

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 1»

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	3
Исходные данные	4
1. Краткие теоритические сведения о шифре.....	5
1.1 Определения шифра и ключа	5
1.2. Составные элементы шифра	5
1.3. Алфавит	5
1.4. Определение шифра в общем случае	6
1.5. Полиалфавинный шифр	6
1.6. Полиалфавитный шифр на основе ключевой последованности	7
2. Практическая часть	8
2.1. Зашифровка сообщения.....	8
2.2. Расшифровка сообщения.....	9
3. Анализ частотности текста.....	10
3.1. Таблица и график частотности исходного алфавита.....	10
3.2. Таблица и график частотности исходного текста.....	10
3.3. Таблица и график частотности зашифрованного текста (шифр Цезаря)	11
3.4. Таблица и график частотности зашифрованного текста (шифр 1)	12
4. Заключение	13

Задание

1. Разработать базовый полиалфавитный шифр.
2. Разобрать таблицы шифрования/расшифрования для шифра №1.
3. Подготовить, зашифровать и расшифровать сообщение.
4. Провести анализ слабостей шифра.
5. 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. Первичный ключ шифра – ШИФРОВАНИЕ
4. Ключевая последовательность – повторение первичного ключа до размера передаваемого сообщения.
5. Передаваемое сообщение: «Уважаемый Игорь Феодосьевич, спешу сообщить Вам о том, что практическая работа 5 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 Определения шифра и ключа

Шифр – система заранее оговоренных обратимых преобразований защищаемой информации (текста, изображений, аудио, видео, ...) 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, ...).

1.2. Составные элементы шифра

- алфавит;
- алгоритмы обратимых преобразований исходного сообщения в криптограммы и обратного преобразования криптограмм в открытое сообщение (зашифрования и расшифрования);
- множество ключей.

1.3. Алфавит

Алфавит – набор уникальных символов для записи зашифрованных сообщений (буквы, цифры, знаки препинания, специальные символы, ...).

Мощность алфавита – полное число символов алфавита.

Мощность алфавита (в общем случае):

- русского языка – 33
- английского – 26

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

1.4. Определение шифра в общем случае

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 KE и соответствующие им обратные функции расшифрования D_k , зависящие от выбранного ключа расшифрования из множества KD , отображающие множество криптограмм C на множество открытых сообщений M .

Запись алгоритма шифрования (общего)

$$E_k, k \in KE : M \rightarrow C,$$

$$D_k, k \in KD : C \rightarrow M,$$

$$\forall k \in KE \exists k \in KD,$$

$$\forall m \in M : E_k(m) = c,$$

$$\forall c \in C : D_k(c) = m$$

1.5. Полиалфавинный 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.

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

$$C_i = M_i \& S_i$$

$$M_i = C_i \& S_i$$

1.6. Полиалфавитный шифр на основе ключевой последовательности

Шифр Виженера – метод простого полиалфавитного шифра замены на основе ключевого слова, преобразованного в одномерный с сообщением ключ, задающий переменный параметр k_i сдвига символов исходного сообщения.

k_i – переменный параметр сдвига по ключевому слову.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Рисунок 1 – Квадрат Виженера

2.2. Расшифровка сообщения

Ниже, на рисунке 4, представлена таблица порядка действий расшифровки текста, для получения исходного, а на рисунке 5, представлена таблица результата расшифровки и длины сообщений.

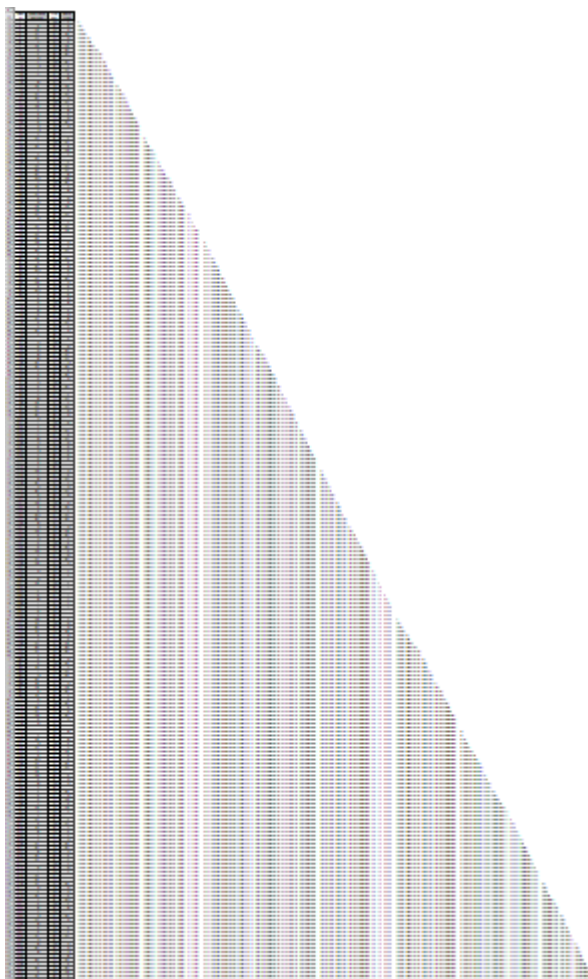


Рисунок 4 – Расшифровка сообщения

Зашифрованное сообщение		Длина сообщения:
К*ЦОЗМВСДОЛ*Д*В*ТЦЙЩХРЧЛЦГНЗНУОЫЙКОУПРВМАЩДЦЮЩЦТЗ*ВНОЛЩКОТ*В*З*РПТ*НЗ*Ч*В*В*Н*Т*Л*Е*Ч*Р*У*В*О*П*И*Д*З*З*О*Б*Д*Е*Т*К*О*З*Ш*Ь*М*Д*Ы*К*Ш*Л*О*У*В*Д*Ц*Р*Ч*А*Р*Ц*Т*Ц*Ц А*В*М*С*Е*В*Л*К*Ш*И*Т*Ь*Р*У*О*Щ*Ц*В*Ь*З*О*Н*Е*В*О*У*О*Н*Щ*Е*А*Ж*Е*Т*О*Л*О*Т*О*М*Щ*Е*В*О*П*Р*Е*В*О*Щ*Е*В*А*Т*Т*И*Н*Ц*К*О*Н*П*А*С*Н*Р*А*У*О*В*Е*Р*Ц*И*Я*В*Ы*И*З*И*С*Ы*Л*У*А*У*А*Н*Ц*О*У*А*Л*О*У*Щ*Ц*В*Ь*З*З*И*О*Г*А*Р*Ш*У*К*О*Ш*И*Т*Ь*А*Л*К*Е*Щ*Д*О*Д*О*В*Б*Т*Ц*Й*Щ*Х*Р*К		306
Расшифрованное сообщение		Длина сообщения:
УВАЖАЕМЫЙ ИГОРЬ ФЕОДОСЬЕВИЧ, СПЕШУ СООБЩИТЬ ВАМ О ТОМ, ЧТО ПРАКТИЧЕСКАЯ РАБОТА : 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		306

Рисунок 5 – Результат расшифровки

3. Анализ частотности текста

3.1. Таблица и график частотности исходного алфавита

Ниже, на рисунке 6, представлена таблица частотности исходного алфавита в порядке уменьшения, а на рисунке 7, представлен график построенный на основе данной таблицы.

Матрица элементов A_{ij} для α		
i	j	Числ. значение
1	1	0,00000
1	2	0,00077
2	1	0,00089
2	2	0,00064
3	1	0,00528
3	2	0,00565
3	3	0,00513
4	1	0,00902
4	2	0,00746
4	3	0,00762
4	4	0,00750
5	1	0,02479
5	2	0,02459
5	3	0,02458
5	4	0,02458
5	5	0,02457
6	1	0,02167
6	2	0,02166
6	3	0,02167
6	4	0,02166
6	5	0,02166
6	6	0,02166
7	1	0,03346
7	2	0,03346
7	3	0,03346
7	4	0,03346
7	5	0,03346
7	6	0,03346
7	7	0,03346
8	1	0,03346
8	2	0,03346
8	3	0,03346
8	4	0,03346
8	5	0,03346
8	6	0,03346
8	7	0,03346
8	8	0,03346
9	1	0,03346
9	2	0,03346
9	3	0,03346
9	4	0,03346
9	5	0,03346
9	6	0,03346
9	7	0,03346
9	8	0,03346
9	9	0,03346
10	1	0,03346
10	2	0,03346
10	3	0,03346
10	4	0,03346
10	5	0,03346
10	6	0,03346
10	7	0,03346
10	8	0,03346
10	9	0,03346
10	10	0,03346

Рисунок 6 – Таблица частоты исходного алфавита

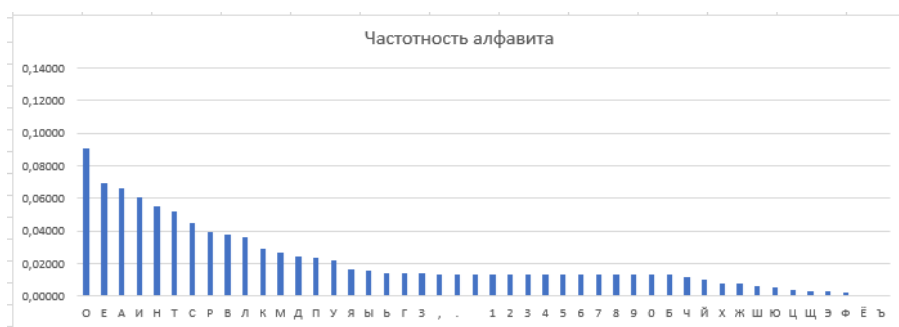


Рисунок 7 – График частотности исходного алфавита

3.2. Таблица и график частотности исходного текста

Ниже, на рисунке 8, представлена таблица частотности использования алфавита в исходном тексте в порядке уменьшения, а на рисунке 9, представлен график построенный на основе данной таблицы.

Частотность исходного текста			
	Символ	Кол-во встречений	Частота
1		57	0,122361
2	Е	38	0,097788
3	О	25	0,064421
4	А	20	0,051948
5	И	20	0,051948
6	Н	17	0,043944
7	В	14	0,036195
8	Р	12	0,031158
9	М	11	0,028466
10	Л	10	0,025977
11	Т	10	0,025977
12	С	9	0,023487
13	У	7	0,018148
14	Г	7	0,018148
15	Ь	6	0,015658
16	Б	5	0,013169
17	Д	5	0,013169
18	Ж	4	0,010679
19	К	4	0,010679
20	З	4	0,010679
21	И	4	0,010679
22	О	4	0,010679
23	А	3	0,008189
24	Н	3	0,008189
25	В	3	0,008189
26	Р	3	0,008189
27	М	2	0,006099
28	Л	2	0,006099
29	Т	2	0,006099
30	С	2	0,006099
31	У	2	0,006099
32	Г	2	0,006099
33	Ж	2	0,006099
34	К	1	0,003558
35	З	1	0,003558
36	И	1	0,003558
37	О	1	0,003558
38	А	1	0,003558
39	Н	1	0,003558
40	В	1	0,003558
41	Р	1	0,003558
42	М	1	0,003558
43	Л	1	0,003558
44	Т	1	0,003558
45	С	1	0,003558
46	У	1	0,003558
47	Г	1	0,003558
48	Ж	1	0,003558
49	К	1	0,003558
50	З	1	0,003558
51	И	1	0,003558
52	О	1	0,003558
53	А	1	0,003558
54	Н	1	0,003558
55	В	1	0,003558
56	Р	1	0,003558
57	М	1	0,003558
58	Л	1	0,003558
59	Т	1	0,003558
60	С	1	0,003558
61	У	1	0,003558
62	Г	1	0,003558
63	Ж	1	0,003558
64	К	1	0,003558
65	З	1	0,003558
66	И	1	0,003558
67	О	1	0,003558
68	А	1	0,003558
69	Н	1	0,003558
70	В	1	0,003558
71	Р	1	0,003558
72	М	1	0,003558
73	Л	1	0,003558
74	Т	1	0,003558
75	С	1	0,003558
76	У	1	0,003558
77	Г	1	0,003558
78	Ж	1	0,003558
79	К	1	0,003558
80	З	1	0,003558
81	И	1	0,003558
82	О	1	0,003558
83	А	1	0,003558
84	Н	1	0,003558
85	В	1	0,003558
86	Р	1	0,003558
87	М	1	0,003558
88	Л	1	0,003558
89	Т	1	0,003558
90	С	1	0,003558
91	У	1	0,003558
92	Г	1	0,003558
93	Ж	1	0,003558
94	К	1	0,003558
95	З	1	0,003558
96	И	1	0,003558
97	О	1	0,003558
98	А	1	0,003558
99	Н	1	0,003558
100	В	1	0,003558
101	Р	1	0,003558
102	М	1	0,003558
103	Л	1	0,003558
104	Т	1	0,003558
105	С	1	0,003558
106	У	1	0,003558
107	Г	1	0,003558
108	Ж	1	0,003558
109	К	1	0,003558
110	З	1	0,003558
111	И	1	0,003558
112	О	1	0,003558
113	А	1	0,003558
114	Н	1	0,003558
115	В	1	0,003558
116	Р	1	0,003558
117	М	1	0,003558
118	Л	1	0,003558
119	Т	1	0,003558
120	С	1	0,003558
121	У	1	0,003558
122	Г	1	0,003558
123	Ж	1	0,003558
124	К	1	0,003558
125	З	1	0,003558
126	И	1	0,003558
127	О	1	0,003558
128	А	1	0,003558
129	Н	1	0,003558
130	В	1	0,003558
131	Р	1	0,003558
132	М	1	0,003558
133	Л	1	0,003558
134	Т	1	0,003558
135	С	1	0,003558
136	У	1	0,003558
137	Г	1	0,003558
138	Ж	1	0,003558
139	К	1	0,003558
140	З	1	0,003558
141	И	1	0,003558
142	О	1	0,003558
143	А	1	0,003558
144	Н	1	0,003558
145	В	1	0,003558
146	Р	1	0,003558
147	М	1	0,003558
148	Л	1	0,003558
149	Т	1	0,003558
150	С	1	0,003558
151	У	1	0,003558
152	Г	1	0,003558
153	Ж	1	0,003558
154	К	1	0,003558
155	З	1	0,003558
156	И	1	0,003558
157	О	1	0,003558
158	А	1	0,003558
159	Н	1	0,003558
160	В	1	0,003558
161	Р	1	0,003558
162	М	1	0,003558
163	Л	1	0,003558
164	Т	1	0,003558
165	С	1	0,003558
166	У	1	0,003558
167	Г	1	0,003558
168	Ж	1	0,003558
169	К	1	0,003558
170	З	1	0,003558
171	И	1	0,003558
172	О	1	0,003558
173	А	1	0,003558
174	Н	1	0,003558
175	В	1	0,003558
176	Р	1	0,003558
177	М	1	0,003558
178	Л	1	0,003558
179	Т	1	0,003558
180	С	1	0,003558
181	У	1	0,003558
182	Г	1	0,003558
183	Ж	1	0,003558
184	К	1	0,003558
185	З	1	0,003558
186	И	1	0,003558
187	О	1	0,003558
188	А	1	0,003558
189	Н	1	0,003558
190	В	1	0,003558
191	Р	1	0,003558
192	М	1	0,003558
193	Л	1	0,003558
194	Т	1	0,003558
195	С	1	0,003558
196	У	1	0,003558
197	Г	1	0,003558
198	Ж	1	0,003558
199	К	1	0,003558
200	З	1	0,003558
201	И	1	0,003558
202	О	1	0,003558
203	А	1	0,003558
204	Н	1	0,003558
205	В	1	0,003558
206	Р	1	0,003558
207	М	1	0,003558
208	Л	1	0,003558
209	Т	1	0,003558
210	С	1	0,003558
211	У	1	0,003558
212	Г	1	0,003558
213	Ж	1	0,003558
214	К	1	0,003558
215	З	1	0,003558
216	И	1	0,003558
217	О	1	0,003558
218	А	1	0,003558
219	Н	1	0,003558
220	В	1	0,003558
221	Р	1	0,003558
222	М	1	0,003558
223	Л	1	0,003558
224	Т	1	0,003558
225	С	1	0,003558
226	У	1	0,003558
227	Г	1	0,003558
228	Ж	1	0,003558
229	К	1	0,003558
230	З	1	0,003558
231	И	1	0,003558
232	О	1	0,003558
233	А	1	0,003558
234	Н	1	0,003558
235	В	1	0,003558
236	Р	1	0,003558
237	М	1	0,003558
238	Л	1	0,003558
239	Т	1	0,003558
240	С	1	0,003558
241	У	1	0,003558
242	Г	1	0,003558
243	Ж	1	0,003558
244	К	1	0,003558
245	З	1	0,003558
246	И	1	0,003558
247	О	1	0,003558
248	А	1	0,003558
249	Н	1	0,003558
250	В	1	0,003558
251	Р	1	0,003558
252	М	1	0,003558
253	Л	1	0,003558
254	Т	1	0,003558
255	С	1	0,003558
256	У	1	0,003558
257	Г	1	0,003558
258	Ж	1	0,003558
259	К	1	0,003558
260	З	1	0,003558
261	И	1	0,003558
262	О	1	0,003558
263	А	1	0,003558
264	Н	1	0,003558
265	В	1	0,003558
266	Р	1	0,003558
267	М	1	0,003558
268	Л	1	0,003558
269	Т	1	0,003558
270	С	1	0,003558
271	У	1	0,003558
272	Г	1	0,003558
273	Ж	1	0,003558
274	К	1	0,003558
275	З	1	0,003558
276	И	1	0,003558
277	О	1	0,003558
278	А	1	0,003558
279	Н	1	0,003558
280	В	1	0,003558
281	Р	1	0,003558
282	М	1	0,003558
283	Л	1	0,003558
284	Т	1	0,003558
285	С	1	0,003558
286	У	1	0,003558
287	Г	1	0,003558
288	Ж	1	0,003558
289	К	1	0,003558
290	З	1	0,003558
291	И	1	0,003558
292	О	1	0,003558
293	А	1	0,003558
294	Н	1	0,003558
295	В	1	0,003558
296	Р	1	0,003558
297	М	1	0,003558
298	Л	1	0,003558
299	Т	1	0,003558
300	С	1	0,003558
301	У	1	0,003558
302	Г	1	0,003558
303	Ж	1	0,003558
304	К	1	0,003558
305	З	1	0,003558
306	И	1	0,003558
307	О	1	0,003558
308	А	1	0,003558
309	Н	1	0,003558
310	В	1	0,003558
311	Р	1	0,003558
312	М	1	0,003558
313	Л	1	0,003558
314	Т	1	0,003558
315	С	1	0,003558
316	У	1	0,003558
317	Г	1	0,003558
318	Ж	1	0,003558
319	К	1	0,003558
320	З	1	0,003558
321	И	1	0,003558
322	О	1	0,003558
323	А	1	0,003558
324	Н	1	0,003558
325	В	1	0,003558
326			

Частотность символов текста, зашифрованного по формуле Цезаря			
	Символ	Код	Частота
1	В	15	0,12238
2	С	25	0,09798
3	М	23	0,08852
4	Х	20	0,08093
5	М	23	0,08093
6	Ъ	17	0,07566
7	О	14	0,06895
8	Ъ	17	0,06876
9	М	23	0,07566
10	В	15	0,07567
11	Р	10	0,07567
12	В	15	0,07567
13	В	15	0,07567
14	Ъ	17	0,07567
15	Ъ	17	0,07567
16	Ъ	17	0,07567
17	Ъ	17	0,07567
18	Ъ	17	0,07567
19	Ъ	17	0,07567
20	Ъ	17	0,07567
21	Ъ	17	0,07567
22	Ъ	17	0,07567
23	Ъ	17	0,07567
24	Ъ	17	0,07567
25	Ъ	17	0,07567
26	Ъ	17	0,07567
27	Ъ	17	0,07567
28	Ъ	17	0,07567
29	Ъ	17	0,07567
30	Ъ	17	0,07567
31	Ъ	17	0,07567
32	Ъ	17	0,07567
33	Ъ	17	0,07567
34	Ъ	17	0,07567
35	Ъ	17	0,07567
36	Ъ	17	0,07567
37	Ъ	17	0,07567
38	Ъ	17	0,07567
39	Ъ	17	0,07567
40	Ъ	17	0,07567
41	Ъ	17	0,07567
42	Ъ	17	0,07567
43	Ъ	17	0,07567
44	Ъ	17	0,07567
45	Ъ	17	0,07567
46	Ъ	17	0,07567
47	Ъ	17	0,07567
48	Ъ	17	0,07567
49	Ъ	17	0,07567
50	Ъ	17	0,07567

Рисунок 10 – Таблица частоты зашифрованного текста



Рисунок 11 – График частотности зашифрованного текста

3.4. Таблица и график частотности зашифрованного текста (шифр 1)

Ниже, на рисунке 12, представлена таблица частотности использования алфавита в зашифрованном тексте в порядке уменьшения, а на рисунке 13, представлен график построенный на основе данной таблицы.

Частотность символов текста, зашифрованного полиалфавитным шифром 1			
	Символ	Кол-во выхождений	Частота
1	З	17	0,05566
2	Ц	15	0,04902
3	Н	14	0,04575
4	В	13	0,04248
5	К	13	0,04248
6	Р	12	0,03922
7	Ы	11	0,03595
8	Ь	10	0,03268
9	Л	10	0,03268
10	Т	9	0,02941
11	М	9	0,02941
12	О	9	0,02941
13	Е	9	0,02941
14	Х	9	0,02941
15	Ш	8	0,02614
16		8	0,02614
17	Щ	8	0,02614
18	П	7	0,02288
19	Ь	7	0,02288
20	И	7	0,02288
21	У	7	0,02288
22	2	7	0,02288
23	9	6	0,01961
24	Ч	6	0,01961
25	Ю	6	0,01961
26	.	6	0,01961
27	6	6	0,01961
28	Н	5	0,01634
29	Ф	5	0,01634
30	Б	5	0,01634
31	4	4	0,01307
32	5	4	0,01307
33	3	4	0,01307
34	И	3	0,00980
35	С	3	0,00980
36	Л	3	0,00980
37	А	3	0,00980
38	Ж	3	0,00980
39	В	3	0,00980
40	8	3	0,00980
41	Г	3	0,00980
42	7	2	0,00654
43	.	2	0,00654
44	1	1	0,00327
45	9	1	0,00327
46	Ё	0	0,00000
			Сумма
			1

Рисунок 12 – Таблица частоты зашифрованного текста



Рисунок 13 – График частотности зашифрованного текста

4. Заключение

В ходе выполнения данной практической работы было реализован полиалфавитный шифр на основе квадрата Виженера, 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 и полиалфавитного шифров, в результате чего выяснилось, что последний обладает большей криптостойкостью. Получены навыки в работе с полиалфавитными шифрами в Excel.