Российский университет транспорта (МИИТ)

Институт транспортной техники и систем управления

Кафедра «Управление и защита информации»

Отчет

по практическому заданию

по теме «Разработка семейства полиалфавитных шифров: шифр 2»

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.

Москва 2023

Оглавление

Задание

1. Разобрать таблицы шифрования/расшифрования для шифра №2.
2. Подготовить, зашифровать и расшифровать сообщение.
3. Провести анализ слабостей шифра, сравнить с результатами предыдущих заданий.
4. Оформить отчет.

Исходные данные

1. Тип полиалфавитного шифра – квадрат Виженера (базовый, первая строка начинается с первого символа алфавита шифра).
2. Первая строка квадрата соответствует моноалфавитному шифру студента.
3. Размер шифруемого блока = мощность алфавита = 46.
4. С переходом к следующему блоку применяется следующий моноалфавитный шифр (следующая строка базового шрифта).
5. Передаваемое сообщение: «Уважаемый Игорь Феодосьевич, спешу сообщить Вам о том, что практическая работа 6 выполнена и готова к проверке. Дроздов Антон Дмитриевич 03.12.2002. Уважаемый Антон Дмитриевич, я безмерно рад нашему сотрудничеству, надеюсь на его дальнейшее успешное и взаимовыгодное развитие. С уважением, Игорь Феодосьевич».

1. Краткие теоритические сведения о шифре

1.1 Полиавлфавиный шифр

Полиалфавитный шифр замены – шифр, при котором символы исходного сообщения заменяются символами исходного алфавита с переменным сдвигом по ключу.

Полиалфавитный шифр на основе ключевой последовательности:

Первичный ключ – любое слово или фраза.

Ключевая последовательность – последовательность символов, сформированная повторением первичного ключа до размера шифруемого сообщения.

M_i – символ на i-й позиции сообщения, $i \in Z$.

C_i – символ на i-й позиции криптограммы.

C_i – суперпозиция i-го символа сообщения и i-го символа ключевой последовательности.

$C_i = M_i \,\&\, S_i$

$M_i = C_i \,\&\, S_i$

1.2. Определение полиафавитного шифра замены

Полиалфавитный шифр замены – шифр, при котором символы исходного сообщения заменяются символами исходного алфавита с переменным сдвигом по ключу.

1.3. Полиалфавитный шифр на основе шифрования блоков

Полиалфавитный шифр – квадрат Виженера с ключом студента. Сообщение разбивается на блоки длиной n, соответствующей мощности моноалфавитного шифра.

Строки квадрата полиалфавитного шифра нумеруются от 0 до $n - 1$. Нулевая строка в шифровании не участвует.

M_i – символ на i-й позиции сообщения.

M_j – символ на j-й позиции в l-м блоке сообщения, $l = 1, \dots, L$.

$j = i/n \bmod n$ – позиция i-го символа в блоке.

$L = [I/n]$ – число блоков сообщения, I – объем сообщения.

C_i - символ на i-й позиции криптограммы.

$C_i = M_i(l)$, $l = [i/n] + 1 \bmod n$

1.4. Пример квадрата Виженера для блочного шифрования

Значение ключа k=32 / Номер блока сообщения	Позиция символа в алфавите шифраа (мощность n = 33)																																
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
		Значение символа в блоке сообщения																																
		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
0	А	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
1	Я	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
2	Б	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
3	В	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
4	Г	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
5	Д	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
6	Е	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
7	Ё	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
8	Ж	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
9	З	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
10	И	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
11	Й	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
12	К	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
13	Л	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
14	М	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
15	Н	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
16	О	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
17	П	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
18	Р	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
19	С	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
20	Т	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
21	У	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
22	Ф	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
23	Х	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
24	Ц	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
25	Ч	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
26	Ш	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
27	Щ	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
28	Ъ	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
29	Ы	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
30	Ь	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
31	Э	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
32	Ю	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

Рисунок 1 – Квадрат Виженера

2. Практическая часть

2.1. Исходные данные

Ниже, на рисунке 2, представлены исходные данные, используемые в нашей практической работе, а на рисунке 3, представлен квадрат Виженера.

Передаваемое сообщение:	Ключ:	Мощность алфавита:	Длина исходного сообщения
Уважаемый Игорь Феодосьевич, сообщаю Вам, что практическое задание номер 6 было полностью выполнено, Дроздов Антон Дмитриевич 03.12.2002. Уважаемый Антон Дмитриевич, я безмерно рад нашему сотрудничеству, надеюсь на его дальнейшее успешное и взаимовыгодное развитие. С уважением Игорь Феодосьевич.	17	46	296

Рисунок 2 – Исходные данные

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

Рисунок 3 – Блокнот шифрования (таблица шифрования, шифр)

2.1. Зашифровка сообщения

Ниже, на рисунке 4, представлена таблица порядка действий зашифровки исходного текста инициатора, а на рисунке 5, представлена таблица результата шифрования и длины сообщений.

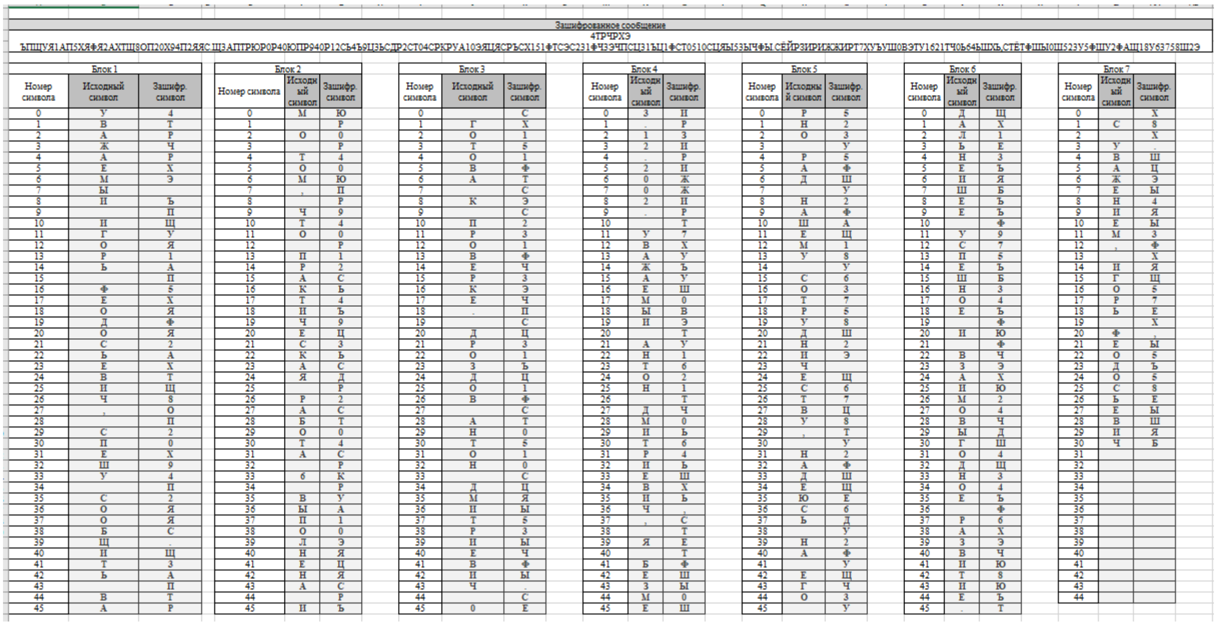


Рисунок 4 – Зашифровка сообщения

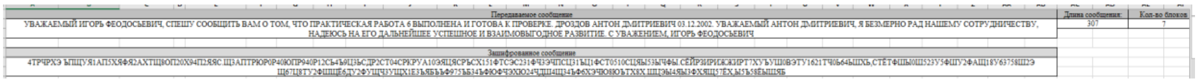
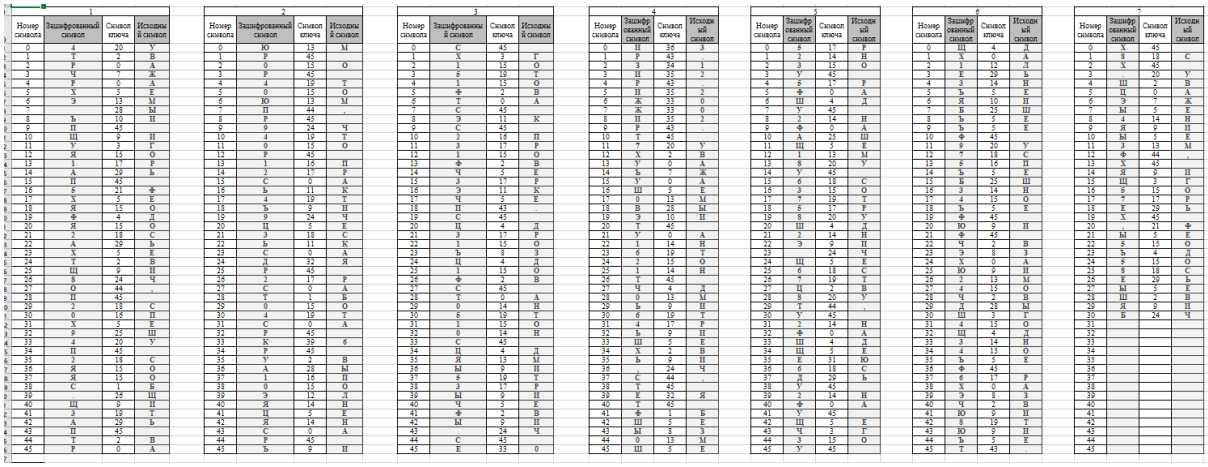


Рисунок 5 – Результат шифрования

2.2. Расшифровка сообщения

Ниже, на рисунке 6, представлена таблица порядка действий расшифровки текста, для получения исходного, а на рисунке 7, представлена таблица результата расшифровки и длины сообщений.



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

2			
Номер символа	Зашифрованный символ	Символ ключа	Исходный символ
0	Ю	13	М
1	Р	45	.
2	0	15	О
3	Р	45	.
4	4	19	Т
5	0	15	О
6	Ю	13	М
7	П	44	,
8	Р	45	.
9	9	24	Ч
10	4	19	Т
11	0	15	О
12	Р	45	.
13	1	16	П
14	2	17	Р
15	С	0	А
16	Ъ	11	К
17	4	19	Т
18	Ъ	9	И
19	9	24	Ч
20	Щ	5	Е
21	3	18	С
22	Ъ	11	К
23	С	0	А
24	Д	32	Я
25	Р	45	.
26	2	17	Р
27	С	0	А
28	Т	3	Б
29	0	15	О
30	4	19	Т
31	С	0	А
32	Р	45	.
33	К	39	6
34	Р	45	.
35	У	2	В
36	А	28	Ы
37	1	16	П
38	0	15	О
39	Э	12	Л
40	Я	14	Н
41	Щ	5	Е
42	Я	14	Н
43	С	0	А
44	Р	45	.
45	Ъ	9	И

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

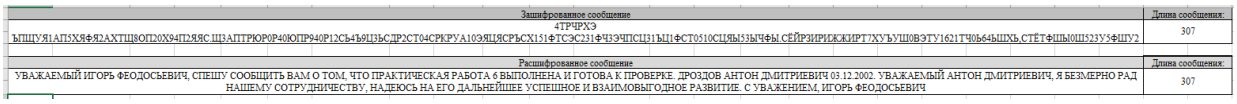
4			
Номер символа	Зашифрованный символ	Символ ключа	Исходный символ
0	И	36	З
1	Р	43	,
2	3	34	1
3	И	35	2
4	Р	43	,
5	И	35	2
6	Ж	33	0
7	Ж	33	0
8	И	35	2
9	Р	43	,
10	Т	45	.
11	7	20	У
12	Х	2	В
13	У	0	А
14	Ъ	7	Ж
15	У	0	А
16	Ш	5	Е
17	7	20	У
18	В	28	Ы
19	Э	10	И
20	Т	45	.
21	У	0	А
22	1	14	Н
23	6	19	Т
24	2	15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

5			
Номер символа	Зашифрованный символ	Символ ключа	Исходный символ
0	5	17	Р
1	2	14	Н
2	3	15	О
3	У	45	.
4	5	17	Р
5	Ф	0	А
6	Ш	4	Д
7	У	45	.
8	2	14	Н
9	Ф	0	А
10	А	25	Ш
11	Щ	5	Е
12	1	13	М
13	8	20	У
14	У	45	.
15	6	18	С
16	3	15	О
17	7	19	Т
18	5	17	Р
19	8	20	У
20	Ш	4	Д
21	2	14	Н
22	Э	9	И
23	.	24	Ч
24	Щ	5	Е
25	6	18	С
26	7	19	Т
27	Ц	2	В
28	8	20	У
29	Т	44	,
30	У	45	.
31	2	14	Н
32	Ф	0	А
33	Ш	4	Д
34	Щ	5	Е
35	Е	31	Ю
36	6	18	С
37	Д	29	Ь
38	У	45	.
39	2	14	Н
40	Ф	0	А
41	У	45	.
42	Щ	5	Е
43	Ч	3	Г
44	3	15	О
45	У	45	.

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

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

Рисунок 6 – Расшифровка сообщения



Зашифрованное сообщение	Длина сообщения:
4ТРЧРХЭ ЪЩЦУЯ1АП5ХЯФЯ2АХТЩ8ОП20Х94П2ЯЯС.Щ3АПТРЮР0Р40ЮПР940Р12СЬЧ9Ц3ЬСДР2СТ04СРКРУА10ЭЯЦЯСРЪСХ151ФТСЭС231ФЧЗЭЧПСЦ31ЪЦ1ФСТ0510СЦЯЫ53ЫЧФЫ.СЁЙРЗИРИЖЖИРТ7ХУЪУЦ00ВЭТУ1621ТЧ0Ь64ЬШХЬ.СТЁТФЩЫ0Ш523УЪФШУ2	307

Расшифрованное сообщение	Длина сообщения:
УВАЖАЕМЫЙ ИГОРЬ ФЕОДОСЬЕВИЧ, СПЕШУ СООБЩИТЬ ВАМ О ТОМ, ЧТО ПРАКТИЧЕСКАЯ РАБОТА 6 ВЫПОЛНЕНА И ГОТОВА К ПРОВЕРКЕ. ДРОЗДОВ АНТОН ДМИТРИЕВИЧ 03.12.2002. УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ, Я БЕЗМЕРНО РАД НАШЕМУ СОТРУДНИЧЕСТВУ, НАДЕЮСЬ НА ЕГО ДАЛЬНЕЙШЕЕ УСПЕШНОЕ И ВЗАИМОВЫГОДНОЕ РАЗВИТИЕ. С УВАЖЕНИЕМ, ИГОРЬ ФЕОДОСЬЕВИЧ	307

Рисунок 7 – Результат расшифровки

3. Анализ частотности шифров

Ниже, на рисунке 8, представлена сравнительная таблица частотности.

Результаты расчёта частотности

Исходный алфавит			Исходный текст				Зашифрованное сообщение инициатора шифром Цезаря				Зашифрованное сообщение полиалфавитным шифром № 1 (по алфавитному ключу)				Зашифрованное сообщение полиалфавитным шифром № 2 (на основе бинарного шифра)			
	Символ	Частота		Символ	Кол-во вхождений	Частота		Символ	Кол-во вхождений	Частота		Символ	Кол-во вхождений	Частота		Символ	Кол-во вхождений	Частота
1	О	0,09050	1		36	0,12162	1	4	36	0,12162	1	Щ	18	0,06081	1	У	14	0,04730
2	Е	0,06971	2	Е	28	0,09459	2	И	28	0,09459	2	З	17	0,05743	2	Т	13	0,04392
3	А	0,06608	3	О	27	0,09122	3	Т	27	0,09122	3	М	15	0,05068	3	І	13	0,04392
4	И	0,06064	4	А	19	0,06419	4	Д	19	0,06419	4	О	12	0,04054	4	0	13	0,04392
5	Н	0,05528	5	И	18	0,06081	5	С	18	0,06081	5	Ш	12	0,04054	5	Я	12	0,04054
6	Т	0,05165	6	В	14	0,04730	6	М	18	0,06081	6	П	11	0,03716	6	2	12	0,04054
7	С	0,04513	7	Н	18	0,06081	7	Ё	14	0,04730	7	Н	10	0,03378	7	Щ	12	0,04054
8	Р	0,03902	8	Р	11	0,03716	8	З	12	0,04054	8	Т	10	0,03378	8	Ф	12	0,04054
9	В	0,03746	9	Т	10	0,03378	9	Ф	11	0,03716	9	Х	10	0,03378	9	Ъ	12	0,04054
10	Л	0,03630	10	Д	12	0,04054	10	Р	10	0,03378	10	Э	10	0,03378	10	Р	11	0,03716
11	К	0,02879	11	М	10	0,03378	11	Х	10	0,03378	11	Ы	9	0,03041	11	З	11	0,03716
12	М	0,02648	12	С	10	0,03378	12	Ц	10	0,03378	12	И	8	0,02703	12	Х	11	0,03716
13	Д	0,02459	13	У	7	0,02365	13	Ы	7	0,02365	13	У	8	0,02703	13	С	10	0,03378
14	П	0,02318	14	Ч	7	0,02365	14	.	7	0,02365	14	Г	8	0,02703	14	4	10	0,03378
15	У	0,02162	15	Ь	7	0,02365	15	Ч	7	0,02365	15	6	8	0,02703	15	Ч	10	0,03378
16	Я	0,01658	16	.	5	0,01689	16	Л	5	0,01689	16	Ъ	8	0,02703	16	П	9	0,03041
17	Ы	0,01568	17	.	5	0,01689	17	Я	5	0,01689	17	Р	7	0,02365	17	Ш	9	0,03041
18	Ь	0,01436	18	П	4	0,01351	18	2	5	0,01689	18	0	7	0,02365	18	5	8	0,02703
19	Г	0,01403	19	Г	4	0,01351	19	3	5	0,01689	19	Б	7	0,02365	19	Ю	8	0,02703
20	З	0,01361	20	Ы	5	0,01689	20	П	4	0,01351	20	Щ	7	0,02365	20	Ц	8	0,02703
21	.	0,01346	21	З	5	0,01689	21	У	4	0,01351	21	Ф	7	0,02365	21	Э	8	0,02703
22	.	0,01346	22	Ш	3	0,01014	22	Ж	4	0,01351	22	К	6	0,02027	22	8	7	0,02365
23		0,01346	23	К	2	0,00676	23	Е	3	0,01014	23	Ч	6	0,02027	23	Ё	7	0,02365
24	І	0,01346	24	0	3	0,01014	24	Н	3	0,01014	24	Й	6	0,02027	24	Ы	6	0,02027
25	2	0,01346	25	Ж	3	0,01014	25	К	3	0,01014	25	С	5	0,01689	25	Ь	6	0,02027
26	3	0,01346	26	Й	3	0,01014	26	Ь	3	0,01014	26	Д	5	0,01689	26	6	6	0,02027
27	4	0,01346	27	Б	3	0,01014	27	Г	3	0,01014	27	Я	5	0,01689	27	7	6	0,02027
28	5	0,01346	28	2	3	0,01014	28		3	0,01014	28	.	5	0,01689	28	А	5	0,01689
29	6	0,01346	29	Л	4	0,01351	29	6	3	0,01014	29	Е	4	0,01351	29	Д	3	0,01014
30	7	0,01346	30	Я	1	0,00338	30	О	2	0,00676	30	Л	4	0,01351	30	З	3	0,01014
31	8	0,01346	31	Ф	2	0,00676	31	Ш	2	0,00676	31	Ь	4	0,01351	31		3	0,01014
32	9	0,01346	32	Ю	3	0,01014	32	І	1	0,00338	32	.	4	0,01351	32	9	3	0,01014
33	0	0,01346	33	І	1	0,00338	33	5	1	0,00338	33		4	0,01351	33	Б	3	0,01014
34	Б	0,01312	34	Щ	1	0,00338	34	7	1	0,00338	34	2	4	0,01351	34	О	2	0,00676
35	Ч	0,01188	35	З	1	0,00338	35	8	1	0,00338	35	З	4	0,01351	35	В	2	0,00676
36	Й	0,00998	36	6	1	0,00338	36	Э	1	0,00338	36	І	3	0,01014	36	.	2	0,00676
37	Х	0,00800	37	9	0	0,00000	37	А	0	0,00000	37	5	3	0,01014	37	,	2	0,00676
38	Ж	0,00776	38	5	0	0,00000	38	В	0	0,00000	38	7	3	0,01014	38	И	1	0,00338
39	Ш	0,00602	39	4	0	0,00000	39	,	0	0,00000	39	Ю	3	0,01014	39	К	1	0,00338
40	Ю	0,00528	40	8	0	0,00000	40	9	0	0,00000	40	4	2	0,00676	40	Г	1	0,00338
41	Ц	0,00396	41	7	0	0,00000	41	0	0	0,00000	41	8	2	0,00676	41	Ж	1	0,00338
42	Щ	0,00297	42	Ё	0	0,00000	42	Б	0	0,00000	42	9	2	0,00676	42	Е	0	0,00000
43	Э	0,00264	43	Х	0	0,00000	43	Й	0	0,00000	43	Ж	2	0,00676	43	Н	0	0,00000
44	Ф	0,00215	44	Ц	0	0,00000	44	Ю	0	0,00000	44	В	1	0,00338	44	Л	0	0,00000
45	Ё	0,00033	45	Ъ	0	0,00000	45	Щ	0	0,00000	45	А	0	0,00000	45	М	0	0,00000
46	Ъ	0,00033	46	Э	0	0,00000	46	Ъ	0	0,00000	46	Ё	0	0,00000	46	Й	0	0,00000
		Сумма			Длина сообщ	Сумма			Длина сообщ	Сумма			Длина сообщ	Сумма			Длина сообщ	Сумма
		1			296	1			296	1			296	1			296	1

Рисунок 8 – Таблица сравнения частоты

Далее, на рисунке 9 представлен график частотности исходного алфавита. На рисунке 10 – график исходного текста.

Рисунок 9 – График частотности исходного алфавита

Рисунок 10 – График частотности исходного текста

Рисунок 11 – это график частотности зашифрованного текста шифров Цезаря.

Рисунок 11 – График частотности текста (на основе Цезаря)

А на рисунках 12 и 13 – графики частотности зашифрованного текста на основе шифра 1 и блочного шифра соответственно.

Рисунок 12 – График частотности текста (на основе шифра 1)

Рисунок 13 – График частотности текста (на основе блочного шифра)

4. Сравнение шифров

В сравнении с моноалфавитным шифром (на основе шифра Цезаря) и полиалфавитным шифром (на основе квадрата Виженера), полиалфавитный шифр, основанный на блочной шифровании обладает большей криптостойкостью, это можно заметить, исследуя частотность символов зашифрованного текста. Частоты символов при применении полиалфавитного шифра с блочным шифрованием распределены более равномерно, что значительно усложняет подбор ключа. Криптостойкость полиалфавитного шифра на основе шифрования блоков зависит от размера блоков, размера ключа и числа раундов шифрования. Чем хуже эти характеристики, тем меньше усилий понадобится злоумышленнику для нахождения ключа и взлома шифра.

Ниже, на рисунке 14, представлен график частотностей каждого шифра.

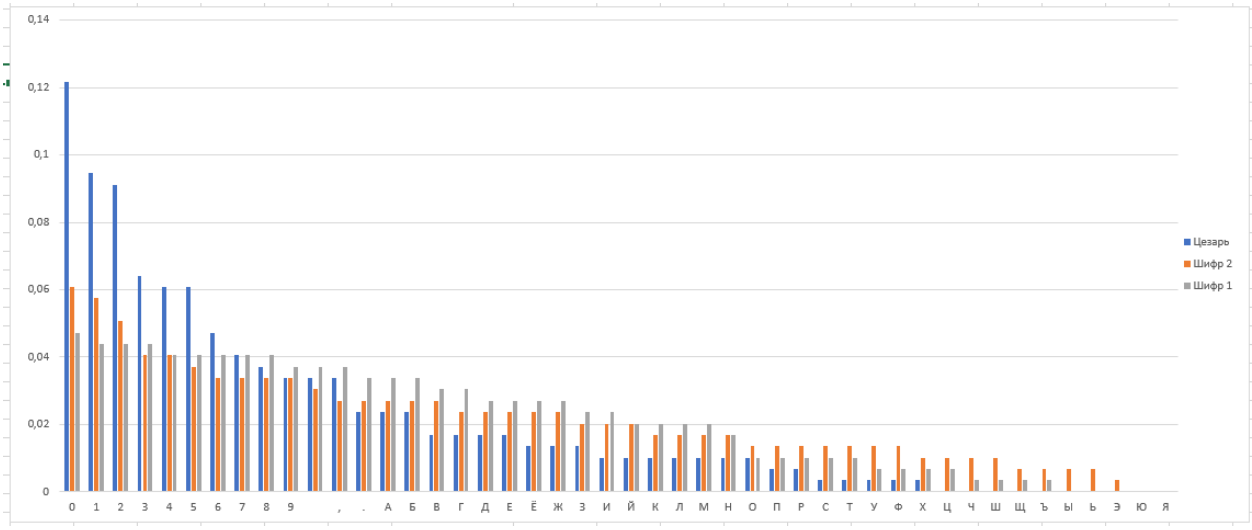


Рисунок 14 – Общий график сравнения шифров

5. Заключение

В ходе выполнения данной практической работы был реализован полиалфавитный шифр на основе шифрования блоков, таблицы шифрования/расшифрования, зашифровано и расшифровано сообщение. Проведен анализ слабостей шифра, приведены таблицы и гистограммы частотности символов исходного алфавита и сообщения, зашифрованного разработанным шифром, описаны слабости шифра. Проведен сравнительный анализ моноалфавитного шифра, полиалфавитного шифров и полиалфавитного шифра на основе шифрования блоков, в результате чего выяснилось, что последний обладает наибольшей криптостойкостью. Получены навыки в работе с полиалфавитными шифрами в Excel.