Федеральное агентство связи

Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ

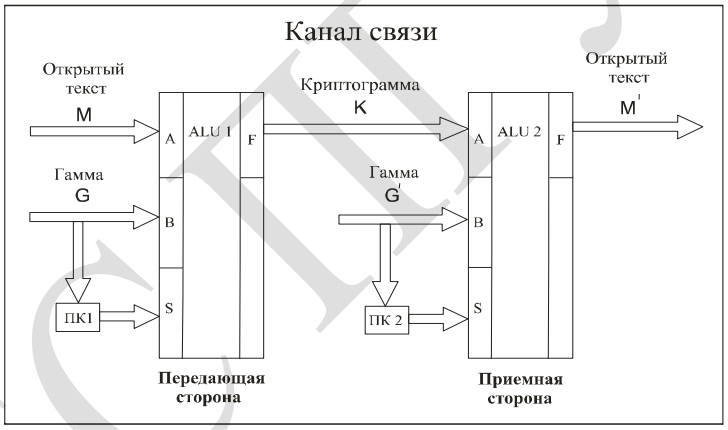
ЭЛЕКТРОННАЯ БИБЛИОТЕЧНАЯ СИСТЕМА

Самара

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»
Кафедра Информатики и вычислительной техники

Шифрование с помощью управляемых операций

Методические указания на проведение лабораторных работ
по дисциплине «Информатика»,
специальности 210400…210406, 210302, 090106



Автор-составитель:
доц., к.т.н. **Алексеев А. П.**

Под общей редакцией **Алексеева А.П.**

Самара, 2010

Введение

В криптографии широко используется аддитивный метод (метод гаммирования). Его идея заключается в том, что к открытому тексту на передаче прибавляется псевдослучайная секретная последовательность, а на приеме эта последовательность вычитается. Известны методы криптоанализа (взлома), которые позволяют произвести дешифрацию криптограммы при малом периоде гаммы даже при неизвестном ключе.

В данной лабораторной работе рассматривается возможность повышения криптостойкости аддитивного метода шифрования, которая основывается на том, что при шифровании открытого текста используется не только логическая операция ИСКЛЮЧАЮЩЕЕ ИЛИ, но и другие логические и арифметические операции. Другими операциями могут быть: логические операции равнозначность, инверсия, повторение и арифметическая операция суммирования по модулю два.

В данной работе моделирование криптосистемы осуществляется с помощью программы Multisim.

Шифрование с помощью управляемых операций

1. Подготовка к работе

По указанной литературе и Приложению к данным методическим указаниям изучить работу пакета Electronics Wokbench (Multisim), принцип гаммирования, ответить на контрольные вопросы.

2. Контрольные вопросы

2.1. В чем состоит основная идея криптографии?
2.2. Дайте определение последовательностных цифровых устройств
2.3. Запишите закон де Моргана.
2.4. Перечислите возможности прибора Logic Converter –XLC1.
2.5. Составьте таблицу истинности логического элемента ИЛИ-НЕ
2.6. Составьте таблицу истинности логического элемента И-НЕ.
2.7. Запишите тождества алгебры логики.
2.8. Как записывается логическая функция в совершенной дизъюнктивной нормальной форме (СДНФ)?
2.9. Как записывается логическая функция в совершенной конъюнктивной нормальной форме (СКНФ)?
2.10. Дайте определение комбинационного цифрового устройства.
2.11. Запишите законы алгебры логики.
2.12. Опишите методику синтеза ПК с помощью диаграмм Вейча.
2.13. Как представить отрицательное число в дополнительном коде?
2.14. Чем отличаются логические и арифметические операции?
2.15. Для чего используются в АЛУ выводы M и CN?
2.16. Чем отличаются комбинационные цифровые устройства от последовательностных цифровых устройств?
2.17. Охарактеризуйте различные версии программы Electronics Workbench.

3. Задания на выполнение лабораторной работы

3.1.1. Задание 1. Синтез преобразователя кода

Используя таблицу 3.1.1 разработать преобразователь кода (ПК), для чего предварительно требуется составить таблицу истинности для своего варианта. Преобразователи кодов нужно синтезировать с помощью блока Logic Converter (логический конвертор), который входит в систему моделирования радиоэлектронных устройств Multisim 8.2.12 Pro.

Таблица 1

Вариант	Зависимость вида операции от значения гаммы			
	$M \oplus G$	$\overline{M \oplus G}$	$M - G$	$M + G$
1	0,5,6,7	1,3,11	2,8,12,15	4,9,10,13,14
2	2,3,7,11	8,12,14,15	0,1,5,9,13	4,6,10
3	0,1,4,5	2,3,12,14,15	6,8,10	7,9,11,13
4	0,13,14,15	4,6,8,10,12	1,3,5	2,7,9,11
5	1,5,9,13	3,7,11,15	2,6,10,14	0,4,8,13
6	0,5,10,15	3,6,9,12	4,8,7,11	1,2,13,14
7	0,4,8,12	1,5,9,13	2,6,10,14	3,7,11,15
8	2,6,10,14	0,4,8,12	3,7,11,15	1,5,9,13
9	3,7,11,15	2,6,10,14	1,5,9,13	0,4,8,12
10	4,5,8,9,	2,3,12,13	0,1,6,7	10,11,14,15
11	13,15,3,7	2,6,9,12	0,4,8,11	1,5,9,10,14
12	2,3,6,7	10,11,14,15	4,5,8,9	0,1,12,13
13	2,6,8,12	3,7,11,15	0,4,10,14	1,5,9,13
14	5,7,10,13	4,6,12,15	0,2,8,11	1,3,9,14
15	0,4,9,13	1,5,8,12	3,7,10,14	2,6,11,15
16	3,7,8,12	0,4,10,14	2,6,11,15	1,5,9,13
17	2,8,12,15	0,5,6,7	1,3,11,4	9,10,13,14
18	0,2,4,6	8,10,12,14	1,5,9,13	3,7,11,15
19	2,3,12,13	0,1,6,7	4,5,8,9	10,11,14,15
20	0,4,8,12	1,5,9,13	2,6,10,14	3,7,11,15
21	1,4,9,12	0,5,8,13	2,7,10,15	3,6,11,14
22	8,9,12,13	0,1,6,7	10,11,14,15	2,3,4,5
23	10,11,14,15	2,3,6,7	0,1,12,13	4,5,8,9
24	8,9,13,14	10,11,12,15	0,2,5,7	1,3,4,6
25	0,1,2,3	4,5,6,7	8,9,10,11	12,13,14,15

3.1.2. Задание 2. Разработка принципиальной схемы криптографической системы

Исследуемое устройство будет работать с использованием четырех операций: ИСКЛЮЧАЮЩЕЕ ИЛИ, равнозначность, сложение и вычитание. Эти операции должны сменять друг друга при изменении значений гаммы.

Для реализации этого при составлении принципиальной схемы криптосистемы следует использовать разработанный преобразователь кода.

Пример составления схемы приведен в методических указаниях.

Составленную принципиальную схему криптосистемы следует использовать для моделирования её работы. Для этого необходимо проверить выполнение шестнадцати логических и арифметических операций.

Значения операндов выбрать такими:

Таблица 2

Значение гаммы (G)		0	1	2	3	4	5	6	7	8
Вариант 1		1	2	3	4	5	6	7	8	9
Вариант 2		2	3	4	5	6	7	8	9	10
Вариант 3		3	4	5	6	7	8	9	10	11
Вариант 4		4	5	6	7	8	9	10	11	12
Вариант 5		5	6	7	8	9	10	11	12	13
Вариант 6		6	7	8	9	10	11	12	13	14
Вариант 7		7	8	9	10	11	12	13	14	15
Вариант 8		8	9	10	11	12	13	14	15	0
Вариант 9		9	10	11	12	13	14	15	0	1
Вариант 10		10	11	12	13	14	15	0	1	2
Вариант 11		11	12	13	14	15	0	1	2	3
Вариант 12		12	13	14	15	0	1	2	3	4
Вариант 13	M	13	14	15	0	1	2	3	4	5
Вариант 14		14	15	0	1	2	3	4	5	6
Вариант 15		15	0	1	2	3	4	5	6	7
Вариант 16		0	1	2	3	4	5	6	7	8
Вариант 17		0	2	4	6	8	10	12	14	1
18		1	3	5	7	9	11	13	15	0
19		5	4	3	2	1	0	10	9	8
20		15	14	13	12	11	10	9	8	7
21		10	9	8	7	6	15	14	13	12
22		0	1	2	3	4	10	11	12	13
23		10	11	12	13	14	15	0	1	2
24		3	5	7	9	11	13	15	0	1
25		3	0	1	2	6	7	4	5	10

Продолжение таблицы 2

Значение гаммы (G)		9	10	11	12	13	14	15
Вариант 1		10	11	12	13	14	15	0
Вариант 2		11	12	13	14	15	0	1
Вариант 3		12	13	14	15	0	1	2
Вариант 4		13	14	15	0	1	2	3
Вариант 5		14	15	0	1	2	3	4
Вариант 6		15	0	1	2	3	4	5
Вариант 7		0	1	2	3	4	5	6
Вариант 8		1	2	3	4	5	6	7
Вариант 9		2	3	4	5	6	7	8
Вариант 10		3	4	5	6	7	8	9
Вариант 11		4	5	6	7	8	9	10
Вариант 12		5	6	7	8	9	10	11
Вариант 13	M	6	7	8	9	10	11	12
Вариант 14		7	8	9	10	11	12	13
Вариант 15		8	9	10	11	12	13	14
Вариант 16		9	10	11	12	13	14	15
Вариант 17		3	5	7	9	11	13	15
18		2	4	6	8	10	12	14
19		7	6	15	14	13	12	11
20		6	0	1	2	3	4	5
21		11	5	4	3	2	1	0
22		14	15	5	6	7	8	9
23		3	4	9	8	7	6	5
24		2	4	6	8	10	12	14
25		11	8	9	14	15	12	13

Результаты моделирования следует сопоставить с результатами ручных расчетов и занести в таблицу (таблица 3).

Таблица 3

№ п/п	Значение гаммы (G)	Значение открытого текста (M)	Результат моделирования	Результат ручного расчета
1	0			
2	1			
3	2			
4	3			

4. Методические указания

Моделирование данного способа шифрования производится с помощью программы Multisim 8.2.12 Professional. Открытый текст, гамма, криптограмма представлена четырехразрядными двоичными операндами, а управляющие сигналы формируются с помощью пяти битов. Структурная схема приведена на рисунке 1.

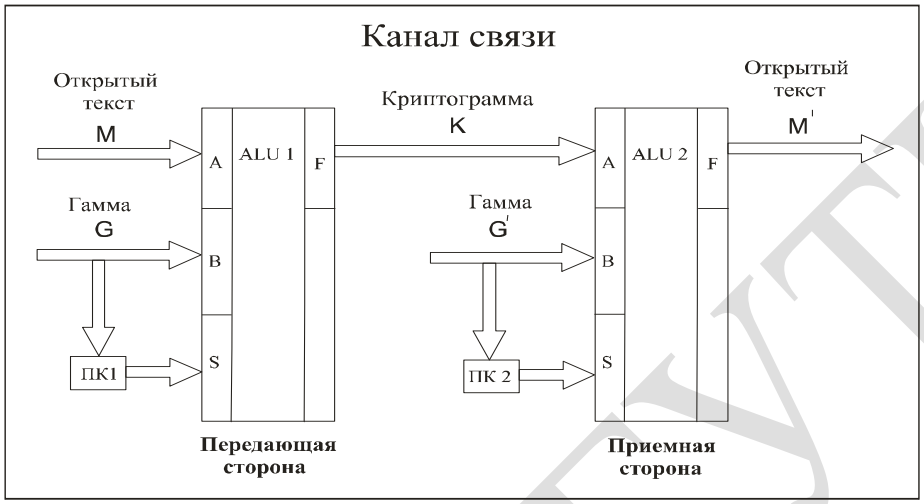


Рис. 1 – Структурная схема криптографической системы

Передающая и приемная стороны имитируются с помощью двух четырехразрядных арифметико-логических устройств (АЛУ). На передающей стороне вход M используется для подачи открытого текста, вход G - для подачи гаммы. На приемной стороне вход K используется для приема криптограммы, вход G' – для подключения гаммы. Потоки открытого текста и гаммы формируются с помощью шестнадцатиразрядного генератора двоичных слов. Для контроля результатов преобразований (открытого текста на приемной и передающей сторонах, гаммы и криптограммы) используют четыре шестнадцатеричных индикатора.

Изменение вида выполняемой операции осуществляются с помощью преобразователя кода (ПК 1 и ПК 2), на вход которого подается гамма (4 бита), а выход которого подключается к управляющим входам АЛУ (5 битов). Сигналы на управляющих входах АЛУ определяют вид выполняемой операции. Изменение гаммы приводит к изменению сигналов на выходе преобразователя кода, а, значит, и к изменению управляющих сигналов на передающей и приемной сторонах.

Для начала требуется произвести синтез преобразователей кода, которые будут подключены к арифметико-логическим устройствам и определять вид выполняемой операции. Используя таблицу 1, составим таблицу истинности для варианта 25.

Таблица 2

№ п/п	Гамма $B_3B_2B_1B_0$ (BCDE)	Операция	Управляющие сигналы $S_3S_2S_1S_0$	Mod	C_N
0	0 0 0 0	$M \oplus G$	0 1 1 0	1	x
1	0 0 0 1		0 1 1 0		
2	0 0 1 0		0 1 1 0		
3	0 0 1 1		0 1 1 0		
4	0 1 0 0	$\overline{M \oplus G}$	1 0 0 1	1	x
5	0 1 0 1		1 0 0 1		
6	0 1 1 0		1 0 0 1		
7	0 1 1 1		1 0 0 1		
8	1 0 0 0	$M - G$	0 1 1 0	0	0
9	1 0 0 1		0 1 1 0		
10	1 0 1 0		0 1 1 0		
11	1 0 1 1		0 1 1 0		
12	1 1 0 0	$M + G$	1 0 0 1	0	1
13	1 1 0 1		1 0 0 1		
14	1 1 1 0		1 0 0 1		
15	1 1 1 1		1 0 0 1		

Первые два столбца таблицы будут одинаковыми для всех вариантов, столбец «Управляющие сигналы» составить следующим образом (на примере варианта № 25): для гаммы равной значениям «0», «1», «2», «3» выполняется операция $M \oplus G$, поэтому для пунктов 0-3 ставится в соответствие данная операция. Другие строки таблицы заполняются аналогично. Столбец «Операция» заполняется исходя из столбца «Управляющие сигналы». Столбец «Mod» определяет, какую операцию выполняет АЛУ: логическую (его значение равно 1) или арифметическую(значение равно 0). Значение C_N означает перенос в разрядах: для логических операций безразлично какое значение примет, поэтому обозначено символом «x», для арифметического вычитания равно «0», для арифметического сложения – «1». Соответствие управляющих сигналов и операций следующее: «$M \oplus G$» – «0 1 1 0», «$\overline{M \oplus G}$» – «1 0 0 1», «$M - G$» – «0 1 1 0», «$M + G$» – «1 0 0 1»

Входы $S_3S_2S_1S_0$ и Mod предназначены для формирования управляющих сигналов, которые позволяют выбрать одну из шестнадцати возможных операций АЛУ.

По данной таблице составляют логические выражения, используемые для синтеза преобразователей кода. Составить логические выражения легче всего с помощью Logic Converter (логический конвертор). Этот инструмент позволяет создавать преобразователи кодов с числом аргументов $n \le 8$. Для получения математических выражений, описывающих работу ПК, достаточно в конвертор ввести таблицу истинности преобразователя кода.

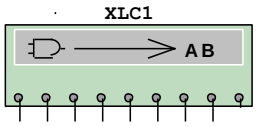


Рис. 2 – Изображение логического конвектора

Для этого нужно запустить Multisim. На панели справа найти нужный блок (он четвертый снизу), однократным щелчком мыши переместить его на рабочее поле. Далее нужно вызвать окно свойств двойным нажатием левой кнопки мыши и внести таблицу истинности в конвертор. Это действие следует произвести для каждого управляющего сигнала (S) в отдельности. Анализируя таблицу, можно заметить, что $S_3 = S_0$, $S_2 = S_1$. Это означает, что выражения для этих управляющих сигналов будут одинаковыми. Для сигналов Mod и C_N также нужно получить логические выражения аналогичным способом. Логические выражения по управляющим сигналам получить последовательным нажатием на вторую и третью кнопки в окне свойств логического конвертора в поле «Conversions» В качестве примера получим выражение для $S_3 = S_0$ для варианта 25 (рис.3).

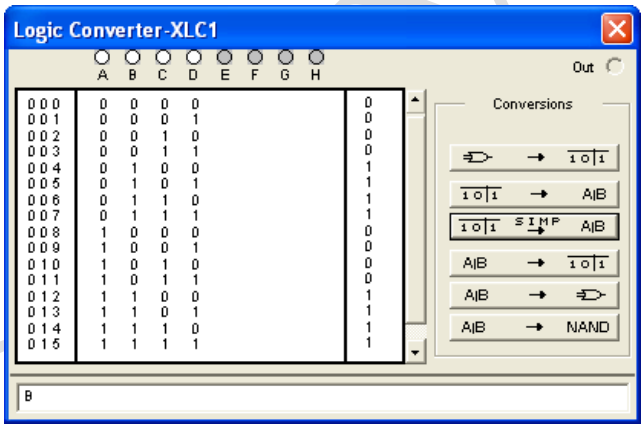


Рис. 3 – Окно свойств логического конвектора

Как видно из рис. 3, результат синтеза – B. Учитывая последовательность ввода операндов и их соответствие операндам S, получаем выражение $S_3 = S_0 = \mathrm{B}_2$.

Для справки: символ A в данном окне соответствует гамме B3, символ B – B2, C – B1, D – B0. Аналогично получаем следующее: $S_2 = S_1 = \overline{\mathrm{B}}_2$, $M = \overline{\mathrm{B}}_3$, $C_N = \mathrm{B}_2$.

Эти выражения для преобразователя кода на передаче.

Теперь аналогично выполним синтез ПК на приеме. Для этого нужно изменить таблицу истинности (изменить управляющие сигналы S). При этом нужно помнить, что логические выражения для приема и передачи не изменятся, а арифметические поменяются на прямо противоположные, т.е., если на передаче у нас было арифметическое сложение, то на приеме будет арифметическое вычитание, и наоборот. В итоге таблица истинности примет следующий вид (обратить внимание, что C_N также поменяло свои значения).

Таблица 3

№ п/п	Гамма $B_3B_2B_1B_0$ (BCDE)	Операция	Управляющие сигналы $S_3S_2S_1S_0$	Mod	C_N
0	0 0 0 0	$M \oplus G$	0 1 1 0	1	x
1	0 0 0 1		0 1 1 0		
2	0 0 1 0		0 1 1 0		
3	0 0 1 1		0 1 1 0		
4	0 1 0 0	$\overline{M \oplus G}$	1 0 0 1	1	x
5	0 1 0 1		1 0 0 1		
6	0 1 1 0		1 0 0 1		
7	0 1 1 1		1 0 0 1		
8	1 0 0 0	$M + G$	1 0 0 1	0	1
9	1 0 0 1		1 0 0 1		
10	1 0 1 0		1 0 0 1		
11	1 0 1 1		1 0 0 1		
12	1 1 0 0	$M - G$	0 1 1 0	0	0
13	1 1 0 1		0 1 1 0		
14	1 1 1 0		0 1 1 0		
15	1 1 1 1		0 1 1 0		

Выражения на приеме примут вид $S_3 = S_0 = \overline{B}_3B_2 + B_3\overline{B}_2$, $S_2 = S_1 = \overline{B}_3\overline{B}_2 + B_3B_2$, $M = \overline{B}_3$, $C_N = \overline{B}_2$.

На основе этих выражений и «собираем» ПК на передаче и приеме, подключаемые к АЛУ. В итоге принципиальная схема примет вид (рис.4)

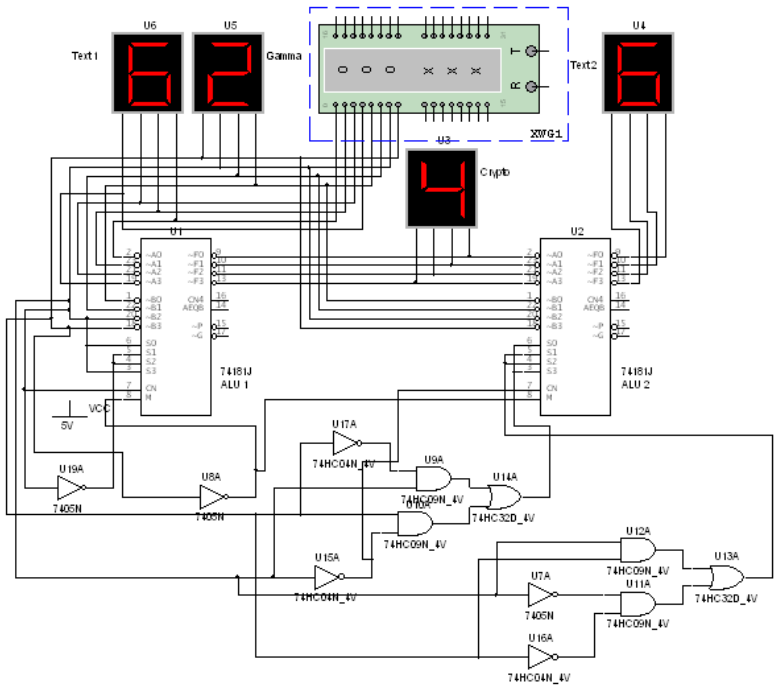


Рис. 4 – Принципиальная схема криптосистемы

Четырехбитный открытый текст подается на вход A первого арифметико-логического устройства (АЛУ). Гамма подается на вход B. Вид выполняемой операции должен задаваться с помощью преобразователя кода ПК1. Криптограмма будет формироваться на выходе F первого АЛУ. Дешифрация криптограммы будет осуществляться на приемной стороне с помощью второго АЛУ. Вид выполняемой операции синхронно изменяется под управлением гаммы. Принятый открытый текст появлялся на выходе F второго АЛУ.

Исходный текст, принятый текст, гамма и криптограмма отображаются с помощью индикаторов U3…U6. Значения гаммы и передаваемый текст формируются с помощью генератора слов XWG1 (Word Generator).

Как и всякая имитация, рассматриваемая модель не полностью соответствует реальной криптографической системе. Например, при моделировании предполагается, что соединение между передающей и приемной сторонами происходит по четырем проводам. В реальной криптосистеме связь должна осуществляться по двухпроводной линии.

Кроме того, при моделировании считается, что операнды, циркулирующие в криптосистеме, являются четырехразрядными целыми числами. Диапазоны изменения чисел составляли $0 \le M \le 15$ и $0 \le G \le 15$. Кроме того, в реальной криптосистеме при формировании криптограммы возможно использование не только целых, но и вещественных чисел.

На следующем этапе выполнения лабораторной работы следует проверить правильность работы схемы. Для этого в окне свойств генератора слов XWG1 нужно выставить значения гаммы и открытого текста как на рисунке 5, и нажатием на клавишу Step, поочередно проверить все операции. Для удобства флажок таблицы исчисления должен стоять на «Hex», значащееся разряды крайние справа: например «0», «6», где «0» – это значение гаммы, а «6» – значение открытого текста. Нужно помнить – числу «10» соответствует буква «A», «11» – «B», «12» – «C», «13» – «D», «14» – «E», «15» – «D».

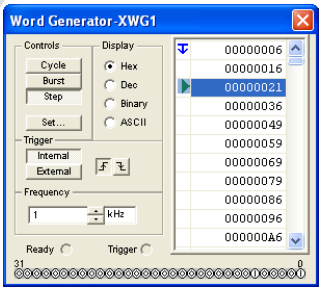


Рис. 5 – Окно свойств генератора слов

Как видно из рисунка 5, выполняется 3-я по счету операция, в таблице 2 – это операция ИСКЛ-ИЛИ. Складываются по модулю 2 числа «2» и «1». Выполнив эту операцию с числами в двоичном коде, получим ответ «3», что и получили на выходе первого АЛУ (криптотекст), а на выходе второго АЛУ получили ответ «1», что соответствует значению открытого текста на входе первого АЛУ, следовательно, операция криптосистемой выполнена верно. Аналогично проверяются и другие строки таблицы. Результаты проверки внести в таблицу 3.

Литература

1 Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптография: скоростные шифры.- СПб: БХВ – Петербург, 2002.- 496 с.

2. Бабаш А.В., Шанкин Г.П. Криптография.- М.: СОЛОН-Р, 2002.- 512 с.

3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии.– М.: Гелиос АРВ, 200.- 480 с.

4. Алексеев А.П., Жеренов Ю.В. Моделирование криптографической системы с помощью программы Multisim. – «Инфокоммуникационные технологии», том 7, № 4, 2009.-78-83 с.

5. Алексеев А.П., Жеренов Ю.В. Моделирование криптографической системы с помощью программы Multisim. – Тезисы конференции – Казань, 2008

6. Алексеев А.П., Жеренов Ю.В. Шифрование с помощью управляемых операций – Тезисы конференции – Самара, 2009

7. Алексеев А. П., Орлов В. В. Стеганографические и криптографические методы защиты информации. – Самара: ПГУТИ, 2010.- 331 с.