Российский университет транспорта (МИИТ)

Институт транспортной техники и систем управления

Кафедра «Управление и защита информации»

Отчет

по практическому заданию

по теме «Разработка многоалфавитного шифра замены»

по дисциплине

«Криптографические методы защиты информации»

Выполнил:

студент группы ТКИ-341

Порхун Д.Д.

Проверил:

Доцент кафедры УиЗИ к.т.н., с.н.с.

Михалевич И.Ф.

Москва 2023

Оглавление

ЗАДАНИЕ

- Разработать моноалфавитный шифр, таблицы шифрования / расшифрования (для варианта шифра);
- Подготовить сообщение (конкатенация 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

Сообщение инициатора:	уважаемый игорь феодосьевич, получил отправленные вами данные, ознакомлюсь и выскажу окончательное решение , с уважением 02.08.2002 порхун димитрий дмитриевич.
Сообщение отвечика:	уважаемый порхун димитрий, безмерно рад нашему сотрудничеству, надеюсь на его дальнейшее успешное и взаимовыгодное развитие, с уважением игорь феодосьевич.

Алфавит	"	,	.	>	<	+	-	=	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	0	1	2	3	4	5	6	7	8	9	
Номер символа алфавита	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	46	47	48	49	50	51
Шифр	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	0	1	2	3	4	5	6	/	8	9		"	,	.	>	<	+	-	=	а	б	в	г	д
Ключ	13																																																				

1. Краткие теоритические сведения по шифру цезаря

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, ...).

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

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

Мощность алфавита – полное число символов алфавита

Мощность алфавита (в общем случае): -русского языка -33-английского – 26Алфавит может дополнительно включать цифры, знаки препинания, специальные символы

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.

Запись алгоритма шифрования (общего):

$$E\_k, k \in K\_ED: M \to C,$$

$$D\_k, k \in K\_ED: C \to M,$$

$$\forall k \in K\_E \exists k \in K\_(D,)$$

$$\forall m \in M: E\_k\ (m) \in c,$$

$$\forall c \in C: D\_k\ (c) \in m,$$

Моноалфавитныйшифр:

$$C\_i = M\_i + K\ mod\ n$$

$$M\_i = C\_i - K\ mod\ n$$

K – ключ, $0 < K \leq$ n ;

n – мощность алфавита.

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

C_i – символ на i – ой позиции криптограммы.

Шифр Цезаря – метод создания просто моноалфавитного шифра на основе ключа с остоянным параметром сдвига на K символов.

$$E: C_i = M_i + K\ mod\ n$$

$$D: M_i = C_i - K\ mod\ n$$

i – позиция символа в алфаите шифра;

M_i, C_i – исходный и зашифрованные символы;

K – параметр сдвига (ключ);

N – мощность алфавита.

2. Блокнот с алфавитом

"
,
.
>
<
+
-
=
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
0
1
2
3
4
5
6
7
8
9

3. Шифрование исходного текста

3.1. Исходный текст

Длина конкатенация сообщений инициатора и ответчика:	314	Ключ:	13
Конкатенация сообщений:			
уважаемый игорь феодосьевич, получил отправленные вами данные, ознакомлюсь и выскажу окончательное решение , с уважением 02.08.2002 порхун димитрий дмитриевич.уважаемый порхун димитрий, безмерно рад нашему сотрудничеству, надеюсь на его дальнейшее успешное и взаимовыгодное развитие, с уважением игорь феодосьевич.			

Номер символа в алфавите после сдвига	ЕСЛИ(ПОИСКПОЗ(значение симлова строки;Алфавит;0)+ключ>51;ПОИСКПОЗ(значение симлова

3.2. Шифрование

Номер символа строки	Символ строки	Номер символа в алфавите после сдвига	Новый символ	Номер символа строки	Символ строки	Номер символа в алфавите после сдвига	Новый символ
1	у	41	0	158	ч	45	4
2	в	24	п	159	.	16	з
3	а	22	н	160	у	41	0
4	ж	28	у	161	в	24	п
5	а	22	н	162	а	22	н
6	е	27	т	163	ж	28	у
7	м	34	щ	164	а	22	н
8	ы	49	8	165	е	27	т
9	й	31	ц	166	м	34	щ
10		13	д	167	ы	49	8
11	и	30	х	168	й	31	ц
12	г	25	р	169		13	д
13	о	36	ы	170	п	37	ь
14	р	38	э	171	о	36	ы
15	ь	50	9	172	р	38	э
16		13	д	173	х	43	2
17	ф	42	1	174	у	41	0
18	е	27	т	175	н	35	ъ
19	о	36	ы	176		13	д
20	д	26	с	177	д	26	с
21	о	36	ы	178	и	30	х
22	с	39	ю	179	м	34	щ
23	ь	50	9	180	и	30	х
24	е	27	т	181	т	40	я
25	в	24	п	182	р	38	э
26	и	30	х	183	и	30	х
27	ч	45	4	184	й	31	ц
28	,	15	ж	185	,	15	ж
29		13	д	186		13	д
30	п	37	ь	187	б	23	о
31	о	36	ы	188	е	27	т
32	л	33	ш	189	з	29	ф
33	у	41	0	190	м	34	щ
34	ч	45	4	191	е	27	т
35	и	30	х	192	р	38	э
36	л	33	ш	193	н	35	ъ
37		13	д	194	о	36	ы
38	о	36	ы	195		13	д
39	т	40	я	196	р	38	э
40	п	37	ь	197	а	22	н
41	р	38	э	198	д	26	с
42	а	22	н	199		13	д
43	в	24	п	200	н	35	ъ
44	л	33	ш	201	а	22	н
45	е	27	т	202	ш	46	5
46	н	35	ъ	203	е	27	т
47	н	35	ъ	204	м	34	щ

48	ы	49	8
49	е	27	т
50		13	д
51	в	24	п
52	а	22	н
53	м	34	щ
54	и	30	х
55		13	д
56	д	26	с
57	а	22	н
58	н	35	ъ
59	н	35	ъ
60	ы	49	8
61	е	27	т
62	,	15	ж
63		13	д
64	о	36	ы
65	з	29	ф
66	н	35	ъ
67	а	22	н
68	к	32	ч
69	о	36	ы
70	м	34	щ
71	л	33	ш
72	ю	1	"
73	с	39	ю
74	ь	50	9
75		13	д
76	и	30	х
77		13	д
78	в	24	п
79	ы	49	8
80	с	39	ю
81	к	32	ч
82	а	22	н
83	ж	28	у
84	у	41	0
85		13	д
86	о	36	ы
87	к	32	ч
88	о	36	ы
89	н	35	ъ
90	ч	45	4
91	а	22	н
92	т	40	я
93	е	27	т
94	л	33	ш
95	ь	50	9
96	н	35	ъ
97	о	36	ы
98	е	27	т
99		13	д
100	р	38	э

205	у	41	0
206		13	д
207	с	39	ю
208	о	36	ы
209	т	40	я
210	р	38	э
211	у	41	0
212	д	26	с
213	н	35	ъ
214	и	30	х
215	ч	45	4
216	е	27	т
217	с	39	ю
218	т	40	я
219	в	24	п
220	у	41	0
221	,	15	ж
222		13	д
223	н	35	ъ
224	а	22	н
225	д	26	с
226	е	27	т
227	ю	1	"
228	с	39	ю
229	ь	50	9
230		13	д
231	н	35	ъ
232	а	22	н
233		13	д
234	е	27	т
235	г	25	р
236	о	36	ы
237		13	д
238	д	26	с
239	а	22	н
240	л	33	ш
241	ь	50	9
242	н	35	ъ
243	е	27	т
244	й	31	ц
245	ш	46	5
246	е	27	т
247	е	27	т
248		13	д
249	у	41	0
250	с	39	ю
251	п	37	ь
252	е	27	т
253	ш	46	5
254	н	35	ъ
255	о	36	ы
256	е	27	т
257		13	д

101	е	27	т
102	ш	46	5
103	е	27	т
104	н	35	ъ
105	и	30	х
106	е	27	т
107		13	д
108	,	15	ж
109		13	д
110	с	39	ю
111		13	д
112	у	41	0
113	в	24	п
114	а	22	н
115	ж	28	у
116	е	27	т
117	н	35	ъ
118	и	30	х
119	е	27	т
120	м	34	щ
121		13	д
122	0	3	.
123	2	5	<
124	.	16	з
125	0	3	.
126	8	11	в
127	.	16	з
128	2	5	<
129	0	3	.
130	0	3	.
131	2	5	<
132		13	д
133	п	37	ь
134	о	36	ы
135	р	38	э
136	х	43	2
137	у	41	0
138	н	35	ъ
139		13	д
140	д	26	с
141	и	30	х
142	м	34	щ
143	и	30	х
144	т	40	я
145	р	38	э
146	и	30	х
147	й	31	ц
148		13	д
149	д	26	с
150	м	34	щ
151	и	30	х
152	т	40	я
153	р	38	э
154	и	30	х

258	и	30	х
259		13	д
260	в	24	п
261	з	29	ф
262	а	22	н
263	и	30	х
264	м	34	щ
265	о	36	ы
266	в	24	п
267	ы	49	8
268	г	25	р
269	о	36	ы
270	д	26	с
271	н	35	ъ
272	о	36	ы
273	е	27	т
274		13	д
275	р	38	э
276	а	22	н
277	з	29	ф
278	в	24	п
279	и	30	х
280	т	40	я
281	и	30	х
282	е	27	т
283	,	15	ж
284		13	д
285	с	39	ю
286		13	д
287	у	41	0
288	в	24	п
289	а	22	н
290	ж	28	у
291	е	27	т
292	н	35	ъ
293	и	30	х
294	е	27	т
295	м	34	щ
296		13	д
297	и	30	х
298	г	25	р
299	о	36	ы
300	р	38	э
301	ь	50	9
302		13	д
303	ф	42	1
304	е	27	т
305	о	36	ы
306	д	26	с
307	о	36	ы
308	с	39	ю
309	ь	50	9
310	е	27	т
311	в	24	п

155	е	27	т	312	и	30	х
156	в	24	п	313	ч	45	4
157	и	30	х	314	.	16	з

3.3. Зашифрованный текст

Зашифрованная строка:
0пнунтщ8цдхрыэ9д1тысыю9тпх4ждьыш04хшдыяьэнпштъъ8тдпнщхдснъъ8тждыфънчыщш"ю9дхдп8ючну0дычыъ4нятш 9ъытдэт5тъхтдждюд0пнутъхтщд.<з.вз<..<дьыэ20ъдсхщхяэхцдсщхяэхтпх4з0пнунтщ8цдьыэ20ъдсхщхяэхцждотфщтэъыдэ нсдън5тщ0дюыяэ0съх4тюяп0ждънст"ю9дъндтрыдснш9ътц5ттд0юьт5ъытдхдпфнхщып8рысъытдэнфпхяхтждюд0пнутъхт щдхрыэ9д1тысыю9тпх4з

4. Расшифровка текста

4.1. Исходный текст

Зашифрованная строка:	0пнунтщ8цдхрыэ9д1тысыю9тпх4ждьыш04хшдыяьэнпштъъ8тдпнщхдснъъ8тждыфънчыщш"ю9дхдп8ючну0дычыъ4нятш 9ъытдэт5тъхтджджюд0пнутъхтщд.<з.вз<..<дьыэ20ъдсхщхяэхцдсщхяэхтпх4з0пнунтщ8цдьыэ20ъдсхщхяэхцждотфщтэъыдэ нсдън5тщ0дюыяэ0съх4тюяп0ждънст"ю9дъндтрыдснш9ътц5ттд0юьт5ъытдхдпфнхщып8рысъытдэнфпхяхтждюд0пнутъхт щдхрыэ9д1тысыю9тпх4з	
	ключ	13

Номер расшифрованного символа в алфавите	ЕСЛИ(ПОИСКПОЗ(зашифрованный симлов;Алфавит;0)- ключ<=0;ПОИСКПОЗ(зашифрованный симлов;Алфавит;0)- ключ+51;ПОИСКПОЗ(зашифрованный симлов;Алфавит;0)- ключ)

4.2. Расшифрование

Номер символа зашифрованной строки	Зашифрованный символ	Номер зашифрованного символа в алфавите	Номер расшифрованного символа в алфавите	Расшифрованный символ
1	0	41	28	у
2	п	24	11	в
3	н	22	9	а
4	у	28	15	ж
5	н	22	9	а
6	т	27	14	е
7	щ	34	21	м
8	8	49	36	ы
9	ц	31	18	й
10	д	13	51	
11	х	30	17	и
12	р	25	12	г
13	ы	36	23	о
14	э	38	25	р
15	9	50	37	ь
16	д	13	51	
17	1	42	29	ф
18	т	27	14	е
19	ы	36	23	о
20	с	26	13	д
21	ы	36	23	о
22	ю	39	26	с
23	9	50	37	ь
24	т	27	14	е
25	п	24	11	в
26	х	30	17	и
27	4	45	32	ч
28	ж	15	2	,
29	д	13	51	
30	ь	37	24	п
31	ы	36	23	о
32	ш	33	20	л
33	0	41	28	у
34	4	45	32	ч
35	х	30	17	и
36	ш	33	20	л
37	д	13	51	
38	ы	36	23	о
39	я	40	27	т
40	ь	37	24	п
41	э	38	25	р
42	н	22	9	а
43	п	24	11	в
44	ш	33	20	л
45	т	27	14	е
46	ъ	35	22	н
47	ъ	35	22	н
48	8	49	36	ы
158	4	45	32	ч
159	з	16	3	.
160	0	41	28	у
161	п	24	11	в
162	н	22	9	а
163	у	28	15	ж
164	н	22	9	а
165	т	27	14	е
166	щ	34	21	м
167	8	49	36	ы
168	ц	31	18	й
169	д	13	51	
170	ь	37	24	п
171	ы	36	23	о
172	э	38	25	р
173	2	43	30	х
174	0	41	28	у
175	ъ	35	22	н
176	д	13	51	
177	с	26	13	д
178	х	30	17	и
179	щ	34	21	м
180	х	30	17	и
181	я	40	27	т
182	э	38	25	р
183	х	30	17	и
184	ц	31	18	й
185	ж	15	2	,
186	д	13	51	
187	о	23	10	б
188	т	27	14	е
189	ф	29	16	з
190	щ	34	21	м
191	т	27	14	е
192	э	38	25	р
193	ъ	35	22	н
194	ы	36	23	о
195	д	13	51	
196	э	38	25	р
197	н	22	9	а
198	с	26	13	д
199	д	13	51	
200	ъ	35	22	н
201	н	22	9	а
202	5	46	33	ш
203	т	27	14	е
204	щ	34	21	м
205	0	41	28	у

49	т	27	14	е
50	д	13	51	
51	п	24	11	в
52	н	22	9	а
53	щ	34	21	м
54	х	30	17	и
55	д	13	51	
56	с	26	13	д
57	н	22	9	а
58	ъ	35	22	н
59	ъ	35	22	н
60	8	49	36	ы
61	т	27	14	е
62	ж	15	2	,
63	д	13	51	
64	ы	36	23	о
65	ф	29	16	з
66	ъ	35	22	н
67	н	22	9	а
68	ч	32	19	к
69	ы	36	23	о
70	щ	34	21	м
71	ш	33	20	л
72	"	1	39	ю
73	ю	39	26	с
74	9	50	37	ь
75	д	13	51	
76	х	30	17	и
77	д	13	51	
78	п	24	11	в
79	8	49	36	ы
80	ю	39	26	с
81	ч	32	19	к
82	н	22	9	а
83	у	28	15	ж
84	0	41	28	у
85	д	13	51	
86	ы	36	23	о
87	ч	32	19	к
88	ы	36	23	о
89	ъ	35	22	н
90	4	45	32	ч
91	н	22	9	а
92	я	40	27	т
93	т	27	14	е
94	ш	33	20	л
95	9	50	37	ь
96	ъ	35	22	н
97	ы	36	23	о
98	т	27	14	е
99	д	13	51	
100	э	38	25	р
101	т	27	14	е
102	5	46	33	ш
103	т	27	14	е

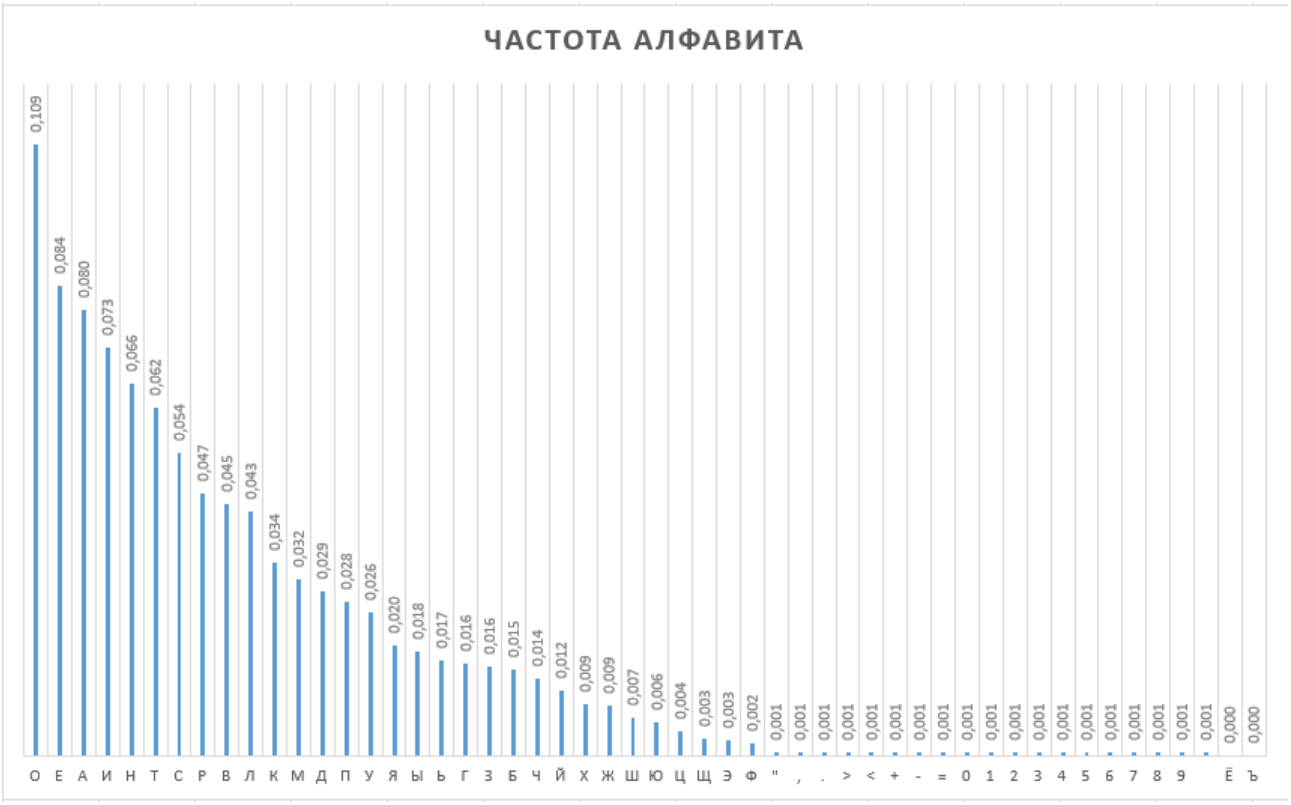
206	д	13	51	
207	ю	39	26	с
208	ы	36	23	о
209	я	40	27	т
210	э	38	25	р
211	0	41	28	у
212	с	26	13	д
213	ъ	35	22	н
214	х	30	17	и
215	4	45	32	ч
216	т	27	14	е
217	ю	39	26	с
218	я	40	27	т
219	п	24	11	в
220	0	41	28	у
221	ж	15	2	,
222	д	13	51	
223	ъ	35	22	н
224	н	22	9	а
225	с	26	13	д
226	т	27	14	е
227	"	1	39	ю
228	ю	39	26	с
229	9	50	37	ь
230	д	13	51	
231	ъ	35	22	н
232	н	22	9	а
233	д	13	51	
234	т	27	14	е
235	р	25	12	г
236	ы	36	23	о
237	д	13	51	
238	с	26	13	д
239	н	22	9	а
240	ш	33	20	л
241	9	50	37	ь
242	ъ	35	22	н
243	т	27	14	е
244	ц	31	18	й
245	5	46	33	ш
246	т	27	14	е
247	т	27	14	е
248	д	13	51	
249	0	41	28	у
250	ю	39	26	с
251	ь	37	24	п
252	т	27	14	е
253	5	46	33	ш
254	ъ	35	22	н
255	ы	36	23	о
256	т	27	14	е
257	д	13	51	
258	х	30	17	и
259	д	13	51	
260	п	24	11	в

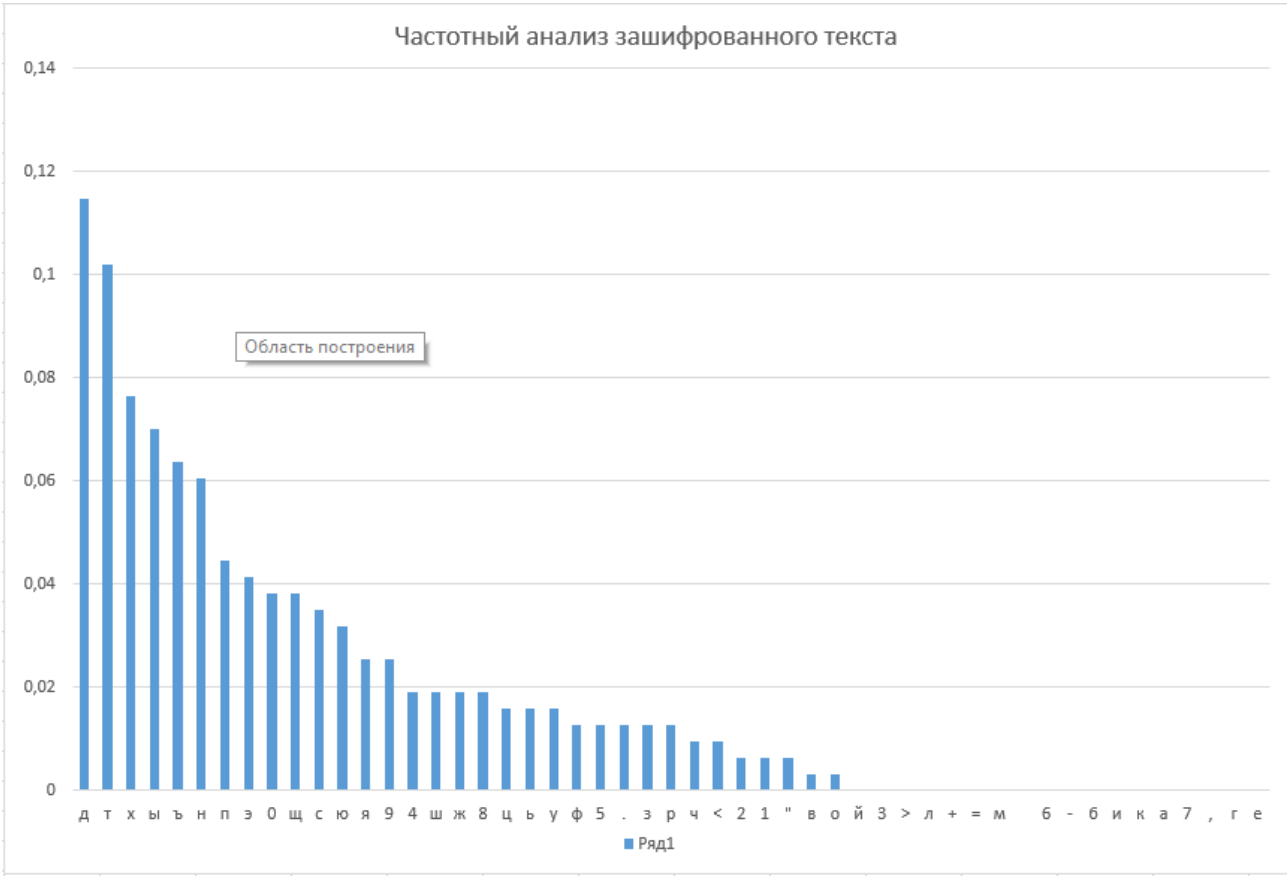
103	т	27	14	е
104	ъ	35	22	н
105	х	30	17	и
106	т	27	14	е
107	д	13	51	
108	ж	15	2	,
109	д	13	51	
110	ю	39	26	с
111	д	13	51	
112	0	41	28	у
113	п	24	11	в
114	н	22	9	а
115	у	28	15	ж
116	т	27	14	е
117	ъ	35	22	н
118	х	30	17	и
119	т	27	14	е
120	щ	34	21	м
121	д	13	51	
122	.	3	41	0
123	<	5	43	2
124	з	16	3	.
125	.	3	41	0
126	в	11	49	8
127	з	16	3	.
128	<	5	43	2
129	.	3	41	0
130	.	3	41	0
131	<	5	43	2
132	д	13	51	
133	ь	37	24	п
134	ы	36	23	о
135	э	38	25	р
136	2	43	30	х
137	0	41	28	у
138	ъ	35	22	н
139	д	13	51	
140	с	26	13	д
141	х	30	17	и
142	щ	34	21	м
143	х	30	17	и
144	я	40	27	т
145	э	38	25	р
146	х	30	17	и
147	ц	31	18	й
148	д	13	51	
149	с	26	13	д
150	щ	34	21	м
151	х	30	17	и
152	я	40	27	т
153	э	38	25	р
154	х	30	17	и
155	т	27	14	е
156	п	24	11	в
157	х	30	17	и
260	п	24	11	в
261	ф	29	16	з
262	н	22	9	а
263	х	30	17	и
264	щ	34	21	м
265	ы	36	23	о
266	п	24	11	в
267	8	49	36	ы
268	р	25	12	г
269	ы	36	23	о
270	с	26	13	д
271	ъ	35	22	н
272	ы	36	23	о
273	т	27	14	е
274	д	13	51	
275	э	38	25	р
276	н	22	9	а
277	ф	29	16	з
278	п	24	11	в
279	х	30	17	и
280	я	40	27	т
281	х	30	17	и
282	т	27	14	е
283	ж	15	2	,
284	д	13	51	
285	ю	39	26	с
286	д	13	51	
287	0	41	28	у
288	п	24	11	в
289	н	22	9	а
290	у	28	15	ж
291	т	27	14	е
292	ъ	35	22	н
293	х	30	17	и
294	т	27	14	е
295	щ	34	21	м
296	д	13	51	
297	х	30	17	и
298	р	25	12	г
299	ы	36	23	о
300	э	38	25	р
301	9	50	37	ь
302	д	13	51	
303	1	42	29	ф
304	т	27	14	е
305	ы	36	23	о
306	с	26	13	д
307	ы	36	23	о
308	ю	39	26	с
309	9	50	37	ь
310	т	27	14	е
311	п	24	11	в
312	х	30	17	и
313	4	45	32	ч
314	з	16	3	.

4.3. Расшифрованный текст

Расшифрованная строка:	уважаемый игорь феодосьевич, получил отправленные вами данные, ознакомлюсь и выскажу окончательное решение , с уважением 02.08.2002 порхун димитрий дмитриевич.уважаемый порхун димитрий, безмерно рад нашему сотрудничеству, надеюсь на его дальнейшее успешное и взаимовыгодное развитие, с уважением игорь феодосьевич.

5. Анализ слабостей шифра цезаря





ЗАКЛЮЧЕНИЕ

В ходе решения практического задания реализован шифр Цезаря. Шифр Цезаря – достаточно простой в реализации шифр, однако он подвержен простому перебору, так как существует малое количество ключей, а также уязвим для частотного анализа текста.