Лабораторная работа №16
Моделирование работы шифра гаммирования

1. Цель работы

Освоить порядок моделирования криптосистемы с помощью программы Multisim 11.0.2.

2. Общие сведения

При шифровании с помощью шифра гаммирования вначале каждую букву открытого текста преобразуют в число. Затем к каждому числу прибавляют секретную псевдослучайную числовую последовательность (гамму). По этой причине такой шифр порой называют **аддитивным шифром**.

При описании этого шифра авторы используют термины типа: суммирование, прибавление, добавление… Нужно чётко помнить, что в классическом шифре гаммирования слияние (соединение, трансформация) символов открытого текста и символов гаммы осуществляется с помощью логической операции Исключающее ИЛИ.

Слияние символов гаммы и символов открытого текста осуществляется поразрядно. Процедуру прибавления гаммы к открытому тексту удобно реализовать с помощью двоичных чисел. При этом на каждый бит открытого текста накладывается бит секретной гаммы. Понятно, что гамма должна быть известна на передающей и приёмной сторонах.

Рассмотрим детальнее процедуру шифрования методом гаммирования. При формировании гаммы генератор формирует псевдослучайную последовательность битов: $\gamma_1, \gamma_2, \gamma_3, \ldots, \gamma_n$. Этот поток битов и поток битов открытого текста $p_1, p_2, p_3, \ldots, p_n$ подвергаются поразрядно логической операции Исключающее ИЛИ. В результате получается поток битов криптограммы:

$$c_i = p_i \oplus \gamma_i.$$

При расшифровании криптограммы на приёмной стороне операция Исключающее ИЛИ выполняется над битами поступившей криптограммы и тем же самым потоком гаммы:

$$p_i = c_i \oplus \gamma_i.$$

Благодаря особенностям логической операции Исключающее ИЛИ на приёмной стороне операция вычитания заменяется логической операцией Исключающее ИЛИ. Сказанное иллюстрируем примером.

Предположим, что открытый текст P = 10011001, а гамма G = 11001110. В результате шифрования на передающей стороне криптограмма C будет иметь следующий вид:

P	1	0	0	1	1	0	0	1
G	1	1	0	0	1	1	1	0
C	0	1	0	1	0	1	1	1

На приёмной стороне над криптограммой и гаммой повторно выполняется логическая операция Исключающее ИЛИ:

C	0	1	0	1	0	1	1	1
G	1	1	0	0	1	1	1	0
P`	1	0	0	1	1	0	0	1

Из этих таблиц видно, что переданный и принятый байты одинаковые.

В ЭВМ преобразование открытого текста в числа происходит естественным путём, так как каждый символ при вводе с клавиатуры кодируется двоичным числом. Для определённости будем считать, что сообщение в ЭВМ кодируется с помощью кодовой таблицы СР-1251. Результаты всех преобразований поместим в таблицу.

Открытый текст	Г	Д	Е	А	Б	Б	А
Десятичное число	195	196	197	192	193	193	192
Двоичное число	11000011	11000100	11000101	11000000	11000001	11000001	11000000
Гамма (десятич.)	32	18	36	11	61	23	3
Гамма (двоич.)	00100000	00010010	00100100	00001011	00111101	00010111	00000011
Криптогр. (двоич.)	11100011	11010110	11100001	11001011	11111100	11010110	11000011
Криптогр. (десят.)	227	214	225	203	252	214	195
Криптограмма	г	Ц	б	Л	ь	Ц	Г

Для наглядности результат шифрования переведён с помощью таблицы СР-1251 в буквы. Из таблицы видно, что открытый текст был записан прописными буквами, а криптограмма содержит как прописные, так и строчные буквы. Очевидно, что если все значения гаммы равны нулю, то в линию будет передан открытый текст. Если же все значения разрядов гаммы равны единицам, то в линию поступит инвертированный открытый текст.

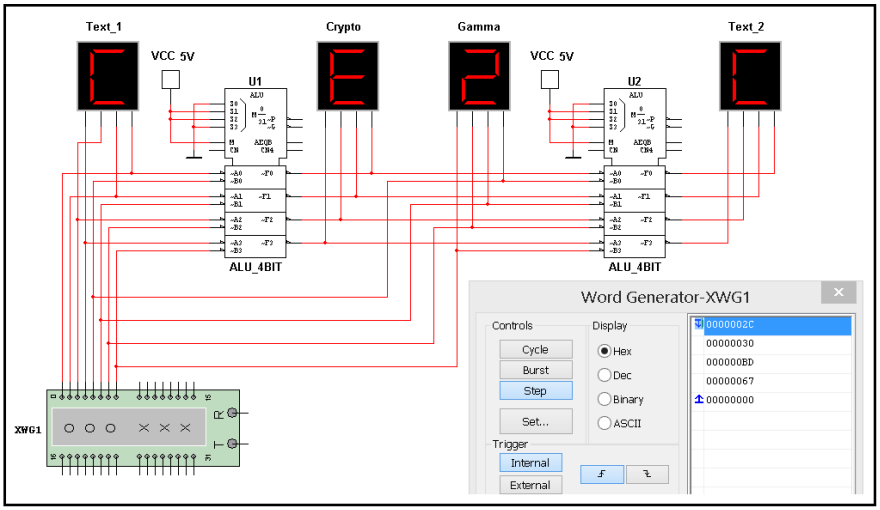
Следует запомнить.

Недопустимо в реальных криптосистемах повторно использовать гамму для шифрования нового текста. Число символов гаммы должно быть не меньше числа символов открытого текста, то есть нельзя циклически повторять гамму.

3. Задания на выполнение лабораторной работы

3.1. Задание 1. Исследование шифра гаммирования

Выполнить моделирование криптосистемы, которая базируется на шифре гаммирования. Принципиальная схема криптосистемы показана на рисунке. Значения открытого текста и гаммы нужно записать в Word Generator. Содержимое Генератора слов (Word Generator XWG1), показанное на рисунке, соответствует варианту 17.



Исходные данные в шестнадцатеричной СС для моделирования и расчётов приведены в таблице.

Таблица 3.1.1

Вар.	Открытый текст	Гамма	Вар.	Открытый текст	Гамма
1	CAFÉ1945	1bA617E7	9	OdA2bAC9	914FbAC9
2	AbbA1812	29FE18db	10	C0d3dACA	10A5AA09
3	bAbA3141	3Cd419EA	11	6AC4E2E4	11FdAA48
4	dEdAC0d4	41F920A3	12	EdA5CAdA	12CdAdA5
5	bEdAC0d5	579A21Fd	13	AbCdA137	13F4dAdA
6	6A6AC0d6	6dbA22dA	14	AdE52008	14AdbdAC
7	COOC2009	78bdAb38	15	EA431917	15FAEAE7
8	6OOC2012	8AEF10bd	16	22061941	dAEE16b9
			17	**C0d7**	**23b6**

Несложно заметить, что шестнадцатеричные числа в таблице 3.1.1 записаны прописными и строчными буквами. Это связано с особенностью конструкции семисегментного индикатора (см. схему исследований), который не позволяет представить все шестнадцатеричные числа заглавными буквами.

Кроме моделирования криптосистемы в программе Multisim в этом задании нужно выполнить ручной расчёт, используя те же исходные данные.

3.2. Задание 2. Оценка влияния состава гаммы на криптограмму

Повторить исследования, описанные в предыдущем задании, взяв одинаковые для всех вариантов значения гаммы 0000FFFF. Открытый текст берётся из таблицы 3.1.1. Провести анализ сформированной криптограммы, дать комментарии. Обратить внимание на имеющиеся закономерности, просматривающиеся при сравнении открытого текста и криптограммы.

3.3. Задание 3. Оценка влияния длины гаммы на криптостойкость

Выполнить моделирование криптосистемы, взяв одинаковые для всех вариантов значения гаммы 7A7A7A7A. Открытый текст должен состоять из восьми символов, равных номеру варианта (шестнадцатеричная система счисления). Провести анализ полученных результатов, дать комментарии.

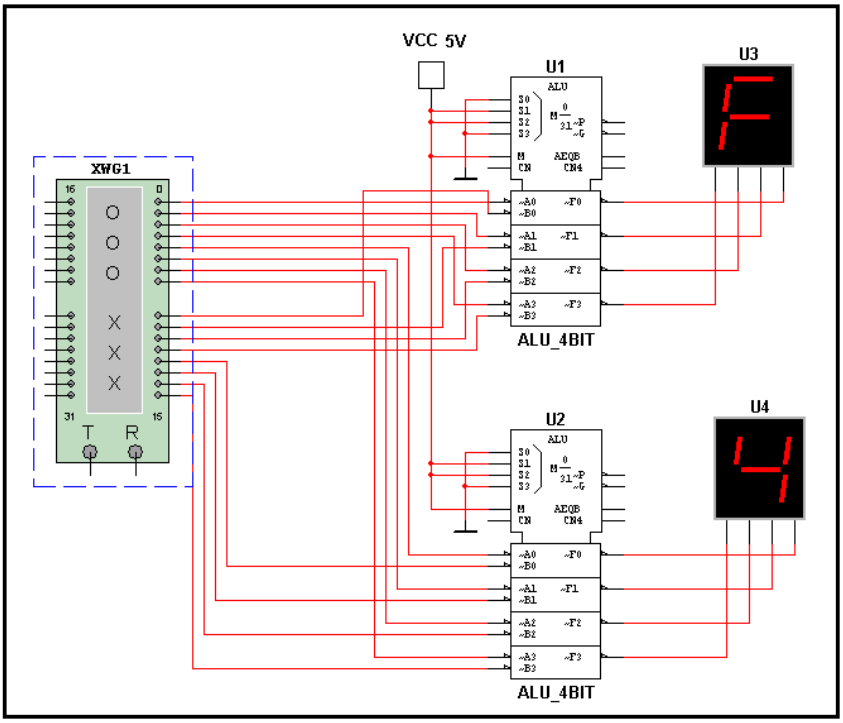
Обратить внимание на имеющиеся закономерности, проявляющиеся при сравнении открытого текста и криптограммы.

3.4. Задание 4. Дешифрирование криптограммы

С помощью криптосистемы, схема которой показана на рисунке, расшифровать криптограмму (см. таблицу).

Таблица 3.4.1

Вар	Крипто-грамма	Гамма	Вар	Крипто-грамма	Гамма
1	D748E615	1BA617E7	9	D720C8AD	914FBAC9
2	6F976ABE	29FE18DB	10	52C9DF6C	10A5AA09
3	8E24F707	3CD419EA	11	A11840A8	11FDAA48
4	8A11D151	41F920A3	12	55A8C1C7	12CDADA5
5	9072CD1D	579A21FD	13	D8112834	13F4DADA
6	25DB57A9	6DBA22DA	14	43C8D4C2	14ADBDAC
7	BB4D45D4	78BDAB38	15	42959883	15FAEAE7
8	CE9D75D4	8AEF10BD	16	1500FD5C	DAEE16B9
			17	**ADDD9524**	**1D2E78CA**



Криптосистема содержит два АЛУ, которые позволяют зашифровать и расшифровать восьмиразрядные символы. Младшие четыре бита криптограммы отображаются на индикаторе U3, а старшая тетрада индицируется на U4.

Открытый текст и гамма размещаются в Генераторе Слов. Открытый текст подаётся на шины A, гамма на шины B арифметико-логических устройств.

Полученные после расшифрования шестнадцатеричные значения открытого текста нужно заменить четырьмя. Для этого следует использовать таблицу СР-1251 (см. Приложение 1).

4. Порядок выполнения лабораторной работы

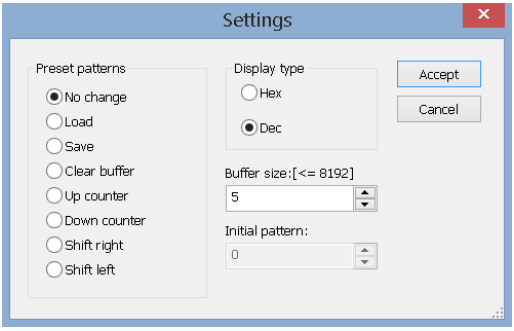
4.1. Методические указания к заданию 3.1

Результаты моделирования и ручных расчётов нужно поместить в таблицу, форма которой приведена ниже. В таблице в качестве примера содержатся результаты моделирования криптосистемы для варианта 17.

Таблица 4.1.1

Данные	Символы							
	1	2	3	4	5	6	7	8
Открытый текст (шестнадцатеричный)	C	0	d	7				
Открытый текст (двоичный)	1100	0000	1101	0111				
Гамма (шестнадцатеричная)	2	3	b	6				
Гамма (двоичная)	0010	0011	1011	0110				
Криптограмма (двоичная, расчёт)	1110	0011	0110	0001				
Криптограмма (моделирование)	E	3	6	1				

Числа открытого текста и гаммы формируются с помощью Генератора слов (Word Generator XWG1). Настройки Генератора, показанные на схеме, соответствуют варианту 17. В остальных вариантах число используемых строк в буфере памяти равно 8. Изменяется объём буфера (число машинных слов) с помощью списка **Buffer size**, который находится в диалоговом окне **Settings**. При выполнении своего задания эту величину нужно увеличить до 8.



Четыре цифровых индикатора на схеме исследований отображают значения передаваемого и принимаемого символов, гаммы и криптограммы.

С помощью управляющих сигналов:

$$S_0 = 0, S_1 = 1, S_2 = 1, S_3 = 0, M = 1$$

оба АЛУ устанавливаются в режим выполнения логической операции Исключающее ИЛИ.

Моделирование криптосистемы ведётся в пошаговом режиме (за счёт многократных щелчков по кнопке **Step…**).

4.2. Методические указания к заданию 3.2

Данное задание выполняется аналогично предыдущему. Отличие заключается в том, что значения гаммы устанавливаются одинаковыми для всех вариантов 0000FFFF.

Наибольшее внимание нужно уделить сравнению криптограммы и открытого текста при различных значениях гаммы.

4.3. Методические указания к заданию 3.3

Данное задание выполняется путём моделирования работы криптосистемы. Значения гаммы устанавливаются одинаковыми для всех вариантов 7A7A7A7A, а значения всех восьми символов открытого текста устанавливаются равными номеру варианта в шестнадцатеричной СС. В таблице открытый текст соответствует варианту 15.

По результатам моделирования нужно заполнить следующую таблицу.

Таблица 4.3.1

Данные	Символы							
	1	2	3	4	5	6	7	8
Открытый текст (шестнадцатеричный)	F	F	F	F	F	F	F	F
Гамма (шестнадцатеричная)	**7**	**A**	**7**	**A**	**7**	**A**	**7**	**A**
Криптограмма (шестнадцатеричная)								

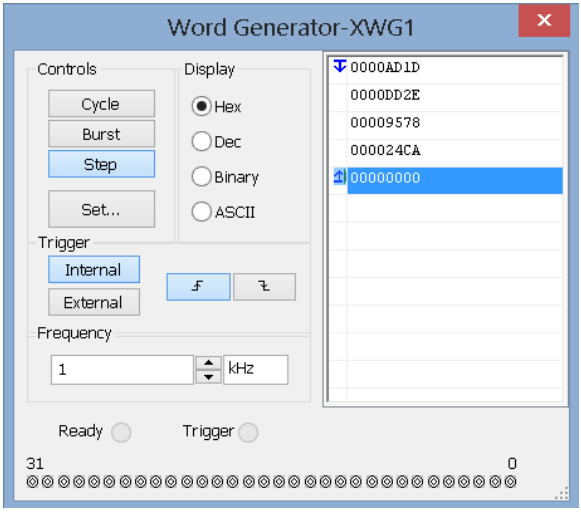
4.4. Методические указания к заданию 3.4

Результаты моделирования следует поместить в таблицу, форма которой приведена ниже. Заданные значения криптограммы и гаммы нужно разбить на пары шестнадцатеричных чисел. В таблице содержатся результаты расшифрования криптограммы для варианта 17.

Таблица 4.4.1

Шестнадцатеричная СС			Открытый текст СР-1251
Крипто-грамма	Гамма	Открытый текст	
AD	1D	B0	Р
DD	2E	F3	у
95	78	ED	н
24	CA	EE	о

На следующем рисунке показан пример заполнения полей Word Generator для варианта 17.



При записи результатов моделирования нужно помнить, что индикатор U3 отображает младшие четыре бита, а U4 – старшие четыре бита расшифрованного текста.

5. Требования к отчёту

Отчёт подготавливается в электронном виде. Он должен содержать постановки задач, скриншоты, которые показывают порядок решения задач, схемы, таблицы с результатами моделирования, результаты расшифрования криптограммы, необходимые комментарии и анализ полученных результатов.

6. Контрольные вопросы

6.1. В чём состоит основная идея шифрования методом гаммирования?
6.2. Какое второе название шифра гаммирования?
6.3. Составьте таблицу истинности для логической функции Исключающее ИЛИ.
6.4. Перечислите системы моделирования радиоэлектронных устройств.
6.5. Перечислите классические методы шифрования.
6.6. Какие требования предъявляются к гамме?
6.7. Как преобразовать десятичное число в двоичное?
6.8. Как преобразовать двоичное число в десятичное?
6.9. Как преобразовать двоичное число в шестнадцатеричное?
6.10. Можно ли одну и ту же гамму использовать для шифрования разных открытых текстов?
6.11. Известны ли Вам примеры неверного промышленного использования метода гаммирования?
6.12. В чём состоит принципиальное различие между криптографией и стеганографией?
6.13. Чем отличаются двоичные коды строчных и прописных букв кодовой таблицы CP-1251?

7. Список литературы

1. Алексеев А.П. Информатика 2015 [Текст]: учеб. пособие/ Алексеев А.П. – М: СОЛОН-Пресс, 2015. – 400 с. ISBN 978-5-91359-158-6.
2. Алексеев А.П. Информатика для криптоаналитиков: учебное пособие/ Алексеев А.П. – Самара: ИУНЛ ПГУТИ, 2015. – 376 с. ISBN 978-5-904029-53-1.
3. Алексеев А.П. Сборник задач по дисциплине «Информатика» для ВУЗов: учебное пособие// Алексеев А.П. – М: СОЛОН-Пресс, 2016. – 104 с. ISBN 978-5-91359-170-8.

Приложение 1. Таблица CP-1251

Десятичная СС	Двоичная СС	Шестнадцате-ричная СС	Символ, команда
0	00000000	00	Ноль
1	00000001	01	Начало заголовка
2	00000010	02	Начало текста
3	00000011	03	Конец текста
4	00000100	04	Конец передачи
5	00000101	05	Запрос
6	00000110	06	Подтверждение приёма
7	00000111	07	Звуковой сигнал
8	00001000	08	Забой (Back Space)
9	00001001	09	Горизонтальная табуляция
10	00001010	0A	Перевод строки
11	00001011	0B	Вертикальная табуляция
12	00001100	0C	Перевод страницы
13	00001101	0D	Возврат каретки
14	00001110	0E	Верхний регистр
15	00001111	0F	Нижний регистр
16	00010000	10	Отключение от линии
17	00010001	11	Управление 1
18	00010010	12	Управление 2
19	00010011	13	Управление 3
20	00010100	14	Управление 4
21	00010101	15	Нет подтверждения
22	00010110	16	Синхронизация
23	00010111	17	Конец передающего блока
24	00011000	18	Отмена
25	00011001	19	Конец носителя
26	00011010	1A	Замена
27	00011011	1B	Прерывание
28	00011100	1C	Разделитель файлов
29	00011101	1D	Разделитель групп
30	00011110	1E	Разделитель записей
31	00011111	1F	Разделитель элементов
32	00100000	20	Пробел

Дес.	Двоичная	Шестнадц.	Символ
33	00100001	21	!
34	00100010	22	“
35	00100011	23	#
36	00100100	24	$
37	00100101	25	%
38	00100110	26	&
39	00100111	27	‘
40	00101000	28	(
41	00101001	29	)
42	00101010	2A	*
43	00101011	2B	+
44	00101100	2C	,
45	00101101	2D	-
46	00101110	2E	.
47	00101111	2F	/
48	00110000	30	0
49	00110001	31	1
50	00110010	32	2
51	00110011	33	3
52	00110100	34	4
53	00110101	35	5
54	00110110	36	6
55	00110111	37	7
56	00111000	38	8
57	00111001	39	9
58	00111010	3A	:
59	00111011	3B	;
60	00111100	3C	<
61	00111101	3D	=
62	00111110	3E	>
63	00111111	3F	?
64	01000000	40	@
65	01000001	41	A
66	01000010	42	B
67	01000011	43	C
68	01000100	44	D

Дес.	Двоичная	Шестнадц.	Символ
69	01000101	45	E
70	01000110	46	F
71	01000111	47	G
72	01001000	48	H
73	01001001	49	I
74	01001010	4A	J
75	01001011	4B	K
76	01001100	4C	L
77	01001101	4D	M
78	01001110	4E	N
79	01001111	4F	O
80	01010000	50	P
81	01010001	51	Q
82	01010010	52	R
83	01010011	53	S
84	01010100	54	T
85	01010101	55	U
86	01010110	56	V
87	01010111	57	W
88	01011000	58	X
89	01011001	59	Y
90	01011010	5A	Z
91	01011011	5B	[
92	01011100	5C	\
93	01011101	5D	]
94	01011110	5E	^
95	01011111	5F	_
96	01100000	60	`
97	01100001	61	a
98	01100010	62	b
99	01100011	63	c
100	01100100	64	d
101	01100101	65	e
102	01100110	66	f
103	01100111	67	g
104	01101000	68	h

Дес.	Двоичная	Шестнадц.	Символ
105	01101001	69	i
106	01101010	6A	j
107	01101011	6B	k
108	01101100	6C	l
109	01101101	6D	m
110	01101110	6E	n
111	01101111	6F	o
112	01110000	70	p
113	01110001	71	q
114	01110010	72	r
115	01110011	73	s
116	01110100	74	t
117	01110101	75	u
118	01110110	76	v
119	01110111	77	w
120	01111000	78	x
121	01111001	79	y
122	01111010	7A	z
123	01111011	7B	{
124	01111100	7C	|
125	01111101	7D	}
126	01111110	7E	~
127	01111111	7F	Удаление (DEL)
128	10000000	80	Ђ
129	10000001	81	Ѓ
130	10000010	82	Нижний апостроф ,
131	10000011	83	ѓ
132	10000100	84	Двойные нижние кавычки „
133	10000101	85	…
134	10000110	86	†
135	10000111	87	‡
136	10001000	88	€
137	10001001	89	Знак промилле ‰
138	10001010	8A	Љ
139	10001011	8B	<
140	10001100	8C	Њ

Дес.	Двоичная	Шестнадц.	Символ
141	10001101	8D	Ќ
142	10001110	8E	Ћ
143	10001111	8F	Џ
144	10010000	90	ђ
145	10010001	91	‘
146	10010010	92	’
147	10010011	93	“
148	10010100	94	”
149	10010101	95	•
150	10010110	96	Короткое тире –
151	10010111	97	Длинное тире —
152	10011000	98	Не определён
153	10011001	99	Торговая марка ™
154	10011010	9A	љ
155	10011011	9B	>
156	10011100	9C	њ
157	10011101	9D	ќ
158	10011110	9E	ћ
159	10011111	9F	џ
160	10100000	A0	Неразрывный пробел
161	10100001	A1	Ў
162	10100010	A2	ў
163	10100011	A3	Ј
164	10100100	A4	¤
165	10100101	A5	Ґ
166	10100110	A6	¦
167	10100111	A7	§
168	10101000	A8	Ё
169	10101001	A9	©
170	10101010	AA	Є
171	10101011	AB	«
172	10101100	AC	¬
173	10101101	AD	-Ї
174	10101110	AE	®
175	10101111	AF	Ї
176	10110000	B0	Градус °

Дес.	Двоичная	Шестнадц.	Символ
177	10110001	B1	±
178	10110010	B2	I
179	10110011	B3	і
180	10110100	B4	ґ
181	10110101	B5	µ
182	10110110	B6	¶
183	10110111	B7	Срединная точка ·
184	10111000	B8	ё
185	10111001	B9	№
186	10111010	BA	є
187	10111011	BB	»
188	10111100	BC	j
189	10111101	BD	S
190	10111110	BE	s
191	10111111	BF	ї
192	11000000	C0	А
193	11000001	C1	Б
194	11000010	C2	В
195	11000011	C3	Г
196	11000100	C4	Д
197	11000101	C5	Е
198	11000110	C6	Ж
199	11000111	C7	З
200	11001000	C8	И
201	11001001	C9	Й
202	11001010	CA	К
203	11001011	CB	Л
204	11001100	CC	М
205	11001101	CD	Н
206	11001110	CE	О
207	11001111	CF	П
208	11010000	B0	Р
209	11010001	B1	С
210	11010010	B2	Т
211	11010011	B3	У
212	11010100	B4	Ф

Дес.	Двоичная	Шестнадц.	Символ
213	11010101	D5	Х
214	11010110	D6	Ц
215	11010111	D7	Ч
216	11011000	D8	Ш
217	11011001	D9	Щ
218	11011010	DA	Ъ
219	11011011	DB	Ы
220	11011100	DC	Ь
221	11011101	DD	Э
222	11011110	DE	Ю
223	11011111	DF	Я
224	11100000	E0	а
225	11100001	E1	б
226	11100010	E2	в
227	11100011	E3	г
228	11100100	E4	д
229	11100101	E5	е
230	11100110	E6	ж
231	11100111	E7	з
232	11101000	E8	и
233	11101001	E9	й
234	11101010	EA	к
235	11101011	EB	л
236	11101100	EC	м
237	11101101	ED	н
238	11101110	EE	о
239	11101111	EF	п
240	11110000	F0	р
241	11110001	F1	с
242	11110010	F2	т
243	11110011	F3	у
244	11110100	F4	ф
245	11110101	F5	х
246	11110110	F6	ц
247	11110111	F7	ч
248	11111000	F8	ш

Дес.	Двоичная	Шестнадц.	Символ
249	11111001	F9	щ
250	11111010	FA	ъ
251	11111011	FB	ы
252	11111100	FC	ь
253	11111101	FD	э
254	11111110	FE	ю
255	11111111	FF	я