

Российский университет транспорта (МИИТ)

Институт транспортной техники и систем управления

Кафедра «Управление и защита информации»

Отчет

по практическому заданию

по теме «Разработка моноалфавитного шифра замены»

по дисциплине «Криптографические методы защиты информации»

Выполнил:

Студент группы ТКИ-342

Дроздов А.Д.

Проверил:

Доцент кафедры УиЗи, к.т.н., с.н.с.

Михалевич И.Ф.

Оглавление

Задание	3
Исходные данные	3
1. Теоретические сведения о шифре	4
1.1. Основные определения	5
1.2. Составные элементы шифра	5
1.3. Мощность алфавита (в общем случае)	5
1.4. Запись общего алгоритма шифрования	7
1.5. Моноалфавитный шифр	7
1.6. Шифра Цезаря	7
2. Практическая часть	8
2.1. Зашифровка сообщения инициатора.....	8
2.2. Расшифровка сообщения инициатора.....	9
2.3. Зашифровка сообщения ответчика.....	11
2.4. Расшифровка сообщения ответчика.....	14
3. Анализ частотности текста.....	16
3.1. Таблица и график частотности исходного алфавита.....	17
3.2. Таблица и график частотности исходного текста.....	18
3.3. Таблица и график частотности зашифрованного текста.....	20
4. Заключение	23

Задание

Разработать моноалфавитный шифр, таблицы шифрования / расшифрования (для варианта шифра). Подготовить сообщение путем СЛИЯНИЯ сообщений инициатора и ответчика. Зашифровать и расшифровать сообщение. Провести анализ слабостей шифра (привести таблицы и гистограммы частотности символов исходного алфавита и сообщения, зашифрованного разработанным шифром, описать слабости шифра). Оформить отчет.

Исходные данные

1. Алфавит, выбранный студентом на основе алфавита русского языка.
2. Ключ – номер студента в группе.
3. Шифр – алфавит со сдвигом вправо по ключу.
4. Передаваемые сообщения: сообщение инициатора, сообщение ответчика.

В первую очередь необходимо обозначить исходный и зашифрованный алфавит, а также ключ 4, что было сделано на рис. 1.

Исходный алфавит		Ключ		Зашифрованный алфавит	
1	.	4		1	2
2	.			2	3
3				3	4
4	1			4	5
5	2			5	6
6	3			6	7
7	4			7	8
8	5			8	9
9	6			9	0
10	7			10	А
11	8			11	Б
12	9			12	В
13	0			13	Г
14	А			14	Д
15	Б			15	Е
16	В			16	Ё
17	Г			17	Ж
18	Д			18	З
19	Е			19	И
20	Ё			20	Й
21	Ж			21	К
22	З			22	Л
23	И			23	М
24	Й			24	Н
25	К			25	О
26	Л			26	П
27	М			27	Р
28	Н			28	С
29	О			29	Т
30	П			30	У
31	Р			31	Ф
32	С			32	Х
33	Т			33	Ц
34	У			34	Ч
35	Ф			35	Ш
36	Х			36	Щ
37	Ц			37	Ъ
38	Ч			38	Ы
39	Ш			39	Ь
40	Щ			40	Э
41	Ъ			41	Ю
42	Ы			42	Я
43	Ь			43	.
44	Э			44	.
45	Ю			45	
46	Я			46	1

Рисунок 1 – Исходный и зашифрованный алфавит с ключом
Далее указываем исходные сообщения инициатора и ответчика – рис.2

Сообщение инициатора	Уважаемый Игорь Феодосьевич, сообщаю Вам, что практическое задание номер четыре было полностью выполнено, Дроздов Антон Дмитриевич 03.12.2002
Длина сообщения	141
Сообщение ответчика	Уважаемый Антон Дмитриевич, я безмерно рад нашему сотрудничеству. Надеюсь на его дальнейшее успешное и взаимовыгодное развитие. С уважением Игорь Феодосьевич.
Длина сообщения	159

Рисунок 2 – Сообщение инициатора и ответчика

1. Теоретические сведения о шифре

1.1. Основные определения

Шифр – система заранее оговоренных обратимых преобразований защищаемой информации (текста, изображений, аудио, видео и др.) с помощью ключа.

Ключ – переменный параметр для обратимых преобразований защищаемой информации (данных).

Ключ – минимальная информация, необходимая для обратимого преобразования защищаемой информации (шифрования и расшифрования, формирования и проверки контрольных сумм и др.).

Алфавит – это набор уникальных символов для записи шифрованных сообщений (буквы, цифры, знаки препинания, специальные символы и др.).

Мощность алфавита – полное число символов алфавита.

Шифр (общий случай) – множество обратимых функций отображения E_k множества открытых сообщений M на множество криптограмм C , зависящих от выбранного ключа шифрования k из множества K_E и соответствующие им обратные функции расшифрования D_k , зависящие от выбранного ключа расшифрования из множества K_D , отображающие множество криптограмм C на множество открытых сообщений M .

1.2. Составные элементы шифра

К составным элементам шифра относится алфавит, алгоритмы обратимых преобразований исходного сообщения в криптограммы и обратного преобразования криптограмм в открытое сообщение (зашифрования и расшифрования), а также множество ключей.

1.3. Мощность алфавита (в общем случае)

Для русского языка мощность алфавита – 33, а для английского – 26.

Алфавит может дополнительно включать цифры, знаки препинания, специальные символы.

1.4. Запись общего алгоритма шифрования

$$\begin{aligned} E_k, k \in K_{ED}: M &\rightarrow C, \\ D_k, k \in K_{ED}: C &\rightarrow M, \\ \forall k \in K_E \exists k \in K_D, \\ \forall m \in M : E_k(m) &= c, \\ \forall c \in C: D_k(c) &= m \end{aligned} \tag{1}$$

1.5. Моноалфавитный шифр

$$\begin{aligned} C_i &= M_i + K \bmod n \\ M_i &= C_i - K \bmod n \end{aligned} \tag{2}$$

K – ключ, $0 < k \leq n$

n – мощность алфавита

M_i – символ на i -й позиции исходного сообщения, $i \in N$

C_i – символ на i -й позиции криптограммы (замененный символ M на i -й позиции сообщения по ключу K)

1.6. Шифра Цезаря

Шифра Цезаря – метод создания простого моноалфавитного шифра на основе ключа с постоянным параметром сдвига на K символов.

$$\begin{aligned} E: C_i &= M_i + K \bmod n \\ D: M_i &= C_i - K \bmod n \end{aligned} \tag{3}$$

i – позиция символа в алфавите шифра

M_i, C_i – исходный и зашифрованные символы

K – параметр сдвига (ключа)

n – мощность алфавита шифра

2. Практическая часть

2.1. Зашифровка сообщения инициатора

На рис.3 – рис.5 представлена зашифровка сообщения инициатора.

С	У	Е	Р	Г	Н	Т	Д	К	Л	М	Н	О	Р
1	У		1	Ч	Ч								
2	В		2	Е	ЧЕ								
3	А		3	Д	ЧЕД								
4	Ж		4	К	ЧЕДК								
5	А		5	Д	ЧЕДКД								
6	Е		6	И	ЧЕДКДИ								
7	М		7	Р	ЧЕДКДИР								
8	Ы		8	Я	ЧЕДКДИРЯ								
9	И		9	Н	ЧЕДКДИРЯН								
10			10	4	ЧЕДКДИРЯН4								
11	И		11	М	ЧЕДКДИРЯН4М								
12	Г		12	Ж	ЧЕДКДИРЯН4МЖ								
13	О		13	Т	ЧЕДКДИРЯН4МСКТ								
14	Р		14	Ф	ЧЕДКДИРЯН4МСКТФ								
15	Б		15	.	ЧЕДКДИРЯН4МСКТФ.								
16			16	4	ЧЕДКДИРЯН4МСКТФ.4								
17	Ф		17	Ш	ЧЕДКДИРЯН4МСКТФ.4Ш								
18	Е		18	И	ЧЕДКДИРЯН4МСКТФ.4ШИ								
19	О		19	Т	ЧЕДКДИРЯН4МСКТФ.4ШИТ								
20	Д		20	З	ЧЕДКДИРЯН4МСКТФ.4ШИТЗ								
21	О		21	Т	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТ								
22	С		22	Х	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ								
23	Б		23	.	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.								
24	Е		24	И	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.И								
25	В		25	Е	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕ								
26	И		26	М	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМ								
27	Ч		27	Ы	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ								
28	.		28	2	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ2								
29			29	4	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24								
30	С		30	Х	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24Х								
31	О		31	Т	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТ								
32	О		32	Т	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТ								
33	Б		33	Е	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕ								
34	Ш		34	Э	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭ								
35	А		35	Д	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД								
36	Ю		36		ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД								
37			37	4	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4								
38	В		38	Е	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4Е								
39	А		39	Д	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕД								
40	М		40	Р	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР								
41	.		41	2	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР2								
42			42	4	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР24								
43	Ч		43	Ы	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР24Ы								
44	Т		44	Ц	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР24ЫЦ								
45	О		45	Т	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР24ЫЦТ								
46			46	4	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР24ЫЦТ4								
47	П		47	У	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР24ЫЦТ4У								
48	Р		48	Ф	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР24ЫЦТ4УФ								
49	А		49	Д	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР24ЫЦТ4УФД								
50	К		50	О	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР24ЫЦТ4УФДО								
51	Т		51	Ц	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР24ЫЦТ4УФДОЦ								
52	И		52	М	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР24ЫЦТ4УФДОЦМ								
53	Ч		53	Ы	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР24ЫЦТ4УФДОЦМЫ								
54	Е		54	И	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР24ЫЦТ4УФДОЦМЫИ								
55	С		55	Х	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР24ЫЦТ4УФДОЦМЫИХ								
56	К		56	О	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР24ЫЦТ4УФДОЦМЫИХО								
57	О		57	Т	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР24ЫЦТ4УФДОЦМЫИХОТ								
58	Е		58	И	ЧЕДКДИРЯН4МСКТФ.4ШИТЗТХ.ИЕМЫ24ХТТЕЭД4ЕДР24ЫЦТ4УФДОЦМЫИХОТИ								

Рисунок 3 – Зашифровка сообщения (1 часть)

Рисунок 8 – Расшифровка сообщения (2 часть)

Рисунок 9 – Расшифровка сообщения (3 часть)

Рисунок 10 – Результат расшифрования

На рис.11 – рис.14 содержится зашифровка сообщения ответчика.

1	У		1	Ч	Ч						
2	В		2	Ё	ЧЁ						
3	А		3	Д	ЧЁД						
4	Ж		4	К	ЧЁДК						
5	А		5	Д	ЧЁДКД						
6	Е		6	И	ЧЁДКДИ						
7	М		7	Р	ЧЁДКДИР						
8	Ы		8	Я	ЧЁДКДИРЯ						
9	Й		9	Н	ЧЁДКДИРЯН						
10			10	4	ЧЁДКДИРЯН4						
11	А		11	Д	ЧЁДКДИРЯН4Д						
12	Н		12	С	ЧЁДКДИРЯН4ДС						
13	Т		13	Ц	ЧЁДКДИРЯН4ДСЦ						
14	О		14	Т	ЧЁДКДИРЯН4ДСЦТ						
15	Н		15	С	ЧЁДКДИРЯН4ДСЦТС						
16			16	4	ЧЁДКДИРЯН4ДСЦТС4						
17	Д		17	3	ЧЁДКДИРЯН4ДСЦТС43						
18	М		18	Р	ЧЁДКДИРЯН4ДСЦТС43Р						
19	И		19	М	ЧЁДКДИРЯН4ДСЦТС43РМ						
20	Т		20	Ц	ЧЁДКДИРЯН4ДСЦТС43РМЦ						
21	Р		21	Ф	ЧЁДКДИРЯН4ДСЦТС43РМЦФ						
22	И		22	М	ЧЁДКДИРЯН4ДСЦТС43РМЦФМ						
23	Е		23	И	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИ						
24	В		24	Ё	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁ						
25	И		25	М	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМ						
26	Ч		26	Ы	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ						
27	,		27	2	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ2						
28			28	4	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ24						
29	Я		29	1	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ241						
30			30	4	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ2414						
31	Б		31	Е	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ2414Е						
32	Е		32	И	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ2414ЕИ						
33	3		33	Л	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ2414ЕИЛ						
34	М		34	Р	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ2414ЕИЛР						
35	Е		35	И	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ2414ЕИЛРИ						
36	Р		36	Ф	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ2414ЕИЛРИФ						
37	Н		37	С	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ2414ЕИЛРИФС						
38	О		38	Т	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ2414ЕИЛРИФСТ						
39			39	4	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ2414ЕИЛРИФСТ4						
40	Р		40	Ф	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ2414ЕИЛРИФСТ4Ф						
41	А		41	Д	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ2414ЕИЛРИФСТ4ФД						
42	Д		42	3	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ2414ЕИЛРИФСТ4ФД3						
43			43	4	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ2414ЕИЛРИФСТ4ФД34						
44	Н		44	С	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ2414ЕИЛРИФСТ4ФД34С						
45	А		45	Д	ЧЁДКДИРЯН4ДСЦТС43РМЦФМИЁМЫ2414ЕИЛРИФСТ4ФД34СД						

Рисунок 11 – Зашифровка сообщения (1 часть)

46	Ш	46	Б	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБ
47	Е	47	И	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИ
48	М	48	Р	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИР
49	У	49	Ч	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ
50		50	4	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4
51	С	51	Х	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4Х
52	О	52	Т	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТ
53	Т	53	Ц	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦ
54	Р	54	Ф	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФ
55	У	55	Ч	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЧ
56	Д	56	З	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗ
57	Н	57	С	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗС
58	И	58	М	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМ
59	Ч	59	Ы	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫ
60	Е	60	И	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫИ
61	С	61	Х	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХ
62	Т	62	Ц	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЦ
63	В	63	Е	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕ
64	У	64	Ч	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ
65	+	65	2	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ2
66		66	4	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24
67	Н	67	С	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24С
68	А	68	Д	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СД
69	Д	69	3	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СД3
70	Е	70	И	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ
71	Ю	71		ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ
72	С	72	Х	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ Х
73	Ъ	73		ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ Х,
74	+	74	4	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ Х,4
75	Н	75	С	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ Х,4С
76	А	76	Д	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ Х,4СД
77		77	4	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ Х,4СД4
78	Е	78	И	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ Х,4СД4И
79	Г	79	Ж	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ Х,4СД4ИЖ
80	О	80	Т	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ Х,4СД4ИЖТ
81		81	4	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ Х,4СД4ИЖТ4
82	Д	82	3	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ Х,4СД4ИЖТ43
83	А	83	Д	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ Х,4СД4ИЖТ43Д
84	Л	84	П	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ Х,4СД4ИЖТ43ДП
85	Ъ	85		ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ Х,4СД4ИЖТ43ДП,
86	Н	86	С	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ Х,4СД4ИЖТ43ДП,С
87	Е	87	И	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ Х,4СД4ИЖТ43ДП,СИ
88	Й	88	Н	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФСТ4ФДЗ3СДБИРЧ4ХТЦФЗСМЫХЕЧ24СДЗИ Х,4СД4ИЖТ43ДП,СИН
89	Ш	89	И	ЧЕДКДПРЯН4ДСЦТС4ЗРМЩФМИЕМЫ2414ЕИЛРИФС

Рисунок 12 – Зашифровка сообщения (2 часть)

91	E		91	H	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4
92			92	I	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4
93	Y		93	C	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CH
94	S		94	X	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CH
95	P		95	U	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CH
96			96	H	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CH
97	Ш		97	B	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYB
98	N		98	S	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBS
99	O		99	T	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBST
100	E		100	I	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBST
101			101	M	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTM
102			102	A	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTM4
103			103	4	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4
104	V		104	E	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4
105			105	F	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4F
106	A		106	L	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FL
107	I		107	M	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLM
108	M		108	P	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLMP
109	O		109	T	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLMPT
110			110	R	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLMPTRE
111	Ы		111	Я	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLMPTYA
112	G		112	J	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLMPTREJ
113	O		113	T	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLMPTREJT
114	D		114	Z	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLMPTREJTZ
115			115	3	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLMPTREJT3T
116	O		116	T	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLMPTREJT3ST
117	E		117	I	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLMPTREJT3ITI
118			118	4	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLMPTREJT3ITIA4
119	F		119	B	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLMPTREJT3ITIB
120	A		120	L	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLMPTREJT3ITIAL
121	3		121	L	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLMPTREJT3ITIAL4L
122	V		122	E	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLMPTREJT3ITIAL4LE
123	I		123	M	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLMPTREJT3ITIAL4LEM
124			124	P	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLMPTREJT3ITIAL4LEMP
125	I		125	M	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JHKT43ZPL SINBHY4CHUYBSTIAM4FLMPTREJT3ITIAL4LEMDM
126	E		126	H	ЧЕЛДРЯНАДСИТ03RPM0F0ME6BY24IENIPRF0T44D3ACSDMR4XTU0F03CMBWDXE2C4SIZI X ASC4JH

Рисунок 13 – Зашифровка сообщения (3 часть)

136	Е		136	И	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
137	Н		137	С	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
138	И		138	М	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
139	Е		139	И	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
140	М		140	Р	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
141			141	4	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
142	И		142	М	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
143	Г		143	Ж	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
144	О		144	Т	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
145	Р		145	Ф	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
146	Б		146		ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
147			147	4	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
148	Ф		148	Ш	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
149	Е		149	И	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
150	О		150	Т	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
151	Д		151	З	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
152	О		152	Т	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
153	С		153	Х	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
154	Б		154		ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
155	Е		155	И	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
156	В		156	Е	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
157	И		157	М	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
158	Ч		158	Ы	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			
159	.		159	3	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС			

Рисунок 14 – Зашифровка сообщения (4 часть)

А результат шифрования – это рис.15.

Сообщение отклика	УВАЖАЕМО! АНТОН АЛБИТРИВич, В РЕЗЕРВНО РАД НАШЕЛУ СОТРУДНИЧЕСТВУ, НАЖЕКОС НА ЕГО ДАЛЬШЕШЕ УСПЕШНОЕ И ВЗАИМОВОЗНОСНОЕ РАЗВИТИЕ. С УВАЖЕНИЕМ ИГОРЬ ФЕОДОСЬЕНЧ	Длина сообщения	159
Зашифрованное сообщение отклика	ЧЕДКДИРЯНАДЦТТС43РМЦМФМЕМЫ2414ЕИПРИФСТ4ФД34СДБИРЧ4ХТЦ4Ф3СМЫОЩЕЧ24СДЗИ Х4СД4ИКТ43П.СИНЫМИ4ЧХУИСТН4М4ЕЛДПРТЕЯКТЗСТИН4ФДЛЕМДМД1344Х4ЧЕДЛИС	Длина сообщения	159

Рисунок 15 – Результат шифрования

2.4. Расшифровка сообщения ответчика

Следующий этап – это расшифровка, представленная на рис.16 – рис.18.

1	Ч		1	У	У										
2	Е		2	В	УВ										
3	Д		3	А	УВА										
4	К		4	Ж	УВАЖ										
5	Д		5	А	УВАЖА										
6	И		6	Е	УВАЖАЕ										
7	Р		7	М	УВАЖАЕМ										
8	Я		8	Ы	УВАЖАЕМЫ										
9	Н		9	И	УВАЖАЕМЫЙ										
10	4		10		УВАЖАЕМЫЙ										
11	Д		11	А	УВАЖАЕМЫЙ А										
12	С		12	Н	УВАЖАЕМЫЙ АН										
13	Ц		13	Т	УВАЖАЕМЫЙ АНТ										
14	Т		14	О	УВАЖАЕМЫЙ АНТО										
15	С		15	Н	УВАЖАЕМЫЙ АНТОН										
16	4		16		УВАЖАЕМЫЙ АНТОН										
17	З		17	Д	УВАЖАЕМЫЙ АНТОН Д										
18	Р		18	М	УВАЖАЕМЫЙ АНТОН ДМ										
19	М		19	И	УВАЖАЕМЫЙ АНТОН ДМИ										
20	Ц		20	Т	УВАЖАЕМЫЙ АНТОН ДМИТ										
21	Ф		21	Р	УВАЖАЕМЫЙ АНТОН ДМИТР										
22	М		22	И	УВАЖАЕМЫЙ АНТОН ДМИТРИ										
23	И		23	Е	УВАЖАЕМЫЙ АНТОН ДМИТРИЕ										
24	Е		24	В	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВ										
25	М		25	И	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИ										
26	Ы		26	Ч	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ										
27	2		27	.	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ.										
28	4		28		УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ.										
29	1		29	Я	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я										
30	4		30		УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я										
31	Е		31	Б	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я Б										
32	И		32	Е	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕ										
33	Л		33	З	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗ										
34	Р		34	М	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМ										
35	И		35	Е	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕ										
36	Ф		36	Р	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕР										
37	С		37	Н	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРН										
38	Т		38	О	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО										
39	4		39		УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО										
40	Ф		40	Р	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО Р										
41	Д		41	А	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО РА										
42	З		42	Д	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО РАД										
43	4		43		УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО РАД										
44	С		44	Н	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО РАД Н										
45	Д		45	А	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО РАД НА										
46	Б		46	Ш	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО РАД НАШ										
47	И		47	Е	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО РАД НАШЕ										
48	Р		48	М	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО РАД НАШЕМ										
49	Ч		49	У	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО РАД НАШЕМУ										
50	4		50		УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО РАД НАШЕМУ										
51	Х		51	С	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО РАД НАШЕМУ С										
52	Т		52	О	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО РАД НАШЕМУ СО										
53	Ц		53	Т	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО РАД НАШЕМУ СОТ										
54	Ф		54	Р	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО РАД НАШЕМУ СОТР										
55	Ч		55	У	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО РАД НАШЕМУ СОТРУ										
56	З		56	Д	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО РАД НАШЕМУ СОТРУД										
57	С		57	Н	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО РАД НАШЕМУ СОТРУДН										
58	М		58	И	УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ. Я БЕЗМЕРНО РАД НАШЕМУ СОТРУДНИ										

Рисунок 16 – Расшифровка сообщения (1 часть)

[illegible][illegible]

А результат расшифрования на рис.19.

[illegible]

3. Анализ частотности текста

3.1. Таблица и график частотности исходного алфавита

Рис. 20 – это частотность исходного алфавита, а на рис. 21 изображен график частотности.

Частотность алфавита		
Исходный алфавит		Частота
1	О	0,09050
2	Е	0,06971
3	А	0,06608
4	И	0,06064
5	Н	0,05528
6	Т	0,05165
7	С	0,04513
8	Р	0,03902
9	В	0,03746
10	Л	0,03630
11	К	0,02879
12	М	0,02648
13	Д	0,02459
14	П	0,02318
15	У	0,02162
16	Я	0,01658
17	Ы	0,01568
18	Ь	0,01436
19	Г	0,01403
20	З	0,01361
21	,	0,01346
22	.	0,01346
23		0,01346
24	1	0,01346
25	2	0,01346
26	3	0,01346
27	4	0,01346
28	5	0,01346
29	6	0,01346
30	7	0,01346
31	8	0,01346
32	9	0,01346
33	0	0,01346
34	Б	0,01312
35	Ч	0,01188
36	П	0,00998
37	Х	0,00800
38	Ж	0,00776
39	Ш	0,00602
40	Ю	0,00528
41	Ц	0,00396
42	Щ	0,00297
43	Э	0,00264
44	Ф	0,00215
45	Ё	0,00033
46	Ъ	0,00033
Сумма		1

Рисунок 20 – Таблица частоты исходного алфавита

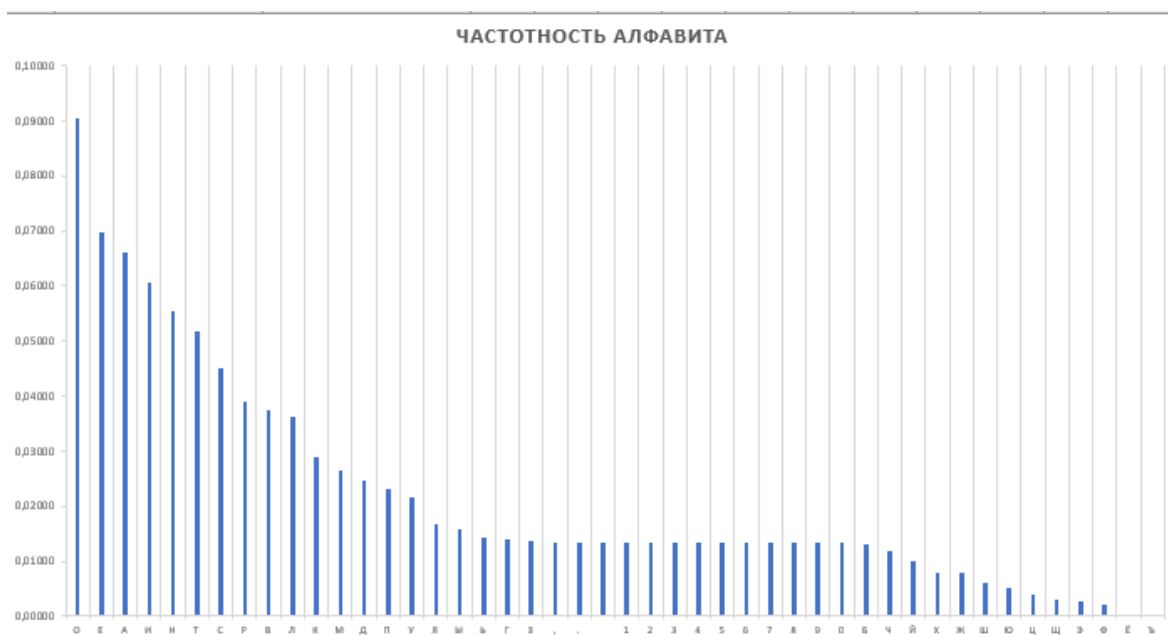


Рисунок 21 – График частотности исходного алфавита

3.2. Таблица и график частотности исходного текста

Рис. 22 – это частотность исходного текста, а на рис. 23 изображен график частотности.

Частотность исходного текста			
	Символ	Частота	Кол-во вложений
1		0,11348	16
2	О	0,11348	16
3	Е	0,07801	11
4	А	0,05674	8
5	И	0,04965	7
6	Н	0,04965	7
7	В	0,04255	6
8	Р	0,04255	6
9	Т	0,04255	6
10	Д	0,03546	5
11	Ч	0,03546	5
12	М	0,02837	4
13	С	0,02837	4
14	Ы	0,02837	4
15	,	0,02128	3
16	0	0,02128	3
17	2	0,02128	3
18	Л	0,02128	3
19	П	0,02128	3
20	Ь	0,02128	3
21	.	0,01418	2
22	Б	0,01418	2
23	З	0,01418	2
24	К	0,01418	2
25	Ю	0,01418	2
26	1	0,00709	1
27	3	0,00709	1
28	Г	0,00709	1
29	Ж	0,00709	1
30	И	0,00709	1
31	У	0,00709	1
32	Ф	0,00709	1
33	Ш	0,00709	1
34	4	0,00000	0
35	5	0,00000	0
36	6	0,00000	0
37	7	0,00000	0
38	8	0,00000	0
39	9	0,00000	0
40	Ё	0,00000	0
41	Х	0,00000	0
42	Ц	0,00000	0
43	Щ	0,00000	0
44	Ъ	0,00000	0
45	Э	0,00000	0
46	Я	0,00000	0
Сумма		1	

Рисунок 22 – Таблица частоты исходного текста

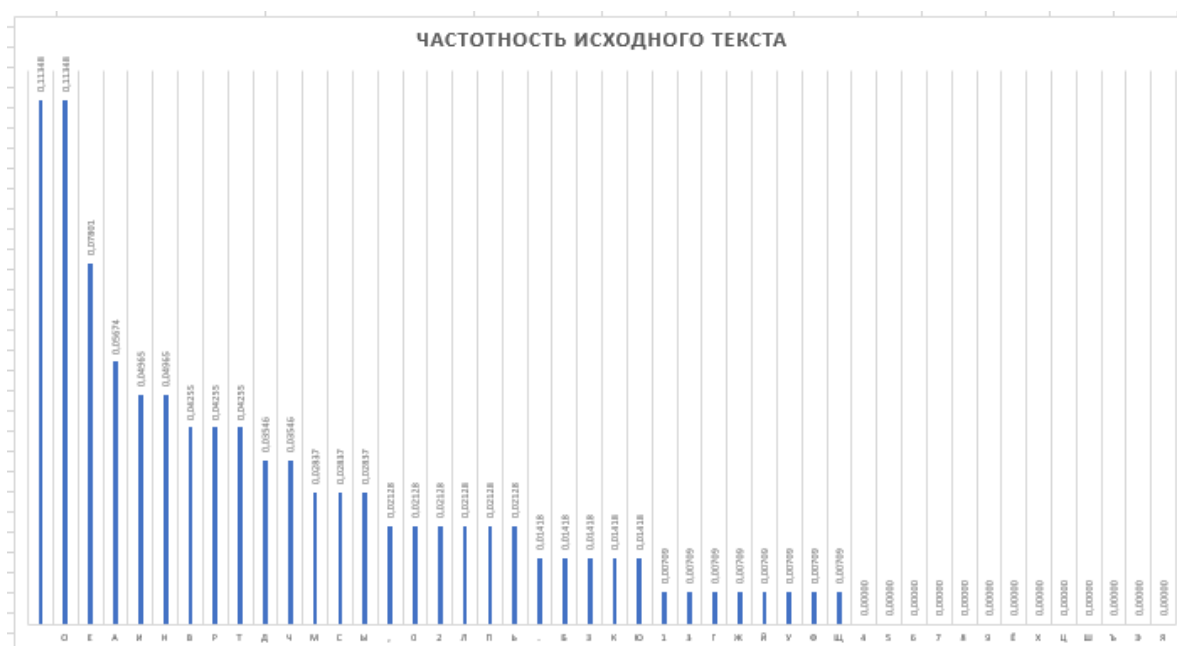


Рисунок 23 – График частотности исходного текста

3.3. Таблица и график частотности зашифрованного текста

Рис. 24 – это частотность зашифрованного текста, а на рис. 25 изображен график частотности.

Частотность зашифрованного текста			
	Символ	Частота	Кол-во вхождений
1	4	0,11348	16
2	Т	0,11348	16
3	И	0,07801	11
4	Д	0,05674	8
5	М	0,04965	7
6	С	0,04965	7
7	Е	0,04255	6
8	Ф	0,04255	6
9	Ц	0,04255	6
10	З	0,03546	5
11	Ы	0,03546	5
12	Р	0,02837	4
13	Х	0,02837	4
14	Я	0,02837	4
15	,	0,02128	3
16	2	0,02128	3
17	6	0,02128	3
18	Г	0,02128	3
19	П	0,02128	3
20	У	0,02128	3
21		0,01418	2
22	3	0,01418	2
23	Е	0,01418	2
24	Л	0,01418	2
25	О	0,01418	2
26	5	0,00709	1
27	7	0,00709	1
28	Ж	0,00709	1
29	К	0,00709	1
30	Н	0,00709	1
31	Ч	0,00709	1
32	Ш	0,00709	1
33	Э	0,00709	1
34	.	0,00000	0
35	0	0,00000	0
36	1	0,00000	0
37	8	0,00000	0
38	9	0,00000	0
39	А	0,00000	0
40	Б	0,00000	0
41	В	0,00000	0
42	Ї	0,00000	0
43	Щ	0,00000	0
44	Ъ	0,00000	0
45	Ь	0,00000	0
46	Ю	0,00000	0
Сумма			1

Рисунок 24 – Таблица частоты зашифрованного текста

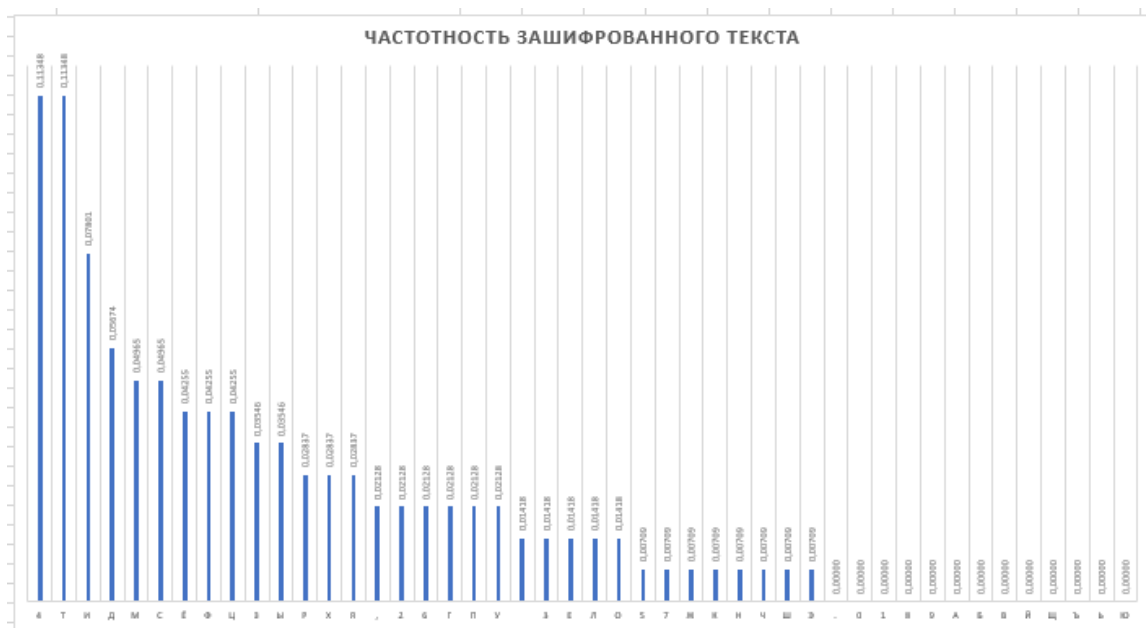


Рисунок 25 – График частотности зашифрованного текста

3.3. Общие данные частотности

На рис. 26 представленная общая таблица в практической работе.

Частотность алфавита			Частотность исходного текста				Частотность зашифрованного текста			
Исходный алфавит		Частота	Символ	Частота	Кол-во вхождений		Символ	Частота	Кол-во вхождений	
1	О	0,09060	1	0,11348	16		1	0,11348	16	
2	Е	0,06971	2	0,11348	16		2	0,11348	16	
3	А	0,06608	3	0,07801	11		3	0,07801	11	
4	П	0,06064	4	0,05674	8		4	0,05674	8	
5	Н	0,05528	5	0,04965	7		5	0,04965	7	
6	Т	0,05165	6	0,04965	7		6	0,04965	7	
7	С	0,04813	7	0,04255	6		7	0,04255	6	
8	Р	0,03902	8	0,04255	6		8	0,04255	6	
9	В	0,03746	9	0,04255	6		9	0,04255	6	
10	Л	0,03630	10	0,03546	5		10	0,03546	5	
11	К	0,02979	11	0,03546	5		11	0,03546	5	
12	М	0,02648	12	0,02837	4		12	0,02837	4	
13	Д	0,02459	13	0,02837	4		13	0,02837	4	
14	П	0,02318	14	0,02837	4		14	0,02837	4	
15	У	0,02162	15	0,02128	3		15	0,02128	3	
16	Я	0,01658	16	0,02128	3		16	0,02128	3	
17	Ы	0,01568	17	0,02128	3		17	0,02128	3	
18	Ь	0,01436	18	0,02128	3		18	0,02128	3	
19	Г	0,01403	19	0,02128	3		19	0,02128	3	
20	З	0,01361	20	0,02128	3		20	0,02128	3	
21	.	0,01346	21	0,01418	2		21	0,01418	2	
22	.	0,01346	22	0,01418	2		22	0,01418	2	
23	.	0,01346	23	0,01418	2		23	0,01418	2	
24	1	0,01346	24	0,01418	2		24	0,01418	2	
25	2	0,01346	25	0,01418	2		25	0,01418	2	
26	3	0,01346	26	0,00709	1		26	0,00709	1	
27	4	0,01346	27	0,00709	1		27	0,00709	1	
28	5	0,01346	28	0,00709	1		28	0,00709	1	
29	6	0,01346	29	0,00709	1		29	0,00709	1	
30	7	0,01346	30	0,00709	1		30	0,00709	1	
31	8	0,01346	31	0,00709	1		31	0,00709	1	
32	9	0,01346	32	0,00709	1		32	0,00709	1	
33	0	0,01346	33	0,00709	1		33	0,00709	1	
34	Б	0,01312	34	0,00000	0		34	0,00000	0	
35	Ч	0,01188	35	0,00000	0		35	0,00000	0	
36	П	0,00998	36	0,00000	0		36	0,00000	0	
37	Х	0,00800	37	0,00000	0		37	0,00000	0	
38	Ж	0,00776	38	0,00000	0		38	0,00000	0	
39	Ш	0,00602	39	0,00000	0		39	0,00000	0	
40	Ю	0,00528	40	0,00000	0		40	0,00000	0	
41	Ц	0,00396	41	0,00000	0		41	0,00000	0	
42	Щ	0,00297	42	0,00000	0		42	0,00000	0	
43	Э	0,00264	43	0,00000	0		43	0,00000	0	
44	Ф	0,00215	44	0,00000	0		44	0,00000	0	
45	Е	0,00033	45	0,00000	0		45	0,00000	0	
46	Ь	0,00033	46	0,00000	0		46	0,00000	0	
Сумма		1	Сумма		1		Сумма		1	

Рисунок 26 – Общая таблица частотности

4. Заключение

В ходе выполнения данной практической работы было реализовано шифрование и расшифрование сообщения с помощью моно алфавитного шифра, произведен анализ слабостей данного шифра. Были получены навыки по работе с Excel и реализацией алгоритмов шифрования.