНСО МЯИТЯНОП И ИИРОТСИ ИИФАРГОТПИРК

В общем случае перестановочный шифр переставляет символы исходного текста по определенной схеме. Перестановка может быть представлена в виде геометрической фигуры.

Пример 1: матрица 2 строки, 5 столбцов. Запись построчная. Чтение по столбцам сверху вниз 4, 1, 2, 5, 3.

Исходный текст M: шифрование

	1	2	3	4	5
1	**ш**	**и**	**ф**	**р**	**о**
2	**в**	**а**	**н**	**и**	**е**

Зашифрованный текст C: ришвиаоефн

Формально эта процедура записывается следующим образом: исходный текст M разбивается на блоки $M = m_1, m_2, \ldots m_i$, все блоки одинаковой длинны. Тогда зашифрованный текст будет представлен как совокупность блоков исходного текста преобразованных в соответствии с функцией f.

$E_k(M) = m_{f1},m_{f2},\ldots,m_{fi}$

Пример 2:Шифр типа «Железнодорожная изгородь». Пусть имеется правило записи текста следующего вида:

1 5 9 13
2 4 6 8 10 12 14
3 7 11 15

Геометрическая фигура соответствует изгороди. В этом случае исходный текст «ЭТО ЛЕКЦИЯ ПО ОСНОВНЫМ ПОНЯТИЯМ И ИСТОРИИ КРИПТОГРАФИИ» будет записан следующим образом:

Э Е Я С Н Я
Т Л К И П О Н В Ы П Н
О Ц О О М О

Т И О К Т И
И М И Т Р И Р П О Р Ф И
Я С И И Г А

При использовании правила чтения по строкам слева направо начиная с первой строки будет получен следующий шифротекст:

«ЭЕЯСНЯТЛКИПОНВЫПНОЦООМОТИОКТИИМИТРИРПОРФИЯСИИГА»

Ключевое слово или ключевая фраза

Одной из наиболее известных модификаций метода перестановки является использование ключевого слова или фразы в качестве правила перестановки столбцов.

Пример 3: КРИПТОГРАФИЯ может быть использовано, как ключ. Буквам ключевого слова назначаются номера, начиная с первого, в соответствии с алфавитом. Если буква встречается несколько раз, то нумерация определяется порядком следования повторяющейся буквы в ключевом слове (запись построчно, чтение по столбцам, начиная с первого столбца).

К	**Р**	**И**	**П**	**Т**	**О**	**Г**	**Р**	**А**	**Ф**	**И**	**Я**
5	8	3	7	10	6	2	9	1	11	4	12
Э	Т	О	Л	Е	К	Ц	И	Я	П	О	О
С	Н	О	В	Н	Ы	М	П	О	Н	Я	Т
И	Я	М	И	И	С	Т	О	Р	И	И	К
Р	И	П	Т	О	Г	Р	А	Ф	И	И	

В результате будет получен следующий шифротекст:

«ЯОРФЦМТРООМПОЯИИЭСИРКЫСГЛВИТТНЯИИПОАЕНИОПНИИОТК».

Метод поворачивающейся решетки

Исходный текст записывается через отверстия в решетке, которая по мере заполнения поворачивается на 90º. Предварительно текст разбивается на блоки (для решетки 4х4 клетки блок равен 16 символам). Если в последнем блоке букв получилось меньше, чем должно быть по размеру решетки – дописываем к ним нужное число букв из последовательности алфавита.

Пример 4: Разобьем исходный текст

«ЭТОЛЕКЦИЯПООСНОВНЫМПОНЯТИЯМИИСТОРИИКРИПТОГРАФИИ» на блоки по 16 символов:

ЭТОЛЕКЦИЯПООСНОВ НЫМПОНЯТИЯМИИСТО РИИКРИПТОГРАФИИ

В последнем блоке получилось 15 символов, значит дописать надо только букву А, чтобы их получилось 16:

ЭТОЛЕКЦИЯПООСНОВ НЫМПОНЯТИЯМИИСТО РИИКРИПТОГРАФИИА

Шаблон решетки представлен на рисунке 1.

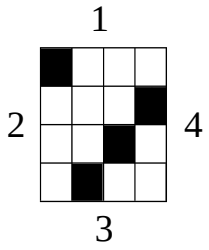


Рисунок 1 – Шаблон заполнения решетки

На рисунке закрашены черным цветом те клетки, в которые будет записываться исходный текст.

В исходном сообщении 3 блока по 16 символов, поэтому будет заполнено 3 решетки. Рассмотрим заполнение первой из них (рисунок 2). Заполнение закрашенных ячеек осуществляется построчно слева направо. Сначала в пустую таблицу в соответствии с закрашенными клетками вписываем первые 4 символа ЭТОЛ (рисунок 2а). Затем поворачиваем шаблон на 90 градусов по часовой стрелке (при этом уже заполненные буквы остаются на своих местах) и вписываем еще 4 символа ЕКЦИ (рисунок 2б). Снова поворачиваем шаблон и вписываем еще символа ЯПОО (рисунок 2в). Последний раз поворачиваем шаблон и вписываем 4 последних символа этой группы СНОВ (рисунок 2г).

э			
			т
		о	
	л		

а)

э			**е**
к			т
	ц	о	
	л	**и**	

б)

э		**я**	е
к	**п**		т
о	ц	о	
	л	и	**о**

в)

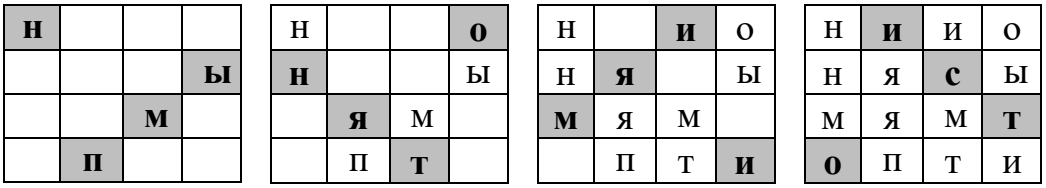
э	**с**	я	е
к	п	**н**	т
о	ц	о	**о**
в	л	и	о

г)

Рисунок 2 – Последовательное заполнение решетки

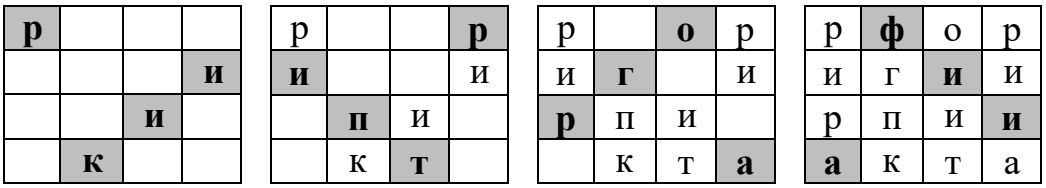
Таким же образом заполняем решетки для двух оставшихся групп символов: НЫМПОНЯТИЯМИИСТО (рисунок 3) и РИИКРИПТОГРАФИИА

(рисунок 4).



а) б) в) г)

Рисунок 3 – Заполнение решетки для текста НЫМПОНЯТИЯМИИСТО



а) б) в) г)

Рисунок 4 – Заполнение решетки для текста РИИКРИПТОГРАФИИА

После того как заполнили все 3 решетки, можно составить шифротекст. Для этого записываем символы из решетки построчно, слева направо, начиная с первой решетки: ЭСЯЕКПНТОЦООВЛИОНИИОНЯСЫМЯМТОПТИ РФОРИГИИРПИИАКТА.

Примечание: решетка не обязательно должна быть именно такой конструкции. Для того чтобы изготовить решетку, нужно:

– построить матрицу 4х4;

– ячейки матрицы, которые при повороте матрицы на 90 градусов занимают одинаковое положение, пронумеровать одинаково

– вырезать по одной ячейке каждого номера.

Простейшие подстановочные шрифты

Исследования по созданию эффективных подстановочных шифраторов были направлены в сторону поиска математического описания процедуры шифрования. В этом случае таблица подстановки присутствует в неявном виде, что существенно упрощает как саму процедуру шифрования, так и использование подобных систем на практике. Классическим примером подобных криптосистем является шифр Цезаря. Свое название этот шифр получил по имени римского императора Гая Юлия Цезаря, который использовал этот шифр при переписке с Цицероном.

Таблица подстановки присутствует в неявном виде, т.е. символ шифротекста вычисляется по математическому выражению (1).

$$c_i = (a_i + k) mod\ n, \quad (1)$$

где a_i– символ исходного текста;

k – ключ;

n – мощность алфавита.

В шифре Цезаря используется k = 3.

Для английского алфавитас использованием последовательной нумерации букв 0–A, 1–B, 2–C, 3–D, 4–E, 5–F, 6–G, 7–H, 8–I, 9–J, 10–K, 11–L, 12–M,13–N, 14–O, 15–P, 16–Q, 17–R, 18–S, 19–T, 20–U, 21–V, 22–W, 23–X, 24–Y,25–Z, процедура шифрования, предложенная Цезарем, будет описываться соотношением (2).

$$c_i = (a_i + 3) mod\ 26. \quad (2)$$

В данном случае и a_i, и c_i представляют собой номера букв в исходном алфавите. При шифровании буквы B исходного алфавита имеющей номер 1, получим$c_i = 1 + 3 = 4$, что соответствует букве E, используемой в качестве подстановочного элемента в шифротексте.

Пример 5: При шифровании исходного текста *M*=C*R*Y*P*TOG*R*A*P*HY получим *C*=FUBSW*R*JUDSKB.

Развитием этого метода является метод, основанный на свойстве децимации (децимация – выборка *k*-тых элементов):

$$c_i = (a_i * k) mod\ n. \quad (3)$$

Тогда номера символов в шифротексте будут в k раз больше номеров символов исходного текста, например

0	1	2	3	0	3	6	9
A	B	C	D	A	D	F	G

Аффинное преобразование:

$$c_i = (k_1 a_i + k_2) mod\ n. \quad (4)$$

В данном случае используется 2 ключа: k_1 и k_2. Причем накладывается требование взаимной простоты (k_1, n) = 1.

Квадрат Полибия

Шахматная доска Полибия – оригинальный код простой замены, одна из древнейших систем кодирования, предложенная Полибием (греческий историк, полководец, государственный деятель, III век до н. э.).

Шаг 1: Формирование таблицы шифрования.

К каждому языку отдельно составляется таблица шифрования (таблица 1) с одинаковым (не обязательно) количеством пронумерованных строк и столбцов, параметры которой зависят от его мощности (количества букв в алфавите). Берутся два целых числа, произведение которых ближе всего к количеству букв в языке – получаем нужное число строк и столбцов. Затем вписываем в таблицу все буквы алфавита подряд – по одной в каждую клетку. При нехватке клеток можно вписать в одну две буквы (редко употребляющиеся или схожие по употреблению).

Таблица 1 – Таблица шифрования для русского алфавита

	1	**2**	**3**	**4**	**5**	**6**
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	—	—	—

Шаг 2: Принцип шифрования.

Метод 1 – Для шифрования на квадрате находили букву текста и вставляли в шифровку нижнюю от нее в том же столбце. Если буква была в нижней строке, то брали верхнюю из того же столбца.

Пример 6: Зашифруем сообщение «ЭТО ЛЕКЦИЯ ПО ОСНОВНЫМ ПОНЯТИЯМ И ИСТОРИИ КРИПТОГРАФИИ».

Буква текста	Э	Т	О	Л	Е	К	Ц	И	Я	П	О	О	С	Н	О	В	Н
Буква шифротекста	А	Ш	Ф	С	К	Р	Ь	О	В	Х	Ф	Ф	Ч	У	Ф	З	У
Буква текста	Ы	М	П	О	Н	Я	Т	И	Я	М	И	И	С	Т	О	Р	И
Буква шифротекста	Д	Т	Х	Ф	У	В	Ш	О	В	Т	О	О	Ч	Ш	Ф	Ц	О
Буква текста	И	К	Р	И	П	Т	О	Г	Р	А	Ф	И	И				
Буква шифротекста	О	Р	Ц	О	Х	Ш	Ф	И	Ц	Ё	Ъ	О	О				

Шифротекст выглядит следующим образом: АШФСКРЬОВХФФЧУФЗУДТХФУВШОВТООЧШФЦООРЦОХШФИЦЁЪОО.

Метод 2 – Сообщение преобразуется в координаты по квадрату Полибия, координаты записываются вертикально (сначала номер столбца, затем номер строки). Затем координаты считывают по строкам, разбив на пары. Далее координаты преобразуются в буквы по тому же квадрату.

Пример 7: Зашифруем сообщение «ЭТО ЛЕКЦИЯ ПО ОСНОВНЫМ ПОНЯТИЯМ И ИСТОРИИ КРИПТОГРАФИИ».

Буква текста	Э	Т	О	Л	Е	К	Ц	И	Я	П	О	О	С	Н	О	В	Н
Номер столбца	1	2	4	1	6	6	6	4	3	5	4	4	1	3	4	3	3
Номер строки	6	4	3	3	1	2	4	2	6	3	3	3	4	3	3	1	3
Буква текста	Ы	М	П	О	Н	Я	Т	И	Я	М	И	И	С	Т	О	Р	И
Номер столбца	5	2	5	4	3	3	2	4	3	2	4	4	1	2	4	6	4
Номер строки	5	3	3	3	3	6	4	2	6	3	2	2	4	4	3	3	2
Буква текста	И	К	Р	И	П	Т	О	Г	Р	А	Ф	И	И				
Номер столбца	4	6	6	4	5	2	4	4	6	1	4	4	4				
Номер строки	2	2	3	2	3	4	3	1	3	1	4	2	2				

Теперь считываем координаты построчно, разбив их на пары: 1 2416664 35441343 36 43 31 24263334331352543324324412464533336 4 263224433246 64524461444232343131422.

Выполнить самостоятельно преобразование данных координат в шифротекст по квадрату.

Метод 3 – Усложненный вариант, который заключается в следующем: полученный первичный шифротекст шифруется вторично. При этом он выписывается без разбиения на пары. Полученная последовательность цифр сдвигается циклически влево на один шаг (нечетное количество шагов). Эта последовательность вновь разбивается в группы по два и по таблице заменяется на окончательный шифротекст.

Шифр Виженера

Примером многоалфавитного шифра замены является так называемая система Виженера. Шифрование осуществляется по таблице (таблица 2),

представляющей собой квадратную матрицу размерностью NxN, гдеN – число символов используемого алфавита.

Таблица 2 – Таблица Виженера для русского алфавита

а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а
в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б
г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в
д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г
е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д
ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е
ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё
з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж
и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з
й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и
к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й
л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к
м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л
н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м
о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н
п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о
р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п
с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р
т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с
у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т
ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у
х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф
ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х
ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ
ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы
э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь
ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э
я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю

Выбирается ключ или ключевая фраза. После чего процесс зашифровывания осуществляется следующим образом: под каждой буквой исходного сообщения последовательно записываются буквы ключа; если ключ оказался короче сообщения, его используют несколько раз. Каждая буква шифротекста находится на пересечении столбца таблицы, определяемого буквой открытого текста, и строки, определяемой буквой ключа.

Пример 8: Зашифруем сообщение «ЭТО ЛЕКЦИЯ ПО ОСНОВНЫМ ПОНЯТИЯМ И ИСТОРИИ КРИПТОГРАФИИ» с ключевым словом ШИФРОТЕКСТ.

Буква текста	Э	Т	О	Л	Е	К	Ц	И	Я	П	О	О	С	Н	О	В	Н
Ключевое слово	Ш	И	Ф	Р	О	Т	Е	К	С	Т	Ш	И	Ф	Р	О	Т	Е
Шифротекст	Х	Ы	Г	Ь	У	Э	Ы	У	Р	В	Ж	Ч	Ё	Ю	Э	Ф	Т
Буква текста	Ы	М	П	О	Н	Я	Т	И	Я	М	И	И	С	Т	О	Р	И
Ключевое слово	К	С	Т	Ш	И	Ф	Р	О	Т	Е	К	С	Т	Ш	И	Ф	Р
Шифротекст	Ё	Ю	В	Ж	Ц	У	Г	Ч	С	С	У	Ъ	Д	К	Ч	Е	Щ
Буква текста	И	К	Р	И	П	Т	О	Г	Р	А	Ф	И	И				
Ключевое слово	О	Т	Е	К	С	Т	Ш	И	Ф	Р	О	Т	Е				
Шифротекст	Ч	Э	Х	У	Б	Е	Ж	Л	Е	Р	Г	Ы	Н				

Расшифровывание осуществляется следующим образом: под буквами шифротекста последовательно записываются буквы ключа; в строке таблицы, соответствующей очередной букве ключа, происходит поиск соответствующей буквы шифротекста. Находящаяся над ней в первой строке таблицы буква является соответствующей буквой исходного текста.

Самостоятельно расшифровать данный текст по таблице Виженера.

Методы криптоанализа

Информация в процессе хранения, передачи и преобразования подвергается воздействию различных атак. Атаки осуществляются противниками (оппонентами, перехватчиками, врагами и т.д.). Основными нарушениями безопасности являются раскрытие информационных ценностей (потеря конфиденциальности), модификация без разрешения автора (потеря целостности) или неавторизованная потеря доступа к этим ценностям (потеря доступности).

Криптоанализ любого шифра невозможен без учета особенностей текстов сообщений, подлежащих шифрованию. Одним из самых популярных методов криптоанализа является частотный анализ текста.

Частотный анализ

Частотный анализ – это один из методов криптоанализа, основывающийся на предположении о существовании нетривиального статистического распределения отдельных символов и их последовательностей как в открытом тексте, так и шифрованном тексте, которое с точностью до замены символов будет сохраняться в процессе шифрования и дешифрования.

Частотный анализ предполагает, что частота появления заданной буквы алфавита в достаточно длинных текстах одна и та же для разных текстов одного языка. При этом в случае моноалфавитного шифрования, если в шифрованном тексте будет символ с аналогичной вероятностью появления, то можно предположить, что он и является указанной зашифрованной буквой. Аналогичные рассуждения применяются к биграммам (двубуквенным последовательностям), триграммам в случае полиалфавитных шифров.

Метод частотного анализа известен с еще IX-го века и связан и именем Ал Кинди. Но наиболее известным случаем применения такого анализа является дешифровка египетских иероглифов Ж.-Ф. Шампольоном в 1822 году. Данный вид анализа основывается на том, что текст состоит из слов, а слова из букв. Количество различных букв в каждом языке ограничено и буквы могут быть просто перечислены. Важными характеристиками текста являются повторяемость букв, пар букв (биграмм) и вообще m-грамм, сочетаемость букв друг с другом, чередование гласных и согласных букв и некоторые другие.

Идея состоит в подсчете чисел вхождений каждой nm возможных m-грамм в достаточно длинных открытых текстах $T=t_1t_2\ldots t_l$, составленных из букв алфавита $\{a_1, a_2, ..., a_n\}$. При этом просматриваются подряд идущие m-граммы текста: $t_1t_2...t_m$, $t_2t_3... t_{m+1}$, ..., $t_{i-m+1}t_{l-m+2}...t_l$. Если T – число появлений m-граммы $a_{i1}a_{i2}...a_{im}$ в тексте, а L – общее число подсчитанных m-грамм, то опыт показывает, что при достаточно больших L частоты для данной m-граммы мало отличаются

друг от друга. В силу этого относительную частоту считают приближением вероятности P ($a_{i1}a_{i2}...a_{im}$) появления данной m-граммы в случайно выбранном месте текста (такой подход принят при статистическом определении вероятности).

Существует множество различных таблиц о распределении букв в том или ином языке, но ни одна из них не содержит окончательной информации – даже порядок букв может отличаться в различных таблицах. Распределение букв очень сильно зависит от типа теста: проза, разговорный язык, технический язык и т.п. Практически в каждом языке примерно девять букв заполняют около 70% любого текста – остальное распределение зависит от содержания и формы текста. В таблицеЗприводятся частоты встречаемости букв в русском языке (в процентах).

Таблица 3 – Частоты букв русского алфавита

Буква алфавита	Показатель частоты встречаемости	Буква алфавита	Показатель частоты встречаемости	Буква алфавита	Показатель частоты встречаемости
О	10,983	М	3,203	Й	1,208
Е	8,483	Д	2,977	Х	0,966
А	7,998	П	2,804	Ж	0,94
И	7,367	У	2,615	Ш	0,718
Н	6,7	Я	2,001	Ю	0,638
Т	6,318	Ы	1,898	Ц	0,486
С	5,473	Ь	1,735	Щ	0,361
Р	4,746	Г	1,687	Э	0,331
В	4,533	З	1,641	Ф	0,267
Л	4,343	Б	1,592	Ъ	0,037
К	3,486	Ч	1,45	Ё	0,013

Устойчивыми являются также частотные характеристики биграмм, триграмм и четырехграмм осмысленных текстов. Существуют специальные таблицы с указанием частоты биграмм некоторых алфавитов. По результатам исследований с помощью таких таблиц ученые определили наиболее часто встречаемые биграммы и триграммы для русского алфавита: СТ, НО, ЕН, ТО, НА, ОВ, НИ, РА, ВО, КО, СТО, ЕНО, НОВ, ТОВ, ОВО, ОВА. Результатом таких исследований является таблица (таблица 4), в которой слева и справа от каждой буквы расположены наиболее предпочтительные «соседи» (в порядке убывания частоты соответствующих биграмм). В таких таблицах обычно указывается также

доля гласных и согласных букв (в процентах), предшествующих данной букве (или следующих за ней).

Таблица 4 – Соседние буквы для текстов из русского алфавита

Г	С	Слева		Справа	Г	С
3	97	л, д, к, т, в, р, н	А	л, н, с, т, р, в, к, м	12	88
80	20	я, е, у, и, а, о	Б	о, ы, е, а, р, у	81	19
68	32	я, т, а, е, и, о	В	о, а, и, ы, с, н, л, р	60	40
78	22	р, у, а, и, е, о	Г	о, а, р, л, и, в	69	31
72	28	р, я, у, а, и, е, о	Д	е, а, и, о, н, у, р, в	68	32
19	81	м, и, л, д, т, р, н	Е	н, т, р, с, л, в, м, и	12	88
83	17	р, е, и, а, у, о	Ж	е, и, д, а, н	71	29
89	11	о, е, а, и	З	а, н, в, о, м, д	51	49
27	73	р, т, м, и, о, л, н	И	с, н, в, и, е, м, к, з	25	75
55	45	ь, в, е, о, а, и, с	К	о, а, и, р, у, т, л, е	73	27
77	23	г, в, ы, и, е, о, а	Л	и, е, о, а, ь, я, ю, у	75	25
80	20	я, ы, а, и, е, о	М	и, е, о, у, а, н, п, ы	73	27
55	45	д, ь, н, о	Н	о, а, и, е, ы, н, у	80	20
11	89	р, п, к, в, т, н	О	в, с, т, р, и, д, н, м	15	85
65	35	в, с, у, а, и, е, о	П	о, р, е, а, у, и, л	68	32
55	45	и, к, т, а, п, о, е	Р	а, е, о, и, у, я, ы, н	80	20
69	31	с, т, в, а, е, и, о	С	т, к, о, я, е, ь, с, н	32	68
57	43	ч, у, и, а, е, о, с	Т	о, а, е, и, ь, в, р, с	63	37
15	85	п, т, к, д, н, м, р	У	т, п, с, д, н, ю, ж	16	84
70	30	н, а, е, о, и	Ф	и, е, о, а, е, о, а	81	19
90	10	у, е, о, а, ы, и	Х	о, и, с, н, в, п, р	43	57
69	31	е, ю, н, а, и	Ц	и, е, а, ы	93	7
82	18	е, а, у, и, о	Ч	е, и, т, н	66	34
67	33	ь, у, ы, е, о, а, и, в	Ш	е, и, н, а, о, л	68	32
84	16	е, б, а, я, ю	Щ	е, и, а	97	3
0	100	м, р, т, с, б, в, н	Ы	л, х, е, м, и, в, с, н	56	44
0	100	н, с, т, л	Ь	н, к, в, п, с, е, о, и	24	76
14	86	с, ы, м, л, д, т, р, н	Э	н, т, р, с, к	0	100
58	42	ь, о, а, и, л, у	Ю	д, т, щ, ц, н, п	11	89
43	57	о, н, р, л, а, и, с	Я	в, с, т, п, д, к, м, л	16	84

В англоязычном тексте наиболее встречающимися буквами будут E, T, A,в то время как самыми редкими буквами являются J, Q, Z. Посчитав частоту появления каждой буквы в тексте, мы можем определить насколько частотная характеристика текста соответствует английскому языку.

Простейшая защита против атак, основанных на подсчете частот,

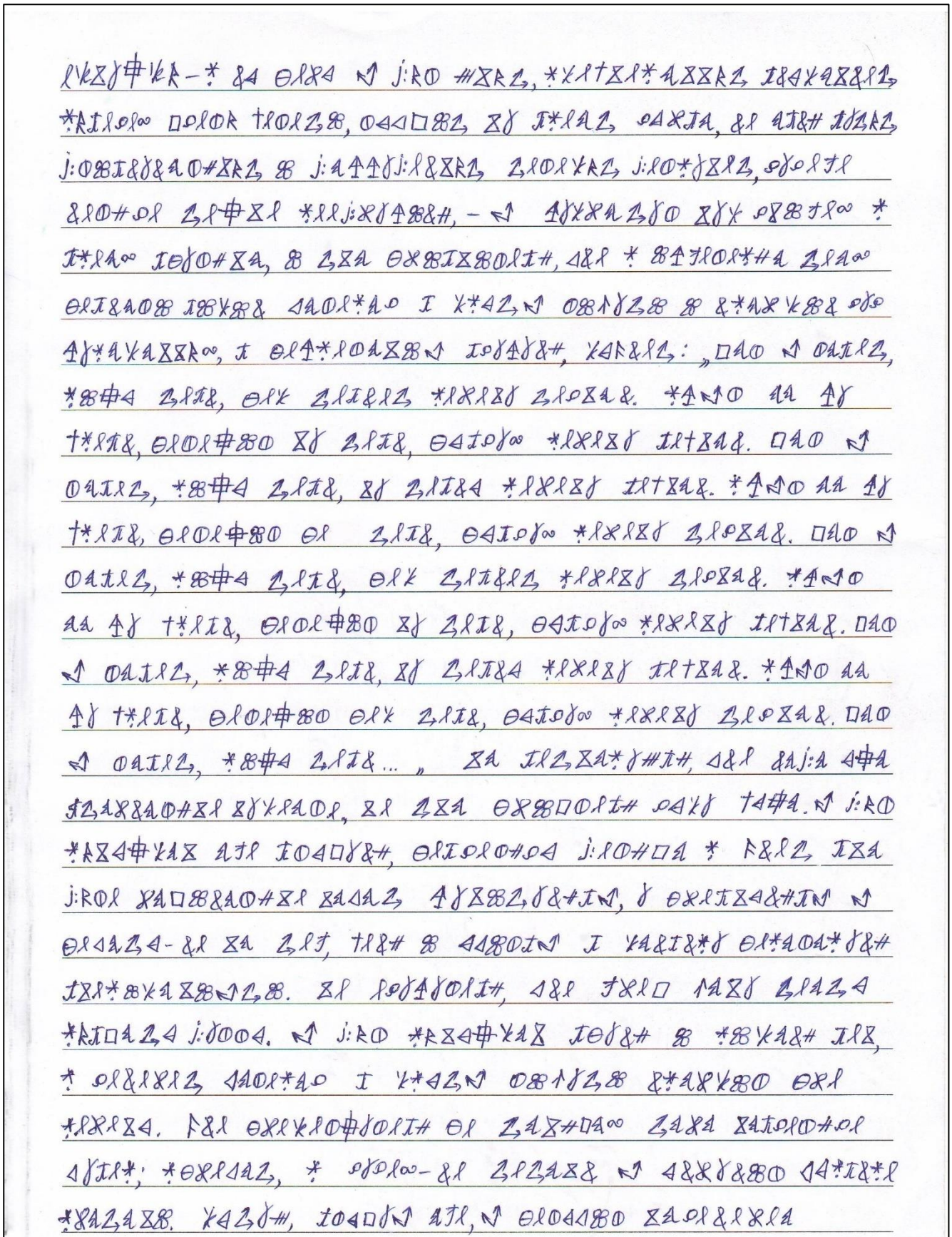
обеспечивается в системе омофонов – однозвучных подстановочных шифров, в которых один символ открытого текста отображается на несколько символов шифротекста, их число пропорционально частоте появления буквы. Шифруя букву исходного сообщения, мы выбираем случайно одну из ее замен. Следовательно, простой подсчет частот ничего не дает криптоаналитику. Однако доступна информация о распределении пар и троек букв в различных естественных языках. Криптоанализ, основанный на такой информации будет более успешным.

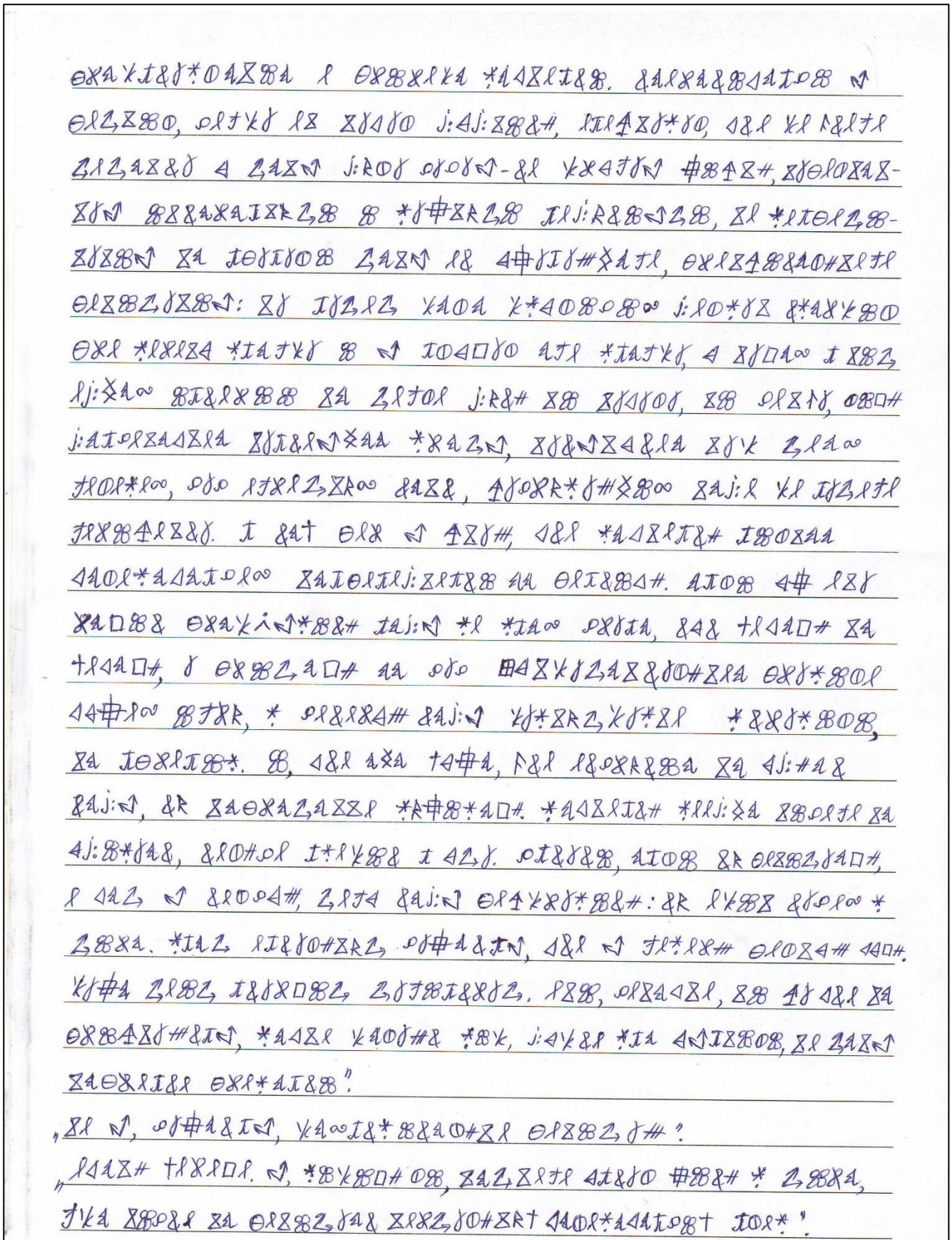
Шифры моноалфавитной замены довольно легко расшифровать даже без знания ключа. Делается это при помощи частотного анализа зашифрованного текста – надо посчитать, сколько раз каждая буква встречается в тексте, и затем поделить на общее число букв. Получившуюся частоту надо сравнить с эталонной. Самая частая буква для русского языка – это буква О, за ней идет Е и т.д. Правда, работает частотный анализ на больших литературных текстах. Если текст маленький или очень специфический по используемым в нем словам, то частотность букв будет отличаться от эталонной, и времени на разгадывание придется потратить больше.

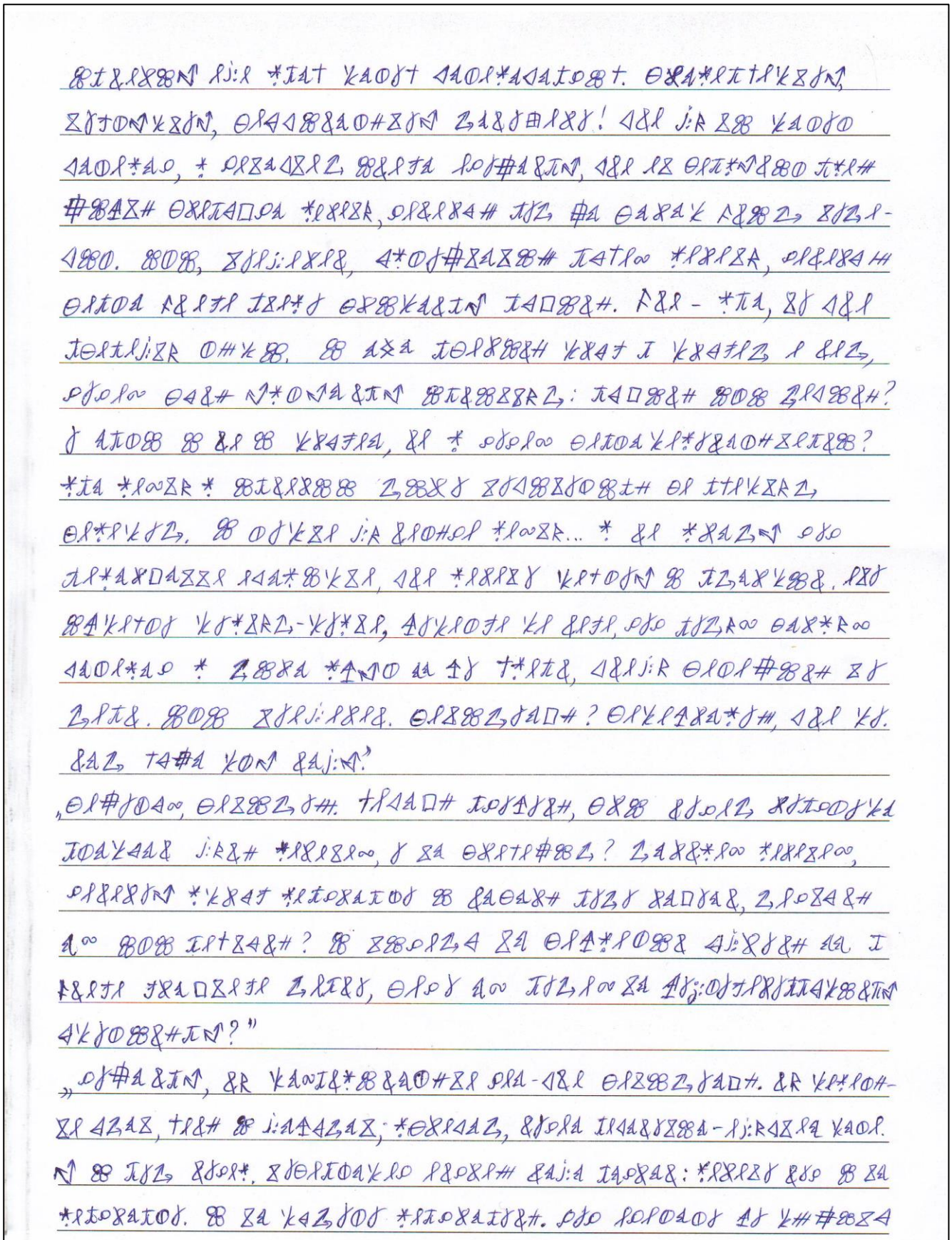
Анализируя достаточно длинный текст, зашифрованный методом замены, можно по частотам появления символов произвести обратную замену и восстановить исходный текст.

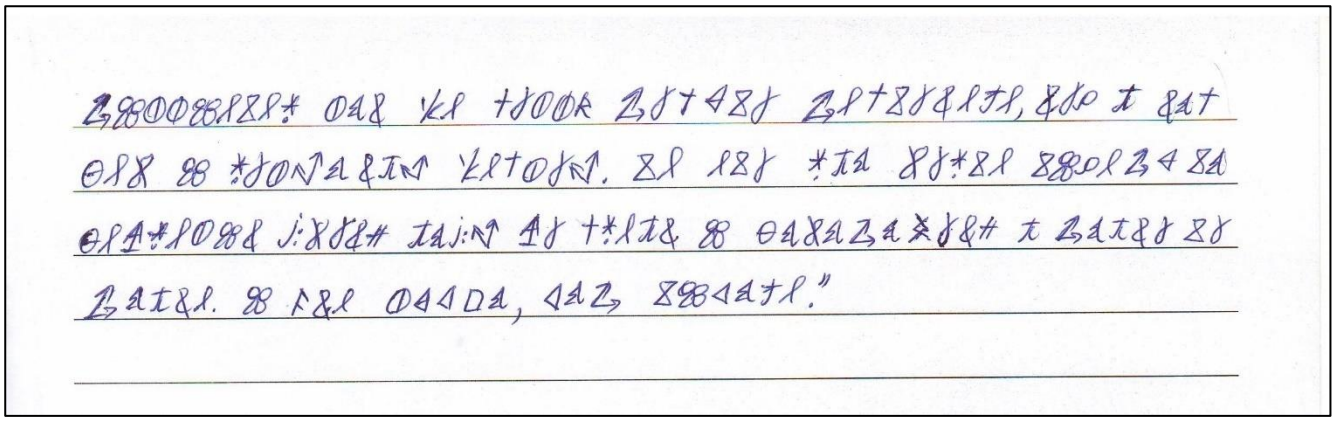
Как было отмечено выше, каждый метод криптоанализа добавляет новые требования к алгоритмам шифрования. Частотный метод, в котором по распределению символов в шифротексте выдвигаются гипотезы о ключе шифрования, породил требование равномерного распределения символов в шифротексте. Кроме того, принципы частотного анализа сегодня широко применяются в программах по поиску паролей и позволяют сократить перебор в десятки и сотни раз.

Пример 9: Рассмотрим механизм частотного анализа для зашифрованного текста. Данный текст относится к художественной литературе.









Сначала необходимо посчитать сколько всего символов в данном тексте. В данном тексте 4381 символ. Затем считаем для каждого символа количество раз, которое он встречается в тексте и вычисляем частоты (делим на общее количество символов). Представим результат вычислений в виде таблицы 5.

Таблица 5 – Частоты символов в тексте

Символ	Количество в тексте	Частота	Символ	Количество в тексте	Частота	Символ	Количество в тексте	Частота
	577	0,1317		127	0,029		50	0,0114
	378	0,0863		123	0,0281		50	0,0114
	290	0,0662		123	0,0281		46	0,0105
	285	0,0651		119	0,0272		44	0,01
	282	0,0644		107	0,0244		25	0,0057
	267	0,0609		102	0,0233		15	0,0034
	263	0,06		83	0,0189		13	0,003
	210	0,0479		71	0,0162		6	0,0014
	199	0,0454		68	0,0155		2	0,0005
	189	0,0431		57	0,013		1	0,0002
	158	0,0361		51	0,0116			

Предположим, что самый часто встречающийся символ из таблицы 5 соответствует самому часто встречающемуся символу из таблицы 3. Тогда

символом  зашифрована буква О. Второй по частоте символ в тексте –  , предположим, что им зашифрована вторая по частоте буква русского алфавита – Е. Теперь нужно попробовать найти в тексте противоречия нашим предположениям или, наоборот, подтвердить их. Противоречием, например, будет являться одиночный символ  в тексте, поскольку слова Е в русском языке нет.

Одиночный символ  в тексте не был найден, однако найдено слово  . В русском языке есть только одно слово, не являющееся каким-либо названием или аббревиатурой, в котором две одинаковые буквы – «её», что подтверждает наше предположение. Таким образом, символ  обозначает буквы Е и Ё. Тогда слово  может обозначать «ЖЕ», «НЕ» или «ТЕ».

В тексте были найдены слова:  ,  ,  , , , т.е. слово О и 4 разных двухбуквенных слова. Тогда вторая буква – точно буква О, поскольку, во-первых, есть слово О, во-вторых, именно с буквой О есть такое количество двухбуквенных слов.

Слово  , такое что известны буквы Е_О, может быть только ЕГО, поэтому символ  обозначает букву Г.

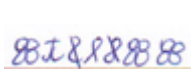
Третий по частоте встречаемости в тексте – символ  , а в русском алфавите – буквы А, И, Н. Рассмотрим возможность того, что символ  – это буква А или буква И. Тогда  – это либо слово АО, либо ИО, а слово  – это либо ОА, либо ОИ, что бессмысленно. Если же символ  – это буква Н, то – это слово НО, а – это слово ОН. Оба слова имеют смысл, поэтому наше предположение верно.

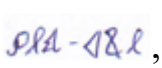
Четвертый по частоте встречаемости в тексте – символ  , а в русском алфавите – А, И, Т. Рассмотрим возможность того, что символ – это буквы А, И или Т. Тогда  – это слово АОА, ИОИ или ТОТ. Очевидно, что смысл будет только в последнем случае, значит – это буква Т.

Следующий символ по частоте встречаемости в тексте –  . Рассмотрим, может ли он обозначать букву А, либо букву И. В тексте есть слово  , слово А, как и слово И также есть в русском языке, поэтому явного противоречия здесь нет. В тексте есть слово  , в котором нам уже известны некоторые буквы: ОН_. Это может быть как слово ОНА, так и слово ОНИ.

Данных недостаточно, для того, чтобы понять, какая буква обозначена данным символом. Поэтому пока рассмотрим следующий символ –  . В тексте есть слово  . Предположим также, что символ  – это буква А или буква И. С буквой И мы можем составить слово ИЛИ. Тогда символ  – это буква И, символ  – это буква Л, а символ  – это буква А.

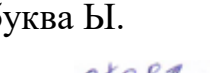
Следующий символ по частоте встречаемости в тексте –  , а в алфавите – буквы С и Р. Предположим, что символ обозначает букву С. В тексте есть слово  , в котором известны буквы Е_ЛИ. Тогда, подставив вместо символа букву С, получим осмысленное слово ЕСЛИ, значит, наше предположение верно.

В тексте есть слово  , в котором мы уже знаем буквы ИСТО_ИИ. Пропущенной буквой может быть только буква Р, значит она обозначена символом  .

В тексте есть слово  , в котором известны буквы _ОЕ-_ТО, где очевидно, что пропущенные буквы могут быть только К и Ч, поэтому делаем вывод, что символ  обозначает букву К, а символ  – букву Ч.

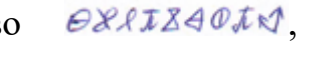
В тексте есть слово  и могут обозначать «ОНО», «ОБО», «ОТО», «ОКО», но т.к. буквы Н, Т и К уже найдены, значит символом обозначена буква Б.

В тексте есть слово , в котором известны буквы ОБ_ЧНОЕ, значит символом обозначена буква Ы.

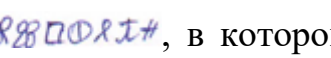
В тексте есть фраза  , в которой известны буквы КАКО_-ТО С_ЫСЛЕ. Очевидно, что в данной фразе пропущена буква М, которая

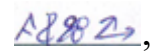
обозначается символом  .

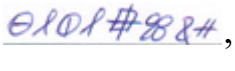
В тексте есть фраза  , в которой известны буквы _ОМЕСТИЛИ БЫ НАС _ О_НОМ КОР__СЕ. Сразу понятно, что символом  обозначена буква В, а в первом слове пропущена буква П, обозначенная символом  . В последнем слове теперь неизвестна только одна буква: КОРП_СЕ. Этой буквой может быть только буква У, обозначенная символом  . В слове О_НОМ может быть пропущена буква Д, обозначенная символом  .

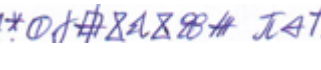
В тексте есть слово  , в котором известны буквы ПРОСНУЛС_, значит символом  обозначена буква Я.

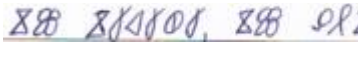
В тексте есть слово  , в котором известны буквы _АБЛАГОРАССУДИТСЯ, а пропущена только буква З, обозначенная символом  .

В тексте есть слово  , в котором известны буквы ПРИ_ЛОС_, тогда понятно, что пропущены буква Ш, обозначенная символом  , и буква Ь, обозначенная символом  .

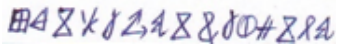
В тексте есть слово  , в котором известны буквы _ТИМ, поэтому можно сказать, что символом  обозначена буква Э.

В тексте есть слово  , в котором известны буквы ПОЛО_ИТЬ, значит, пропущена здесь буква Ж, обозначенная символом  .

В тексте есть фраза  , в которой известны буквы УВЛАЖНЕНИ_ СУ_О_, значит, в первом слове символом  может быть обозначена только буква Ю (буквы Е и Я уже заняты). По смыслу подбираем второе слово из неизвестных нам пока букв: СУХОЙ. Значит, символом  обозначена буква Х, а символом  – буква Й.

В тексте есть фраза  , в которой известны буквы НИ НАЧАЛА, НИ КОН_А, значит, пропущена буква Ц, обозначенная

символом  .

В тексте есть слово  , в котором известны буквы _УНДАМЕНТАЛЬНОЕ, значит, пропущенная буква Ф обозначается символом  .

В тексте есть слово  , в котором известны буквы НАСТОЯ_ЕЕ, значит, пропущенная буква Щ обозначается символом  .

В итоге мы знаем, как обозначаются все буквы кроме Ъ, которая обозначается символом  .

Результат частотного анализа представлен в таблице 6.

Таблица 6 – Алфавит, полученный в результате частотного анализа

Символ	Буква	Символ	Буква	Символ	Буква	Символ	Буква
	О		М		Ь		Ж
	Е/Ё		В		Ч		Й
	Н		Р		Ы		Ю
	Т		К		Б		Э
	А		Д		З		Щ
	И		П		Г		Ц
	С		У		Ш		Ф
	Л		Я		Х		Ъ

2 Лабораторные работы

2.1 Лабораторная работа «Подстановочные и перестановочные шифры»

2.1.1 Задания

Лабораторная работа состоит из двух частей. Для выполнения первой части в качестве домашнего задания студентам выдается следующее: посмотреть видео Взломщики кодов, прочитать произведения Артура Конан Дойля «Пляшущие человечки» и Эдгара Аллана По «Золотой жук».

Часть 1

Задание 1: Посмотреть видео «Взломщики кодов». Выписать примеры применения криптографии, рассмотренные в данном видео.

Задание 2: Изучить применение криптографии в произведении Артура Конан Дойля «Пляшущие человечки». Ответить на вопросы:

– Кто в произведении использовал шифр?

– Кому предназначался зашифрованный текст?

– На каком носителе он был написан?

– Какая информация передавалась (записать текст в зашифрованном и расшифрованном виде)?

Задание 3: Изучить применение криптографии в произведении Эдгара Аллана По «Золотой жук». Ответить на вопросы:

– Кто расшифровывал зашифрованный текст?

– На каком носителе он был написан?

– Какая информация передавалась? (записать текст в зашифрованном и расшифрованном виде).

Задание 4: Привести свой пример использования криптографии в литературе. Описать метод шифрования и назначение зашифрованного текста.

Часть 2

Задание 1: Разработать программу, выполняющую шифрование текста и его дальнейшее расшифрование не менее чем двумя перестановочными методами.

Задание 2: Разработать программу, выполняющую шифрование текста подстановочным методом (аффинное преобразование) и его расшифрование. Добавить возможность сохранять полученный шифротекст в текстовый файл.

2.1.2 Требования к отчету по лабораторной работе

В отчете по лабораторной работе «Подстановочные и перестановочные шифры» необходимо представить:

– для каждого задания части 1 подробный ответ на вопросы;

– для каждого задания части 2 отформатированный код, сопровождаемый разумным количеством комментариев и результат запуска программы (снимок окна приложения с результатом, выведенным на экран после нажатия кнопки).

Отчет по лабораторной работе оформляется в соответствии с требованиями, принятыми в КГПИ ФГБОУ ВО «КемГУ», предоставляется преподавателю в электронном виде.

2.1.3 Контрольные вопросы

1. Как принято классифицировать традиционные криптографические системы?
2. Какие шифры относятся к простейшим перестановочным?
3. К какому типу шифров относится шифр Цезаря?
4. В чем суть метода Виженера?
5. Как выглядит таблица Виженера?
6. В чем суть метода поворачивающейся решетки?
7. В чем суть метода Квадрат Полибия?
8. Какие существуют варианты шага 2 для метода «Квадрат Полибия»?

2.2 Лабораторная работа «Методы вскрытия шифров»

2.2.1 Задания

Лабораторная работа состоит из двух заданий.

Задание 1. Выполнить дешифрование текста методом частотного анализа.

Ƶ∞ ⁂€∞□♫

— …¥ Ω♠Ω ∞®֍¥≠ α μξ≠♣■¥☼ μ∞Ƶ®∞☼, — βξαξ֍¥⁑ ƵΩƵ∞⁂♥⁑Ƶ♥± ⁑ξƵ¥, — €∞-€∞, α⁂Ω ☺αΩ⁑∞, ®֍ξπΩ ®֍∞τ≠∞®∞. ¥ ®¥⁂⁂¥. ƵΩ⁑, ƵΩ ♦⁑¥, ∞ αξƵ ⁑Ω. TΩ֍α♥±, α⁑ξ֍ξ±, ⁑֍Ω⁑¥± ¥ Ƶ♫≠Ωα®♫. ¥ πξ©Ω⁑ μ♥⁑♣… €∞, αξ⁑ ⁑∞®ξ± π∞⁂⁂¥☼¥Ƶ. ¥ Ω♠Ω ⁑∞®ξ±. ∞ ♦⁑ξ ♫ Ƶ∞⁂ □⁑ξ αξƵ Ƶ∞ ⁑ξ± τξ≠®Ω?..

Tξ®∞ π♥ τ∞®♫Ωπ €ξμ♥□♫ α ֍♪®£∞®¥, π∞≠ΩƵ♣®∞⅟ ⁂Ω€∞⅟ τ֍ξ€∞α♠¥☺∞ ⁂♫Ω⁑≠¥αξ ֍ξΩ⁑⁂⅟ α ®∞⁂⁂Ω, ®∞® τ⁑¥☺∞ α ®ξ֍π♫■®Ω, ¥♠Ω⁑ ⁑∞π ⁂€∞□♫ ⁂ ⁑ξƵ¥Ƶξ± €α♫☼⁂ξ⁑≠¥⁑ξαξ± ®♫τ♪֍♥.

— ΠΩ≠ξ□¥ ⁂ξα⁂Ωπ ƵΩ⁑, — Ƶ∞®ξƵΩ☺ α£€♥☼∞Ω⁑ ξƵ∞. — Πξ©Ω⁑ μ♥⁑♣, αξ£♣πΩ⁑Ω Ƶ∞ ⁂€∞□♫?

®≠∞€Ω⁑ Ƶ∞ τ֍¥≠∞αξ® ®ξ֍ξμ®♫ ⁂ ☺αΩ⁑Ƶ♥π¥ πΩ≠®∞π¥. ƵΩ τ∞⁂⁑Ω≠♣Ƶ♥π¥, ƵΩ αξ⁂®ξα♥π¥ €∞©Ω, ∞ ξμ♥□Ƶ♥π¥, ®ξ⁑ξ֍♥Ω ⁑ξ≠♣®ξ ¥ βξ€⅟⁑⁂⅟ Ƶ∞ ■®ξ≠♣Ƶξ± €ξ⁂®Ω ֍¥⁂ξα∞⁑♣. ¥ ®ξƵΩ□Ƶξ, Ƶ∞ ∞⁂ ▼∞≠♣⁑Ω.

ΠƵΩ ƵΩ €ξ πΩ≠®ξα, ⅟ τ♥⁑∞♪⁂♣ £∞⁂⁑ΩβƵ♫⁑♣ ֍♪®£∞®, ∞ ⁑ξƵ¥ ֍∞⁂⁂Ω⅟ƵƵξ ⁂♫Ω⁑ ®ξ֍ξμ®♫ α ®∞֍π∞Ƶ. T֍ξ€∞α♠¥☺∞, ♫μΩ€¥α■¥⁂♣, □⁑ξ τ֍ξμ≠Ωπ∞ ⁂ξ ⁂€∞□Ω± ♫≠∞©ΩƵ∞, ֍∞⁂τ≠♥α∞Ω⁑⁂⅟ α ♫≠♥μ®Ω.

— Aξ⁑ ¥ ☼ξ֍ξ■ξ, — βξαξ֍¥⁑ ξƵ∞ Ƶ∞π α⁂≠Ω€. — €Ω⁑⅟π τξ€∞֍¥⁑Ω, τ♫⁂⁑♣ ֍¥⁂♫♪⁑.

Ƶ¥ ♫ ⁑ξƵ¥, Ƶ¥ ♫ πΩƵ⅟ ƵΩ⁑ €Ω⁑Ω±. Ƶξ ♦⁑♫ ¥Ƶ▼ξ֍π∞☺¥♪ π♥ ξ⁂⁑∞α≠⅟Ωπ τ֍¥ ⁂ΩμΩ, □⁑ξμ♥ ƵΩ ֍∞£ξ□∞֍ξα♥α∞⁑♣ π∞≠ΩƵ♣®♫♪ ⁂Ω€♫♪ τ⁑¥□®♫.

£∞ τξ֍ξβξπ ⁂¥⅟♪⁑ ☺Ω≠♥☼ €α∞ ⁂ξ≠Ƶ☺∞ — ƵΩμΩ⁂ƵξΩ ¥ Ωβξ ξ⁑֍∞©ΩƵ¥Ω α ⁂Ω֍Ωμ֍¥⁂⁂ξ-⁂¥ƵΩ± ≠♫©Ω, ֍∞£≠¥α■Ω±⁂⅟ Ƶ∞ α⁂♪ τ֍ξΩ£©♫♪ □∞⁂⁑♣. ¥ €♫Ω⁑ αΩ⁑Ω֍, τξ-αΩ⁂ΩƵƵΩπ♫ ⁑Ωτ≠♥± ¥ ⁑∞®ξ± ⁂¥≠♣Ƶ♥±, □⁑ξ π♥ ⁂֍∞£♫ ©Ω ξ⁂⁑∞α≠⅟Ωπ τξτ♥⁑®¥ ⁂∞πξ⁂⁑ξ⅟⁑Ω≠♣Ƶξ α♥μ֍∞⁑♣ €∞≠♣ƵΩ±■¥± π∞֍■֍♫⁑ ¥ ֍∞£αξ֍∞□¥α∞Ωπ⁂⅟ ⁑∞®, □⁑ξμ♥ ξƵ €♫≠ Ƶ∞π α ⁂τ¥Ƶ♫.

— ⁂ξ≠ƵΩ□Ƶ♥± αΩ⁑Ω֍, — βξαξ֍¥⁑ ⁑ξƵ¥. ¥ ♠♫֍¥⁂⁂⅟, ®∞® €ξαξ≠♣Ƶ♥± ®ξ⁑.

Π♥ ⁂αξ֍∞□¥α∞Ωπ £∞ ♫βξ≠, Ƶ∞ ♫≠¥☺♫ ∞■π⅟Ƶξ⁂, ∞ ⁑∞π, β≠⅟€¥-®∞, τξ□⁑¥ Ƶ¥®∞®ξβξ αΩ⁑֍∞. ¥ π♥, ®ξƵΩ□Ƶξ, ⁂֍∞£♫ ©Ω α⁂τξπ¥Ƶ∞Ωπ, □⁑ξ €∞αƵ♥π-€∞αƵξ ☼ξ⁑Ω≠¥ τξ®♫֍¥⁑♣. Ω♠Ω €ξ ⁑ξβξ, ®∞® £∞■≠¥ α ≠∞α®♫. ∞ ♫© ⁑ΩτΩ֍♣-⁑ξ ®∞® ☼ξ⁑¥π, ⁂≠ξα ƵΩ⁑.

⁑ξƵ¥ αξ£¥⁂⁂⅟ ⁂ π∞■¥Ƶ®ξ± €≠⅟ Ƶ∞μ¥α®¥ ⁂¥β∞֍Ω⁑ ¥ ⁑֍ΩτΩ⁑Ƶ♥π¥ τ♫⁂⁑♥π¥ β¥≠♣£∞π¥, ∞ ⅟ ⁂≠ξƵ⅟♪⁂♣ αξ®֍♫β, α⁂Ωπ ⁂αξ¥π α¥€ξπ ¥£ξμ֍∞©∞⅟ πξ֍∞≠♣Ƶ♫♪ τξ€€Ω֍©®♫. ¥ ®ξƵΩ□Ƶξ, β≠∞£Ω♪ τξ ⁂⁑ξ֍ξƵ∞π, τξ ⁂⁑∞֍ξ± τ֍¥α♥□®Ω ®∞€֍¥֍♫♪ ξ®֍♫©∞♪♠¥± π¥֍ — ®≠∞☺, ®≠∞☺,

®≠∞☺.

— ⁂π⁑⁑₹¥, — βξαξ₹♪, τ₹¥Ϫ¥π∞⸗ ¥£ ⁑ξϪ¥Ϫ♥☼ ₹♫® ⁂¥β∞₹Ω⁑♫, — ®ξπ♫-⁑ξ ⸗αϪξ ϪΩ €∞≠¥ τξ¥β₹∞⁑♣ α «®≠∞⁂⁂¥®¥».

— €ξ₹¥⁂ξα∞⁑♣ — ¥ ⁑ξ ϪΩ €∞≠¥, — ®¥α∞Ω⁑ ξϪ.

⁑₹ξ⁑♫∞₹ ¥ τ₹∞α€∞ ₹∞⁂□Ω₹□ΩϪ Ϫ∞ ®α∞€₹∞⁑♥, ∞ ατ¥⁂∞⁑♣ α Ϫ¥☼ ⁂ξξ⁑αΩ⁑⁂⁑α♫♪♠¥Ω ☺¥▼₹♥ ϪΩαΩ€ξπ♥± ☼♫€ξ©Ϫ¥® ♫©Ω ϪΩ ♫⁂τΩ≠. ⁑ξ ≠¥ ξμΩ€∞⁑♣ τξ£α∞≠¥, ⁑ξ ≠¥ τ₹ξ⁂⁑ξ €∞≠¥ τξ ♫■∞π £∞ τξ₹□♫ ξμ♠Ω⁂⁑αΩϪϪξβξ ∞⁂ ▼∞≠♣⁑∞.

£∞⁑ξ Ϫ∞π, ⁂□∞⁂⁑≠¥α♥π αΩ≠¥®ξαξ£₹∞⁂⁑Ϫ♥π €♫₹∞®∞π, £∞®ξϪ ϪΩ τ¥⁂∞Ϫ. Ϫ∞⁂ ♫©Ω €∞αϪξ Ϫ¥®⁑ξ ϪΩ £ξαΩ⁑ ξμΩ€∞⁑♣. ¥ τξ ♫■∞π Ϫ∞π ϪΩ ξ□ΩϪ♣-⁑ξ Ϫ∞€∞Ω■♣, €ξ Ϫ¥☼ ⁂τΩ₹α∞ Ω♠Ω τξ€¥ €ξτ₹♥βϪ¥.

Ξτ♣⸗ϪΩα ξ⁑ αϪΩ£∞τϪξ (≠Ω⁑ ⁑₹¥€☺∞⁑♣ Ϫ∞£∞€) Ϫ∞⁂⁑⁑♫τ¥α■Ω± ¥ α⁂Ω Ω♠Ω αξ⁂☼¥⁑¥⁑Ω≠♣ϪΞ± α⁂Ω€ξ£αξ≠ΩϪϪξ⁂⁑¥, ⁂ξ≠ϪΩ□Ϫξβξ αΩ⁑₹∞, ⁑∞μ∞□Ϫξβξ €♥π∞ ¥ ⁑⸗©Ω⁂⁑¥ Ϫ∞μ¥⁑ξβξ ®₹∞⁂®∞π¥ ₹♪®£∞®∞, ⸗ α♥⁑∞⁂®¥α∞♪ ¥£ ⁑ξϪ¥Ϫξβξ ®∞₹π∞Ϫ∞ ®ξ₹ξμ®♫ ⁂ πΩ≠®∞π¥, ⁂∞©♫⁂♣ Ϫ∞ ®ξ₹⁑ξ□®¥ αξ£≠Ω τΩ₹αξ± ®≠Ω⁑®¥, Ϫ∞πΩ₹Ωα∞⸗⁂♣ Ϫ∞τ¥⁂∞⁑♣ ⁑∞π μξ≠♣■♫♪ ☺¥▼₹♫ 1. ⸗₹®ξ-⁂¥Ϫ♪♪, ®∞® ϪΩμξ α ≠♫©∞☼ τξ€ Ϫ∞■¥π¥ Ϫξβ∞π¥, ¥≠¥ ©Ω≠⁑♫♪, ®∞® αΩ⁂Ω≠ξΩ αΩ⁂ΩϪϪΩΩ ⁂ξ≠Ϫ☺Ω, ¥≠¥ £Ω≠ΩϪ♫♪, ®∞® μ♫€♫♠∞⸗, ϪΩα¥€¥π∞⸗ τξ®∞ ≠¥⁂⁑α∞, ¥≠¥ ®₹∞⁂Ϫ♫♪, ®∞® ⁑ξϪ¥Ϫ∞ ⁂⁑∞₹∞⸗ ®♫₹⁑®∞. Ϫξ, α£⸗α α ₹♫®¥ πΩ≠ξ®, ⁑♫⁑ ©Ω £∞μ♥α∞♪ ξ τΩ₹αξϪ∞□∞≠♣Ϫξπ £∞π♥⁂≠Ω ¥ £∞□Ωπ-⁑ξ £∞®₹∞■¥α∞♪ ⁂¥Ϫ¥π α⁂♪ ®≠Ω⁑®♫. ϪΩ ♫€ξα≠Ω⁑αξ₹¥α■¥⁂♣ €ξ⁂⁑¥βϪ♫⁑♥π, α♥⁑₹⸗☼¥α∞♪ ¥£ ®ξ₹ξμ®¥ ξ⁂⁑∞≠♣Ϫ♥Ω πΩ≠®¥ ¥ Ϫ∞□¥Ϫ∞♪ ₹¥⁂ξα∞⁑♣ ₹♥μ. Tξ⁑ξπ♫ □⁑ξ ⁂¥Ϫ⸗⸗ ®≠Ω⁑®∞ — ♦⁑ξ, ®ξϪΩ□Ϫξ ©Ω, πξ₹Ω. ⁂♫€⸗ τξ ⸗₹®ξ± ξ®₹∞⁂®Ω ₹♥μ, ®₹∞⁂ϪξΩ. Ϫ∞τ₹¥πΩ₹. Aτ₹ξ□Ωπ, ϪΩ⁂®ξ≠♣®ξ π¥Ϫ♫⁑ ⁂τ♫⁂⁑⸗ ₹♥μ♥ πξ¥ τ₹¥Ϫ¥π∞♪⁑ ξ□Ω₹⁑∞Ϫ¥⸗ ⁂⁑ξ≠♣ τ₹¥□♫€≠¥α♥Ω, □⁑ξ πξ₹Ω ⁑Ωτ₹Ω♣ ⸗αϪξ τ₹¥€Ω⁑⁂⸗ τΩ₹Ω€∞⁑♣ α €∞₹ ¥Ϫξτ≠∞ϪΩ⁑⸗Ϫ∞π. T♫⁂⁑♣ ξϪ¥ ⁂ ♦⁑¥π¥ ₹♥μ∞π¥ €ξβξα∞₹¥α∞♪⁑⁂⸗ ξ ⁑ξαπΩ⁂⁑Ϫξπ ⁂♫♠Ω⁂⁑αξα∞Ϫ¥¥. Tξ⁑ξπ♫ □⁑ξ □Ω≠ξαΩ□Ω⁂⁑αξ α πξΩπ ≠¥☺Ω — τ∞⁂.

— ♫☼ ⁑♥, — βξαξ₹¥⁑ ⁑ξϪ¥.

ΞϪ ♫©Ω α♥μ₹ξ⁂¥≠ €ξ®♫₹ΩϪϪ♫♪ ⁂¥β∞₹Ω⁑♫ ¥ ₹αΩ⁑⁂⸗ α μξ±.

Ωπ♫ ⁑ξ≠♣®ξ τξαξ€ €∞±.

A⁑ξ₹♫♪ ®≠Ω⁑®♫ ⁑ξϪ¥ ♫αΩ₹ΩϪϪξ ■⁑₹¥☼♫Ω⁑ £Ω≠ΩϪ♥π ¥ ⁂¥Ϫ¥π, ¥ πϪΩ £∞₹∞ϪΩΩ ⸗⁂Ϫξ, □⁑ξ ♦⁑ξ μ♫€Ω⁑ AΩϪΩ☺¥⸗, Ϫ∞ ®ξ⁑ξ₹±ξ ξϪ ⁂ξαΩ₹■ΩϪϪξ τξπΩ■∞Ϫ, αξ⁑ ¥ ₹∞£Ϫξ☺αΩ⁑Ϫ♥Ω €ξπ∞ τξ€Ϫ¥π∞♪⁑⁂⸗ ¥£ αξ€♥, Ϫξ απΩ⁂⁑ξ βξϪ€ξ≠ ¥ πξ⁑ξ₹ϪΩ♥☼ ≠ξ€ξ® τΩ±£∞© αϪΩ£∞τϪξ £∞τξ≠Ϫ⸗Ω⁑⁂⸗ ®₹♥≠∞⁑♥π¥ ⁂♫♠Ω⁂⁑α∞π¥, τξ☼ξ©¥π¥ ξ€Ϫξα₹ΩπΩϪϪξ Ϫ∞ ≠♪€Ω± ¥ Ϫ∞ ≠¥⁂.

— Π∞⁑Ω₹♣ μξ©♣⸗, ♦⁑ξ ®⁑ξ ⁑∞®¥Ω? — ¥£♫π≠ΩϪϪξ ⁂τ₹∞■¥α∞♪ ⸗.

⁑ξϪ¥ ⁂πΩΩ⁑⁂⸗:

— TξϪ⸗⁑¥⸗ ϪΩ ¥πΩ♪. ⁂∞π¥ τ₹¥■≠¥ ¥ £∞☼ξ⁑Ω≠¥ μ♥⁑♣. ΠξΩ €Ω≠ξ π∞≠ΩϪ♣®ξΩ.

— ≠∞€Ϫξ, τ♫⁂⁑♣ ⁑ξβ€∞ πξ¥ ₹♥μ♥ ©¥α♫⁑ α ¥☼ αξ€Ω, — βξαξ₹♪ ⸗. — ΞϪ¥, τξ-πξΩπ♫, €₹♫β €₹♫β♫ τξ€☼ξ€⸗⁑.

— Aτξ≠ϪΩ, — ⁂ξβ≠∞■∞Ω⁑⁂⸗ ⁑ξϪ¥, τΩ₹Ω⁂⁑∞α≠⸗⸗ ®ξ₹ξμ®♫ ⁂ πΩ≠®∞π¥ ⁑∞®, □⁑ξμ♥ πϪΩ ⁑ξ©Ω μ♥≠ξ ♫€ξμϪξ ¥☼ μ₹∞⁑♣.

⁑֍Ω⁑♣♪ ¥ □Ω⁑αΩ֍⁑♫♪ ®≠Ω⁑®¥ π♥ ֍∞£֍¥⁂ξα♥α∞Ωπ ξ€Ӿξα֍ΩπΩӾӾξ, πξ©Ӿξ ⁂®∞£∞⁑♣ Ӿ∞τΩ֍ΩβξӾ®¥. ⁑ξӾ¥, ®ξӾΩ□Ӿξ, α♥☼ξ€¥⁑ τξμΩ€¥⁑Ω≠Ωπ — α⁂Ω-⁑∞®¥ τ֍ξ▼Ω⁂⁂¥ξӾ∞≠. Tξ€Ӿ¥π∞Ω⁑⁂⅟, ֍∞£β¥μ∞Ω⁑ ⁂τ¥Ӿ♫, τξ⁑⅟β¥α∞Ω⁑⁂⅟, ⁂ ⅟αӾ♥π ♫€ξαξ≠♣⁂⁑α¥Ωπ ֍∞£β≠⅟€♥α∞Ω⁑ ֍Ω£♫≠♣⁑∞⁑.

— ♫☼ ⁑♥! ∞ ♫ ⁑Ωμ⅟ ♦⁑ξ □⁑ξ? — ⁂τ֍∞■¥α∞Ω⁑ ξӾ.

— Ӿ∞αΩ֍ӾξΩ, ®∞֍⁑∞ βξ֍ξ€∞, — ӾΩ♫αΩ֍ΩӾӾξ βξαξ֍♪ ⅟, ξ⁑®≠∞€♥α∞⅟ α ⁂⁑ξ֍ξӾ♫ ▼¥ξ≠Ω⁑ξα♥± πΩ≠ξ®. — Ӿ♫ ⁑ξ□Ӿξ, ®∞֍⁑∞. ⁑∞®∞⅟, £Ӿ∞Ω■♣, ⁂☼Ωπ∞ π∞֍■֍♫⁑ξα €≠⅟ ⁑♫֍¥⁂⁑ξα. ΩΩ ®∞©€♥± €ΩӾ♣ ֍¥⁂♫♪⁑ Ӿ∞ βξ֍ξ€⁂®ξ± ⁂⁑ΩӾΩ. ∞ Ӿξ□♣♪ ¥€Ω⁑ €ξ©€♣ ¥ ⁂π♥α∞Ω⁑ ֍¥⁂♫Ӿξ®. Tξ♦⁑ξπ♫ τξ ♫⁑֍∞π τ֍¥☼ξ€¥⁑ €Ω©♫֍Ӿ♥± ☼♫€ξ©Ӿ¥® ¥ ֍¥⁂♫Ω⁑ Ӿξα♫♪ ®∞֍⁑♫. ΞӾ, ®ξӾΩ□Ӿξ, ӾΩ ξ□ΩӾ♣-⁑ξ τξπӾ¥⁑, □⁑ξ μ♥≠ξ Ӿ∞ α□Ω֍∞■ӾΩπ ֍¥⁂♫Ӿ®Ω, €∞ ¥ ӾΩ ⁂⁑∞֍∞Ω⁑⁂⅟ α⁂τξπӾ¥⁑♣, ∞ τ֍ξ⁂⁑ξ □Ω֍⁑¥⁑ ®∞® μξβ Ӿ∞ €♫■♫ τξ≠ξ©¥⁑. Ӿξ ⁑♫֍¥⁂⁑♥ α⁂Ω ֍∞αӾξ πξβ♫⁑ Ω♪ τξ≠♣£ξα∞⁑♣⁂⁑: τξ®∞ ☼♫€ξ©Ӿ¥® ֍¥⁂♫Ω⁑ Ӿξα♫♪ ®∞֍⁑♫, βξ֍ξ€ πΩӾ⅟Ω⁑⁂⅟ α τξ≠Ӿξπ ⁂ξξ⁑αΩ⁑⁂⁑α¥¥ ⁂ ӾΩ±.

— ⁑ξβ€∞ ☼♫€ξ©Ӿ¥®ξα €ξ≠©Ӿξ μ♥⁑♣ €αξΩ, — βξαξ֍¥⁑ ⁑ξӾ¥. — Aξ-τΩ֍α♥☼, ӾΩ≠♣£⅟ □Ω≠ξαΩ®♫ ֍∞μξ⁑∞⁑♣ μΩ£ α♥☼ξ€Ӿ♥☼. ∞ αξ-α⁑ξ֍♥☼, ⁑∞® Ω♠Ω μξ≠♣■Ω τΩ֍ΩπΩӾ ¥ τ♫⁑∞Ӿ¥☺♥. ¥ α⁂Ω €ξαξ≠♣Ӿ♥.

Ωβξ ®∞֍⁑¥Ӿ®∞ α □Ω⁑αΩ֍⁑ξ± ®≠Ω⁑®Ω τξ≠Ӿξ⁂⁑♣♪ ⁂ξξ⁑αΩ⁑⁂⁑α♫Ω⁑ ♦⁑ξπ♫ ♫⁑αΩ֍©€ΩӾ¥♪. Ӿ∞ ӾΩ± €α∞ □֍Ω£α♥□∞±Ӿξ €ξαξ≠♣Ӿ♥☼ ®֍♥≠∞⁑♥☼ □Ω≠ξαΩ®∞-≠¥⁂∞, ӾΩπӾξβξ — Ӿ∞⁂®ξ≠♣®ξ ♦⁑ξ αξ£πξ©Ӿξ ⁂ ¥☼ ≠¥⁂♣π¥ πξ֍€∞π¥ — τξ☼ξ©¥Ω Ӿ∞ Ӿ∞⁂, τ∞֍⅟⁑ Ӿ∞€ ⁂αξ¥π βξ֍ξ€ξπ-ξ£Ω֍ξπ ⁂ μξ≠♣■¥π¥ ®֍∞⁂Ӿ♥π¥ ®֍♫©®∞π¥ α ֍♫®∞☼.

— ΞӾ¥ Ӿ∞αΩ֍Ӿ⅟®∞ τ♣♪⁑ ®ξ▼Ω, — βξαξ֍♪ ⅟.

— ®ξӾΩ□Ӿξ. ®∞® μ♥ ⁑♥ Ӿ¥ α♥β≠⅟€Ω≠ ¥ β€Ω μ♥ Ӿ¥ ©¥≠, ∞ μΩ£ ®ξ▼Ω Ӿ¥®∞® ӾΩ≠♣£⅟.

Π♥ μ♥ ⁑ξ©Ω πξβ≠¥ ⁂Ω±□∞⁂ ξ⁑τ֍∞α¥⁑♣⁂⁑⅟ τ¥⁑♣ ®ξ▼Ω — ⁂ξμ⁂⁑αΩӾӾξ, π♥ ¥ ⁂ξμ¥֍∞≠¥⁂♣, — Ӿξ απΩ⁂⁑ξ ♦⁑ξβξ ⁑ξӾ¥ Ӿ∞□¥Ӿ∞Ω⁑ ⁂αξ֍∞□¥α∞⁑♣ ξ□Ω֍Ω€Ӿ♫♪ ⁂¥β∞֍Ω⁑♫, ∞ ⅟ — ֍∞£֍¥⁂ξα♥α∞⁑♣ τ⅟⁑♫♪ τξ ⁂□Ω⁑♫ ®≠Ω⁑®♫. ⁂ξαΩ֍■ΩӾӾξ ӾΩαξ£πξ©Ӿξ ξ⁂⁑∞Ӿξα¥⁑♣⁂⁑⅟.

— □⁑ξ ♦⁑ξ? — ⁂τ֍∞■¥α∞Ω⁑ ⁑ξӾ¥. — Ξ□ΩӾ♣ ®֍∞⁂¥αξ, Ӿξ Ӿ¥ □Ω֍⁑∞ ӾΩ τξӾ⅟⁑Ӿξ.

— Ӿ∞αΩ֍ӾξΩ, — βξαξ֍♪ ⅟, — ♦⁑ξ ⁑∞®∞⅟ ®Ӿ¥β∞. AΩ֍ӾΩΩ, ⁑ξ, □⁑ξ ♫ Ӿ¥☼ απΩ⁂⁑ξ ®Ӿ¥β. ®ξβ€∞ τξ⁂⁑ξ⅟ӾΩξ ≠Ω⁑∞Ω■♣ Ӿ∞€ αξ€ξ±, ξ□ΩӾ♣ £€ξ֍ξαξ, Ω⁂≠¥ α ӾΩ± ξ⁑֍∞©∞♪⁑⁂⁑⅟ α⁂⅟®¥Ω ¥Ӿ⁑Ω֍Ω⁂Ӿ♥Ω ■⁑♫®¥. Ӿ∞τ֍¥πΩ֍, ®Ӿ¥©®¥ ⁂ ®∞֍⁑¥Ӿ®∞π¥, ®ξ⁑ξ֍♥Ω α ⁑∞®ξ± ӾΩτ֍ξ⁂⁑ξ± ⁂¥⁑♫∞☺¥¥ ≠♫□■Ω ⁂֍∞£♫ τ¥⁂∞⁑♣ Ӿ∞ ξμ≠∞®∞☼. T֍¥□Ωπ α £Ω֍®∞≠♣Ӿξπ α¥€Ω. □⁑ξμ♥ ξ⁑֍∞©∞≠¥⁂♣ ♫©Ω ®∞® Ӿ∞€ξ.

— ≠∞€Ӿξ, — ®¥α∞Ω⁑ ⁑ξӾ¥. Ξ⁑€∞Ω⁑ πӾΩ ⁂¥β∞֍Ω⁑♫, ξ⁑μ¥֍∞Ω⁑ πΩ≠®¥ ¥, τξ®∞ ⅟ τΩ֍Ωαξ©♫ €♫☼, μ♥⁂⁑֍ξ-μ♥⁂⁑֍ξ ֍¥⁂♫Ω⁑ α ■Ω⁂⁑ξ± ®≠Ω⁑®Ω ≠Ω⁑∞♪♠¥☼ τ¥⁂∞⁑Ω≠Ω±, ⁂⁑∞֍∞⁑Ω≠♣Ӿξ τξ®֍♥α∞♪♠¥☼ ξμ≠∞®∞ τ¥⁂♣πΩӾ∞π¥.

— ∞β∞, ¥πΩӾӾξ ⁑∞® ξӾ¥ ¥ ֍∞μξ⁑∞♪⁑, — ®¥α∞♪ ⅟.

¥ τ֍¥Ӿ¥π∞♪⁂♣ £∞ ⁂Ω€♣π♫♪ ®≠Ω⁑®♫, ∞ ⁑ξӾ¥ €ξ⁂⁑∞Ω⁑⁂⅟ αξ⁂♣π∞⅟.

⅟ ֍¥⁂♫♪ τξ⁑ξ®¥ ֍∞£Ӿξ☺αΩ⁑Ӿξβξ αΩ⁑֍∞ Ӿ∞€ β♫⁂⁑ξ± □Ω֍Ӿξ⁑ξ±

τ֍¥μ֍Ω©Ӿ♥☼ τ≠ξ€ξα♥☼ ⁂∞€ξα, ∞ ⁑ξӾ¥ ®ξ֍τ¥⁑ Ӿ∞€ β≠∞αӾξ± τ≠ξ♠∞€♣♪, β€Ω α♥⁂∞©ΩӾ♥ τξ€αξ€Ӿ♥Ω €Ω֍Ωα♣⅟, Ӿ∞⁂⁑ξ≠♣®ξ α♥⁂ξ®¥Ω, □⁑ξ α ¥☼ τξ€Ӿ⅟α■¥☼⁂⅟ Ӿ∞€ τξαΩ֍☼Ӿξ⁂⁑♣♪ ξ£Ω֍∞ αΩ⁑α⅟☼ πξβ♫⁑ ξ⁑€ξ☼Ӿ♫⁑♣ ♫⁂⁑∞≠♥Ω ≠Ω⁑♫Ӿ♥.

A €Ωα⅟⁑ξ± ®≠Ω⁑®Ω ⅟ ֍¥⁂♫♪ πξ⁂⁑, Ӿξ ӾΩ πΩ©€♫ μΩ֍Ωβ∞π¥, ∞ πΩ©€♫ £Ωπ≠Ω± ¥ ӾΩμξπ. A ⁑ξ□Ӿξ⁂⁑¥ ®∞® ⁂⁑∞֍♥± ≠ξӾ€ξӾ⁂®¥± πξ⁂⁑, ξӾ £∞⁂⁑֍ξΩӾ €ξπ∞π¥, τξ ®֍∞±ӾΩ± πΩ֍Ω Ӿ∞ ξμξ£֍¥πξπ ♫□∞⁂⁑®Ω, ∞ □⁑ξ €Ω≠∞Ω⁑⁂⅟ α♥■Ω, £∞ ξμ≠∞®∞π¥, ⅟ ӾΩ £Ӿ∞♪. ®♫€∞ ♫© πӾΩ.

⁑ξӾ¥ Ω♠Ω ֍¥⁂♫Ω⁑, τξ♦⁑ξπ♫ ⁂¥β∞֍Ω⁑♥ €≠⅟ Ӿ∞⁂ ⁂αξ֍∞□¥α∞♪ ⅟.

£∞®ξӾ□¥α τξ⁂≠Ω€Ӿ♪♪, €Ω⁂⅟⁑♫♪ ®≠Ω⁑®♫, ξӾ μΩ֍Ω⁑ ♫ πΩӾ⅟ ⁂∞πξ®֍♫⁑®♫ ¥, £∞μ♥α τ֍¥®♫֍¥⁑♣, £∞π¥֍∞Ω⁑, ♫⁂⁑∞α¥α■¥⁂♣ α ӾΩμξ. ∞ ⅟ ξ£∞€∞□ΩӾӾξ ֍∞£β≠⅟€♥α∞♪ Ωβξ ®∞֍⁑¥Ӿ®♫. Ӿ∞®ξӾΩ☺ ⁂τ֍∞■¥α∞♪:

— ⁂≠♫■∞±, ∞ □⁑ξ ♦⁑ξ?

— Ӿ∞αΩ֍ӾξΩ, ®∞֍⁑∞, — ♫≠♥μ∞Ω⁑⁂⅟ ⁑ξӾ¥. — Ӿξ ӾΩ βξ֍ξ€∞, ®∞® ♫ ⁑Ωμ⅟ μ♥≠∞. ∞ ®∞® ⁑♫€∞ €ξμ֍∞⁑♣⁂⅟. A ⁂π♥⁂≠Ω ξ⁑⁂♪€∞. Ӿ♫, Ω⁂≠¥ α€֍♫β τ֍¥⁂τ¥□¥⁑. Π∞≠ξ ≠¥ □⁑ξ.

— Ξβξ, — βξαξ֍♪ ⅟, α⁂π∞⁑֍¥α∞⅟⁂♣ α ֍¥⁂♫Ӿξ®. ¥ τξα⁑ξ֍⅟♪: — Ξβξ.

∞ □⁑ξ ⁑♫⁑ Ω♠Ω ⁂®∞©Ω■♣.

Π♥ ⁂¥€¥π τ֍⅟πξ Ӿ∞ μξ֍€♪֍Ω ¥ ®♫֍¥π. Ӿ∞π, τξ τ֍∞α€Ω βξαξ֍⅟, €ξαξ≠♣Ӿξ £⅟μ®ξ, τξ⁑ξπ♫ □⁑ξ Ӿ∞■ τ֍¥⅟⁑Ω≠♣ αΩ⁑Ω֍ ⁂Ӿξα∞ ⁑♫⁑ ®∞® ⁑♫⁑. Tξ®∞ π♥ ֍¥⁂ξα∞≠¥, ξӾ ξ⁑€ξ☼Ӿ♫≠ ¥ ⁑ΩτΩ֍♣ βξ⁑ξα €♫⁑♣ ⁂®ξ≠♣®ξ ♫βξ€Ӿξ.

Ӿ∞π, Ω⁂≠¥ τξ ♫π♫, ⁂≠Ω€ξα∞≠ξ μ♥ ξ⁑ξ֍α∞⁑♣ £∞€Ӿ¥☺♥ ξ⁑ ☼ξ≠ξ€Ӿξβξ ⁑֍ξ⁑♫∞֍∞ ¥ μΩβξπ μΩ©∞⁑♣ α μ≠¥©∞±■♫♪ ®ξ▼Ω±Ӿ♪ ¥≠¥ ⁂֍∞£♫ €ξπξ±. Ӿξ π♥ ⁑∞® ♫⁂⁑∞≠¥, □⁑ξ τξ®∞ πξ©Ωπ ⁑ξ≠♣®ξ ®♫֍¥⁑♣ Ӿ∞ ≠Ω€⅟Ӿξπ ⁂ξ≠ӾΩ□Ӿξπ αΩ⁑֍♫ ¥ μ≠∞©ΩӾӾξ ♫≠♥μ∞⁑♣⁂⅟, β≠∞£Ω⅟ Ӿ∞ τ֍¥□♫€≠¥αξΩ €Ω≠ξ ⁂αξ¥☼ ֍♫®.

¥£ ⁂ξ⁂Ω€ӾΩβξ €αξ֍∞ α♥☼ξ€¥⁑ €Ωαξ□®∞ ≠Ω⁑ ⁂Ωπ¥. ֍♥©∞⅟ €Ωαξ□®∞ α ⁂⁑∞֍ξπ ®֍∞⁂Ӿξπ τ∞≠♣⁑ξ, €ξ⁂⁑∞⁑ξ□Ӿξ τ♫☼≠∞⅟, □⁑ξμ♥ £∞⁂≠♫©¥⁑♣ αξ €αξ֍Ω τ֍ξ£α¥♠Ω «μξπμ∞» ¥≠¥ □⁑ξ-⁑ξ α ⁑∞®ξπ ֍ξ€Ω. ♫ €Ωαξ□®¥ ®ξ⁂∞ €ξ τξ⅟⁂∞, ®֍♫β≠♥Ω £Ω≠ΩӾ♥Ω β≠∞£∞, ♫τ֍⅟π♥± ≠ξμ ¥ ⁑∞®ξ± αξ≠Ωαξ± τξ€μξ֍ξ€ξ®, □⁑ξ ӾΩ ☼ξ⁑Ω≠ξ⁂⁑♣ μ♥ πӾΩ ξ®∞£∞⁑♣⁂⁑⅟ Ӿ∞ πΩ⁂⁑⁑Ω ΩΩ β¥τξ⁑Ω⁑¥□Ω⁂®¥☼ ξμ¥€□¥®ξα. A ≠Ωαξ± ֍♫®Ω ♫ €Ωαξ□®¥ ⁂Ω֍∞⅟ α⅟£∞Ӿ∞⅟ ■∞τ®∞, ®ξ⁑ξ֍♫♪ ξӾ∞ ⁑ξ≠♣®ξ □⁑ξ ⁂Ӿ⅟≠∞ ⁂ ֍∞⁂⁑֍Ωτ∞ӾӾξ± ⁂αξΩ± βξ≠ξα♥, α τ֍∞αξ± — ®֍♫β≠∞⅟ τ≠ξ⁂®∞⅟ μΩ≠∞⅟ ®ξ֍ξμξ□®∞, ®ξ⁑ξ֍♫♪ ατξ≠ӾΩ πξ©Ӿξ ¥⁂τξ≠♣£ξα∞⁑♣ ®∞® μ¥⁑♫. Ӿ∞ ≠¥☺Ω ♫ €Ωαξ□®¥ ®֍♫τӾ♥π¥ μ♫®α∞π¥ Ӿ∞τ¥⁂∞Ӿξ ӾΩ⁂β¥μ∞ΩπξΩ Ӿ∞πΩ֍ΩӾ¥Ω ӾΩπΩ€≠ΩӾӾξ τξ¥β֍∞⁑♣ α «®≠∞⁂⁂¥®¥», ®ξ⁑ξ֍♥Ω ξӾ∞ ⁂∞π∞ ⁑∞® ⁂⁑∞֍∞⁑Ω≠♣Ӿξ □Ω֍⁑¥≠∞ τΩ֍Ω€ ξμΩ€ξπ, □⁑ξμ♥ μ♥≠¥ ⁑ξ≠♣®ξ ΩΩ, □⁑ξμ♥ Ӿ¥®⁑ξ ӾΩ πΩ■∞≠ τ֍♥β∞⁑♣ ¥ ӾΩ ⁂πΩ⅟≠⁂⅟ Ӿ∞€ τ֍ξπ∞☼∞π¥.

♫α¥€Ωα Ӿ∞■¥ ⁂ ⁑ξӾ¥ ֍¥⁂♫Ӿ®¥, €Ωαξ□®∞ ¥£♫π≠ΩӾӾξ £∞π¥֍∞Ω⁑. ⁂Ω®♫Ӿ€ Ӿ∞ τ⅟⁑♣, ӾΩ μξ≠♣■Ω. Tξ⁑ξπ ®≠∞€Ω⁑ μ¥⁑♫ Ӿ∞ τΩ֍α♫♪ ®≠Ω⁑®♫, τ֍⅟πξ Ӿ∞ βξ≠ξα♫ ξ€Ӿξ± ¥£ πξ¥☼ ֍♥μ. ¥ Ӿ∞□¥Ӿ∞Ω⁑ τ֍♥β∞⁑♣.

€Ωαξ□®∞ τ֍♥β∞Ω⁑ ξ□ΩӾ♣ ∞®®♫֍∞⁑Ӿξ. Tξ€ξ≠β♫ ⁂⁑ξ¥⁑ α ®∞©€ξ± ®≠Ω⁑®Ω, τ֍¥πΩ֍⅟⅟⁂♣ ® ⁂≠Ω€♫♪♠Ωπ♫ τ֍♥©®♫. ΞӾ∞ ⁂⁑∞֍∞Ω⁑⁂⅟ —

ƛΩ ⁑ξ τξ αξ£πξ©ƛξ⁂⁑¥ ⁂ξ☼֍∞ƛ¥⁑♣ ®∞֍⁑¥ƛ®¥, ƛΩ ⁑ξ τ֍ξ⁂⁑ξ €ξμ¥⁑♣⁂⇟ ¥€Ω∞≠♣ƛξ± ⁑ξ□ƛξ⁂⁑¥ €α¥©ΩƛΩ¥±. Ω±, τξ☼ξ©Ω, ατξ≠ƛΩ ♫€∞Ω⁑⁂⇟ ¥ ⁑ξ, ¥ €֍♫βξΩ.

€ξμ֍∞α■¥⁂♣ €ξ €Ωα⇟⁑ξ± ®≠Ω⁑®¥, €Ωαξ□®∞ £∞π¥֍∞Ω⁑ ¥ αƛ¥π∞⁑Ω≠♣ƛξ ֍∞£β≠⇟€♥α∞Ω⁑ €Ω⁂⇟⁑♫♪. ƛ∞®ξƛΩ☺, απΩ⁂⁑ξ ⁑ξβξ □⁑ξμ♥ τ֍♥β∞⁑♣, ƛξ⁂®ξπ ☺αΩ⁑∞⁂⁑ξβξ ֍Ω£¥ƛξαξβξ ⁂∞τξβ∞ ξ⁂⁑ξ֍ξ©ƛξ τξ€⁑∞≠®¥α∞Ω⁑ μ¥⁑♫ ® β֍∞ƛ¥☺Ω πΩ©€♫ ®≠Ω⁑®∞π¥.

Aξ⁑ μ¥⁑∞ ♫©Ω τξ€τξ≠£≠∞ ® πΩ≠ξαξ± □Ω֍⁑Ω. ¥ τξ⁑¥☼ξƛ♣®♫ €α¥ƛ♫≠∞⁂♣ €∞≠♣■Ω. Aξ⁑… □Ω֍⁑, €∞ β€Ω ©Ω ξƛ∞?

⁑ξ≠⁂⁑∞⇟ €Ωαξ□®∞ α ®֍∞⁂ƛξπ τ∞≠♣⁑ξ ⁂⁑ξ¥⁑ α €Ωα⇟⁑ξ± ®≠Ω⁑®Ω, ƛ∞ πξΩπ πξ⁂⁑♫ πΩ©€♫ £Ωπ≠Ω± ¥ ƛΩμξπ. ¥ ξ£∞€∞□ΩƛƛΞ ֍∞£β≠⇟€♥α∞Ω⁑ €Ω⁂⇟⁑♫♪, α ®ξ⁑ξ֍ξ± ƛΩ⁑ ƛ¥□Ωβξ, ®֍ξπΩ ⁑ξƛ¥ƛξβξ ֍¥⁂♫ƛ®∞. μΩ≠∞⇟ τ≠ξ⁂®∞⇟ ®ξ֍ξμξ□®∞ ƛ¥®∞® ƛΩ πξβ≠∞ τξ⁑Ω֍⇟⁑♣⁂⇟ ƛ∞ Ωβξ ▼ξƛΩ. ⁑Ωπ ƛΩ πΩƛΩΩ ΩΩ ⁑∞π ƛΩ⁑.

€Ωαξ□®∞ ֍ξƛ⇟Ω⁑ ƛ∞ £Ωπ≠♪ ⁂αξ♪ ⁂Ω֍♫♪ ■∞τ®♫. Π∞■¥ƛ∞≠♣ƛξ ⁂♫Ω⁑ α ֍ξ⁑ ®ξƛ□¥® €≠¥ƛƛξ± ®ξ⁂♥. €♫π∞Ω⁑. ⁂∞€¥⁑⁂⇟ ƛ∞ ®ξ֍⁑ξ□®¥, αƛ¥π∞⁑Ω≠♣ƛξ ⁂πξ⁑֍¥⁑ ƛ∞ ®∞֍⁑¥ƛ®♫. Ξ⁂⁑ξ֍ξ©ƛξ ⁑֍ξβ∞Ω⁑ ΩΩ ֍♫®ξ±. ƛ∞®ξƛΩ☺ τξ€ƛ¥π∞Ω⁑⁂⇟ ¥ €Ω≠∞Ω⁑ ■∞β ατΩ֍Ω€.

Π♥ ⁂ ⁑ξƛ¥ β≠⇟€¥π ƛ∞ ƛΩΩ ®∞® £∞αξ֍ξ©ΩƛƛΩ.

Задание 2. Зашифровать текст любым способом, стойким к частотному анализу.

Таблица 7 – Задания

№ варианта	Текст задания
1	А. Куприн «Гранатовый браслет»
2	А. Куприн «Дознание»
3	А. Куприн «Последний дебют»
4	А. Чехов «Человек в футляре»
5	А. Чехов «Крыжовник»
6	А. Чехов «Палата №6»
7	А. Чехов «Каштанка»
8	М. Булгаков «Морфий»
9	М. Булгаков «Китайская история»
10	М. Булгаков «Вьюга»

2.2.2 Требования к отчету по лабораторной работе

В отчете по лабораторной работе «Методы вскрытия шифров» необходимо представить:

1. основные этапы и результат дешифрование текста методом

частотного анализа;

2. алфавит, алгоритм и результат шифрования для задания 2.

Отчет по лабораторной работе оформляется в соответствии с требованиями, принятыми в КГПИ ФГБОУ ВО «КемГУ», предоставляется преподавателю в электронном виде.

2.1.3 Контрольные вопросы

1. Что такое криптоанализ?
2. Какие виды криптоанализа вы знаете?
3. В чем суть частотного криптоанализа?
4. Как можно улучшить алгоритм шифрования, чтобы он был более стойким против частотного криптоанализа?
5. Есть ли разница в частотах «встречаемости» букв между текстами художественного и научного стиля?

3 Образец тестовых заданий

1.Некоторое слово зашифровано шифром Цезаря с ключом 31. Получилась криптограмма пжйжимл. Расшифруйте слово.

2.Слово камелия зашифровано шифром Цезаря с ключом 29. Запишите полученную криптограмму.

а) жьибзеы;

б) еьивзеъ;

в) жьквзды;

г) зьидзеэ.

3. Шифрование – это:

а) способ, обеспечивающий изменение передаваемого сообщения. Служит для искажения его содержимого;

б) преобразование обычного текста в код;

в) структурирование данных тем или иным способом;

г) преобразование исходного текста в зашифрованный.

4. Соотнесите алгоритмы шифрования и их определения:

1) Алгоритм гаммирования	а) Символы оригинального текста меняются местами по определенному принципу;
2) Алгоритм перестановки	б) Символы оригинального текста заменяются символами, взятыми из одного или нескольких алфавитов;
3) Алгоритм подстановки	в) Символы исходного текста складываются с символами некой случайной последовательности.

5. Программное средство защиты информации

а) криптография;

б) источник бесперебойного питания;

в) резервное копирование;

г) дублирование данных.

6. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод

а) гаммирования;

б) подстановки;

в) перестановки;

г) аналитических преобразований.

7. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод

а) гаммирования;

б) подстановки;

в) перестановки;

г) аналитических преобразований.

8. ... - это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

а) шифр Цезаря;

б) шифрование с помощью квадрата Полибия;

в) шифр Виженера;

г) шифр Плейфейера.

9. Криптография необходима для реализации следующих сервисов безопасности ...

а) контроль конфиденциальности;

б) контроль целостности;

в) контроль доступности;

г) контроль доступа.

10. Метод, в котором исходный текст записывается через отверстия в решетке, которая по мере заполнения поворачивается на 90º. Предварительно текст разбивается на блоки, называется...

а) симметричное шифрование;

б) асимметричное шифрование;

в) метод поворачивающейся решетки;

г) железнодорожная изгородь.

11. Принцип Кирхгофа:

а) секретность ключа определена секретностью открытого сообщения;

б) секретность информации определена скоростью передачи данных;

в) секретность закрытого сообщения определяется секретностью ключа;

г) секретность ключа, информации и закрытого сообщения не определена.

12. Шифром Цезаря зашифровали словосочетание ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. Как выглядит зашифрованное сообщение?

а) ФЩАЪЬШЛВФЪЩЩЛК ОТХЬЭНЯЫЬЯАЙ;

б) РХЬЦШФЗЮРЦХХЗЖ ИМПЦЧЗЩХЦЩЪД;

в) СЦЭЧЩХИЯСЧЦЦИЗ ЙНРЧШИЪЦЧЪЫЕ;

г) СЦЭЧЩХИЯСЧЦЦИЗ ОТХЬЭНЯЫЬЯАЙ.

13. Шифром Виженера было зашифровано сообщение «ЗАЩИТА ИНФОРМАЦИИ», в результате получилось сообщение «АИНЩКИ ЭЮМЧЕЭШЯЭЩ». Ключ для шифрования данного сообщения выглядит так:

а) код;

б) информация;

в) шифр;

г) текст.

14. Асимметричные шифры работают следующим образом:

а) ключ для шифрования знают все, ключ для дешифрования – только получатель;

б) ключ для шифрования знает только один отправитель, ключ для дешифрования знают все;

в) ключ для шифрования знает только один отправитель, ключ для дешифрования знает только один получатель;

г) нет верного ответа.

20. Каким свойствами должен обладать сертификат открытого ключа?

а) каждый пользователь центра сертификации, имеющий доступ к открытому ключу центра, может изменить открытый ключ, включенный в сертификат;

б) каждый пользователь центра сертификации, имеющий доступ к открытому ключу центра, может извлечь открытый ключ, включенный в сертификат;

в) любой пользователь системы может изменить сертификат;

г) нет верного ответа.

4 Рекомендуемая литература

Основная учебная литература

1. Внуков, А.А. Защита информации : учебное пособие для вузов / А.А. Внуков – МОСКВА : Изд-во Юрайт, 2023. – 161 с. – ISBN 978-5-534-07248-8. – URL: https://urait.ru/viewer/zaschita-informacii-512268#page/2. - (дата обращения: 12.12.2022). – Текст : электронный.

Дополнительная литература

1. Лось, А.Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. – Москва : Издательство Юрайт, 2023. – 473 с. – ISBN 978-5-534-12474-3. – URL: https://urait.ru/book/kriptograficheskie-metody-zaschity-informacii-dlya-izuchayuschih-kompyuternuyu-bezopasnost-511138. - (дата обращения: 12.12.2022). – Текст : электронный.

2. VisualStudio : сайт. – 2020 - . - URL: https://visualstudio.microsoft.com/ru/(дата обращения: 12.12.2022). – Текст : электронный.

3. IntelliJIDEA : сайт. – 2000 - . - URL: https://www.jetbrains.com/idea/(дата обращения: 12.12.2022). – Текст : электронный.

Литература для оформления отчетов

1. Правила оформления учебных работ студентов : учебно-методическое пособие / И.А. Жибинова, А.Е. Аракелян, О.В. Соколова, Ю.Н. Соина-Кутищева. – Новокузнецк : НФИ КемГУ, 2018. – 124 с. – Текст : непосредственный.

2. ГОСТ 19.701-90 (ИСО 5807-85) Единая система программной документации (ЕСПД). Схемы алгоритмов, программ, данных и систем. Обозначения условные и правила выполнения : межгосударственный стандарт : издание официальное : введен впервые : дата введения 1992-01-01 / Москва Стандартинформ, 2010 – 158 с. – Текст: непосредственный.

Современные профессиональные базы данных и справочные системы

CITForum.ru :on-line библиотека свободно доступных материалов по информационным технологиям на русском языке : сайт.– 2001 – URL: http://citforum.ru (дата обращения: 12.12.2022). – Текст: электронный.

eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 - . – URL: http://www.elibrary.ru (дата обращения: 12.12.2022). – Режим доступа: для зарегистрир. пользлвателей. – Текст: электронный.

Единое окно доступа к образовательным ресурсам : сайт. – Москва, 2005 - . – URL: http://window.edu.ru/ (дата обращения: 12.12.2022). –Текст: электронный.