Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет информационной безопасности

Кафедра защиты информации

А. М. Тимофеев

СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ: СТАНДАРТ DES. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

*Рекомендовано УМО по образованию
в области информатики и радиоэлектроники
в качестве учебно-методического пособия для специальностей
1-41 01 03 «Квантовые информационные системы»,
1-98 01 02 «Защита информации в телекоммуникациях»*

Минск БГУИР 2024

УДК 004.056.55(076)
ББК 32.972.5я73
Т41

Р е ц е н з е н т ы:

кафедра телекоммуникационных систем учреждения образования
«Белорусская государственная академия связи»
(протокол № 3 от 4.10.2023);

доцент кафедры информационно-измерительной техники
и технологии Белорусского национального технического университета
кандидат технических наук, доцент Н. Н. Ризноокая

Тимофеев, А. М.

Т41 Симметричные криптосистемы : Стандарт DES. Лабораторный практикум : учеб.-метод. пособие / А. М. Тимофеев. – Минск : БГУИР, 2024. – 123 с. : ил.

ISBN 978-985-543-756-8.

Пособие содержит пять лабораторных работ и направлено на изучение базовых криптографических и криптоподобных операций, выполняемых применительно для симметричных алгоритмов и стандартов шифрования данных (на примере стандарта DES). Композиционно каждая лабораторная работа включает краткие теоретические сведения, практическое задание, содержание отчета и перечень контрольных вопросов. Для выполнения практических заданий используется специально разработанная компьютерная программа TAMbsuirCryptoLab.

Предназначено для студентов всех форм обучения, может быть полезно магистрантам инфокоммуникационных специальностей, а также специалистам, работающим в области проектирования, создания и эксплуатации систем защиты информации.

УДК 004.056.55(076)
ББК 32.972.5я73

ISBN 978-985-543-756-8

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 5
ЛАБОРАТОРНАЯ РАБОТА 1
СХЕМА ГЕНЕРАЦИИ РАУНДОВЫХ КЛЮЧЕЙ DES НА БАЗЕ БЛОКОВ *LS* 9
1.1 Краткие теоретические сведения 9
1.2 Практическое задание 12
1.3 Содержание отчета 21
1.4 Контрольные вопросы 21
ЛАБОРАТОРНАЯ РАБОТА 2
СХЕМА ГЕНЕРАЦИИ РАУНДОВЫХ КЛЮЧЕЙ DES НА БАЗЕ БЛОКОВ *RS* 23
2.1 Краткие теоретические сведения 23
2.2 Практическое задание 26
2.3 Содержание отчета 33
2.4 Контрольные вопросы 33
ЛАБОРАТОРНАЯ РАБОТА 3
DES В РЕЖИМЕ ЗАШИФРОВАНИЯ ДАННЫХ 35
3.1 Краткие теоретические сведения 35
3.2 Практическое задание 41
3.3 Содержание отчета 48
3.4 Контрольные вопросы 48
ЛАБОРАТОРНАЯ РАБОТА 4
DES В РЕЖИМЕ РАСШИФРОВАНИЯ ШИФРТЕКСТОВ 49
4.1 Краткие теоретические сведения 49
4.2 Практическое задание 51
4.3 Содержание отчета 58
4.4 Контрольные вопросы 58

ЛАБОРАТОРНАЯ РАБОТА 5
РЕЖИМЫ РАБОТЫ СИММЕТРИЧНЫХ КРИПТОСИСТЕМ БЛОЧНОГО ТИПА НА БАЗЕ DES 59
5.1 Краткие теоретические сведения 59
5.2 Практическое задание 82
5.3 Содержание отчета 90
5.4 Контрольные вопросы 90
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 91
ПРИЛОЖЕНИЕ А
Дополнительные опции программы 93
ПРИЛОЖЕНИЕ Б
Сведения о возможных сообщениях программы 94
ПРИЛОЖЕНИЕ В
Исходные данные к лабораторной работе 1 97
ПРИЛОЖЕНИЕ Г
Исходные данные к лабораторной работе 2 98
ПРИЛОЖЕНИЕ Д
Исходные данные к лабораторной работе 3 99
ПРИЛОЖЕНИЕ Е
Исходные данные к лабораторной работе 4 100
ПРИЛОЖЕНИЕ Ж
Исходные данные к лабораторной работе 5 101
ПРИЛОЖЕНИЕ И
Примеры решений практических заданий 117

ВВЕДЕНИЕ

В настоящее время использование криптографических и криптоподобных преобразований информации является одним из наиболее эффективных и широко используемых методов защиты информации, передаваемой через открытые сети (например, Интернет), а также хранимой и обрабатываемой на отдельных вычислительных комплексах и персональных компьютерах. В результате таких преобразований можно обеспечивать конфиденциальность информации, контролировать целостность данных, а также устанавливать подлинность как самих данных, так и их отправителя и др. [1–5].

В классификации криптосистем (криптоалгоритмов) отдельный класс образуют симметричные одноключевые криптосистемы (с секретным ключом), в которых преобразование зашифрования является симметричным относительно преобразования расшифрования. Эти криптосистемы весьма распространены и включают зарубежные (DES, IDEA NXT, AES и пр.) и отечественные криптоалгоритмы (ГОСТ 28147-89, СТБ 34.101.31-2011 и др.) [1–11].

Следует отметить, что криптографические операции, как и их последовательность выполнения, для различных криптосистем, конечно, отличаются. Однако существует несколько важных особенностей, свойственных и являющихся общими для многих современных криптосистем.

Во-первых, имеются несколько базовых криптографических операций, используемых в различных криптосистемах. Среди таких криптографических операций можно выделить следующие:

– операции перестановки и подстановки;

– операции циклического сдвига влево и вправо на различное число двоичных разрядов;

– операции суммирования по некоторому модулю (2, 2^{16}, 2^{16-1}, 2^{32}, 2^{32-1} и др.).

Во-вторых, для многих криптоалгоритмов передача (распределение) отправителю (стороне, которая будет зашифровывать данные) и получателю (стороне, которая будет расшифровывать шифртексты) секретного криптографического ключа имеет особенность. Эта особенность заключается в следующем. Секретный криптографический ключ, как правило, имеет сравнительно небольшую длину. Однако ключевой массив (или набор раундовых ключей), требуемый отправителю и получателю соответственно для зашифрования данных и расшифрования шифртекстов, достаточно часто в несколько раз превышает длину секретного криптографического ключа. Для выработки (генерации) из этого секретного криптографического ключа требуемого ключевого массива отправитель и получатель используют специальные схемы.

В-третьих, базовые криптоалгоритмы, как правило, применяются с использованием специальных режимов работы (схемных решений), направленных на повышение криптостойкости.

Одним из стандартов, предусматривающих изучение базовых криптографических операций, принципов генерации раундовых ключей на стороне отправителя зашифрованных данных и на стороне получателя шифртекстов, а также режимов работы криптосистем, является стандарт шифрования данных DES (Data Encryption Standard). Этот стандарт в «чистом» виде в настоящее время применяется исключительно для устаревших систем (чаще всего используют его более криптоустойчивые версии – 3DES или DESX). Однако, по мнению автора настоящего учебно-методического пособия, целесообразность изучения DES определяется тем, что DES не только предусматривает наличие указанных выше базовых криптографических операций, схем генерации раундовых ключей и режимов работы, но и может быть чрезвычайно полезным при реализации криптосистем различного назначения на базе любого другого стандартного криптоалгоритма.

Так, например, режимы работы DES в настоящее время используют [12 – 16]:

– в сетевом протоколе аутентификации Kerberos (режимы работы CBC и PCBC), который поддерживается многими операционными системами (ОС): Windows, UNIX и UNIX подобными ОС (Apple Mac OS X, Red Hat Enterprise Linux 4, FreeBSD, Solaris, AIX, OpenVMS);

– для приложений, в которых существует необходимость зашифрования открытого текста произвольной длины с помощью стандартного криптоалгоритма таким образом, чтобы избыточность в полученном шифртексте была минимальной либо вовсе отсутствовала (режимы работы CFB и OFB);

– при создании потокового шифра из стандартного блочного криптоалгоритма (режимы работы CFB и OFB);

– для повышения криптостойкости любого другого стандартного криптоалгоритма на основе методе отбеливания ключа (режим DESX);

– во многих финансовых приложениях (для эмиссии и обработки кредитных карт VISA, EuroPay и пр.), а также для защиты информации, содержащейся в биометрических паспортах.

Таким образом, при подготовке специалистов в области информационной безопасности представляется весьма важным изучение на примере стандарта DES базовых криптографических операций, принципов генерации раундовых ключей на стороне отправителя зашифрованных данных и на стороне получателя шифртекстов, а также режимов работы криптосистем.

Содержание учебно-методического пособия включает пять тем лабораторных работ, направленных на изучение схем генерации раундовых ключей на базе блоков циклического сдвига влево *LS* (лабораторная работа 1) и вправо *RS* (лабораторная работа 2), схем зашифрования данных (лабораторная работа 3) и расшифрования шифртекстов (лабораторная работа 4), а также основных режимов работы симметричных криптосистем, построенных на базе

DES (лабораторная работа 5). Композиционно каждая лабораторная работа включает краткие теоретические сведения, практическое задание, содержание отчета и перечень контрольных вопросов.

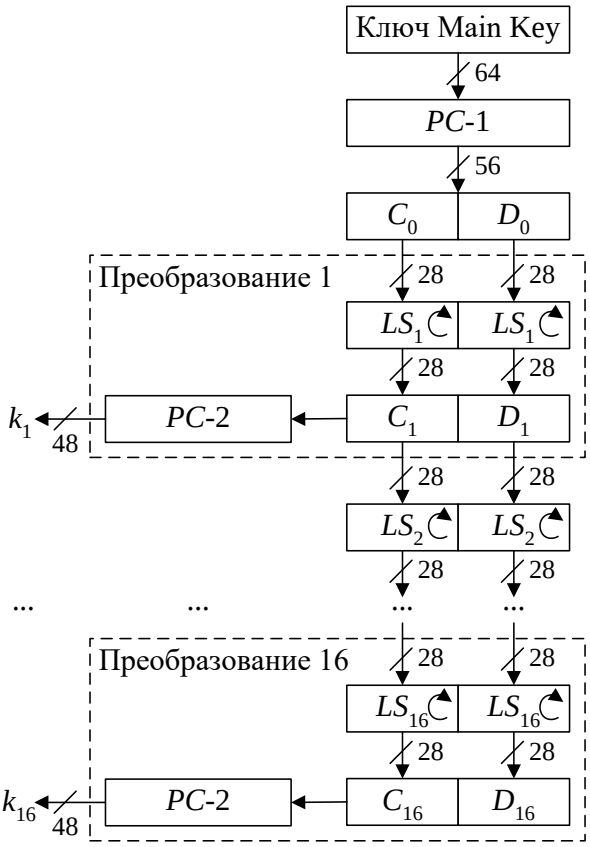
Для выполнения практических заданий используется специально разработанная компьютерная программа, позволяющая генерировать секретный криптографический ключ и на его основе вычислять раундовые ключи для зашифрования данных и расшифрования шифртекстов, а также непосредственно выполнять зашифрование данных, расшифрование шифртекстов и реализовывать основные режимы работы симметричных криптосистем, построенных на базе DES.

ЛАБОРАТОРНАЯ РАБОТА 1
СХЕМА ГЕНЕРАЦИИ РАУНДОВЫХ КЛЮЧЕЙ DES НА БАЗЕ БЛОКОВ *LS*

Цель: изучение схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига влево *LS*.

1.1 Краткие теоретические сведения

На рисунке 1 показана структурная схема генерации ключей DES, которая вырабатывает 16 раундовых ключей k_i (i = 1, 2, …, 16).



На i-м преобразовании формируется k_i раундовый ключ (i = 1, 2, …, 16)

Рисунок 1 – Структурная схема генерации раундовых ключей DES на базе блоков циклического сдвига влево *LS*

Каждый раундовый ключ k_i состоит из 48 бит исходного секретного ключа Main Key. Ключ Main Key содержит 56 значащих бит и 8 проверочных бит для контроля на четность, расположенных в позициях 8, 16, 24, 32, 40, 48, 56, 64. Для удаления контрольных битов и подготовки ключа к работе используется функция первоначальной подготовки ключа *PC*-1, поясняемая рисунком 2.

57	49	41	33	25	17	9	C_0
1	58	50	42	34	26	18	
10	2	59	51	43	35	27	
19	11	3	60	52	44	36	
63	55	47	39	31	23	15	D_0
7	62	54	46	38	30	22	
14	6	61	53	45	37	29	
21	13	5	28	20	12	4	

Рисунок 2 – Функция первоначальной подготовки ключа *PC*-1

Как видно из рисунка 2, функция *PC*-1 разделена на две части: C_0 и D_0 по 28 бит каждая. Первые четыре строки матрицы *PC*-1 определяют, как выбираются биты последовательности C_0 (первым битом C_0 будет бит 57 ключа Main Key, затем бит 49 и т. д., а последними битами – биты 44 и 36), а следующие четыре строки – биты последовательности D_0 (первым битом D_0 будет бит 63 ключа Main Key, затем бит 55 и т. д., а последними битами – биты 12 и 4).

После определения C_0 и D_0 рекурсивно определяются C_i и D_i путем циклического сдвига влево на один или два бита C_{i-1} и D_{i-1} соответственно в зависимости от номера преобразования, как показано в таблице 1.

Таблица 1 – Количество сдвигов для вычисления раундовых ключей

Номер преобразования	Количество сдвигов, бит	Номер преобразования	Количество сдвигов, бит
1	1	9	1
2	1	10	2
3	2	11	2
4	2	12	2
5	2	13	2
6	2	14	2
7	2	15	2
8	2	16	1

Операции циклического сдвига влево выполняются для последовательностей C_i и D_i независимо (см. рисунок 1). Например, последовательность C_5 получается посредством циклического сдвига влево на две позиции последовательности C_4, последовательность D_5 – посредством сдвига влево на две позиции последовательности D_4, а C_{16} и D_{16} получаются из C_{15} и D_{15} посредством циклического сдвига влево на одну позицию (см. таблицу 1).

Раундовый ключ k_i, определяемый на каждом преобразовании (см. рисунок 1), есть результат выбора конкретных битов из 56-битовой последовательности C_iD_i и их перестановки, что реализуется функцией, завершающей подготовку ключа *PC*-2, поясняемой рисунком 3.

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Рисунок 3 – Функция, завершающая подготовку ключа *PC*-2

Как видно из рисунка 3, первым битом раундового ключа k_i будет 14-й бит последовательности C_iD_i, вторым – 17-й бит, и т. д., а последним – 32-й бит.

1.2 Практическое задание

1 Включите персональный компьютер и запустите файл «TAMbsuirCryptoLab.exe» на выполнение.

После запуска файла «TAMbsuirCryptoLab.exe» активизируется программное обеспечение, и появится окно выбора задания для выполнения, показанное на рисунке 4.

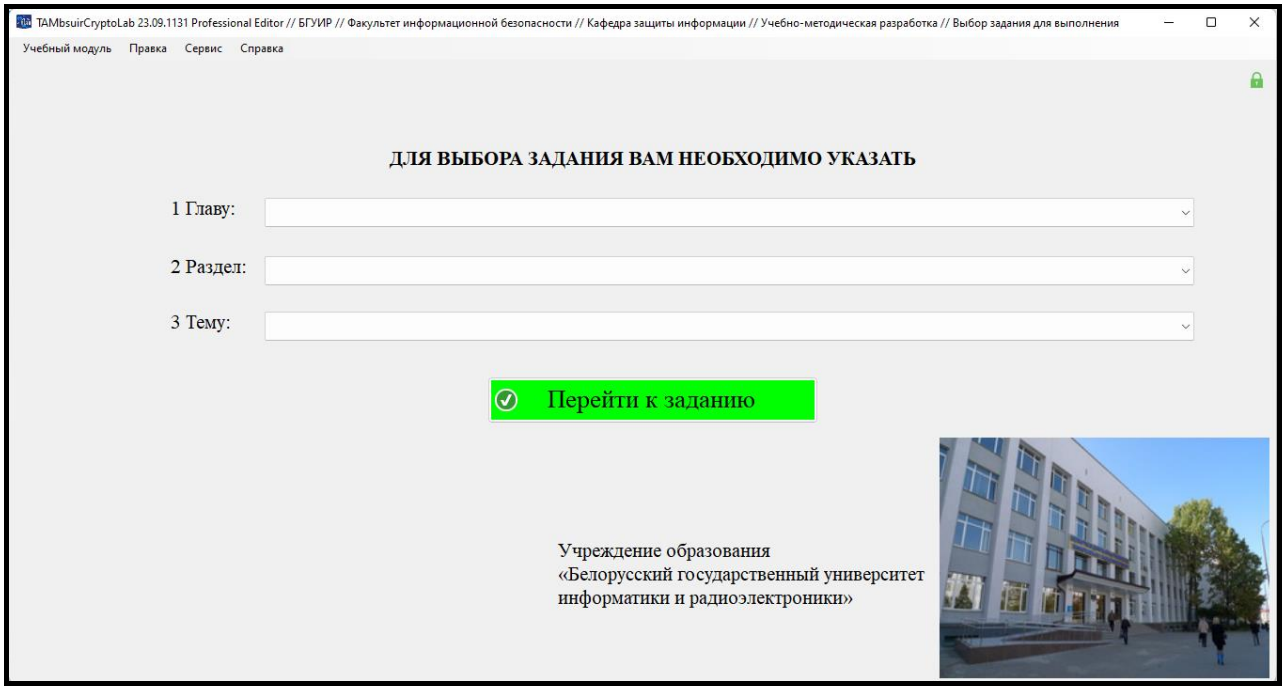


Рисунок 4 – Окно выбора задания

В верхней области окна программы (см. рисунок 4) имеется графическое главное меню с четырьмя вкладками: «Учебный модуль», «Правка», «Сервис» и «Справка». Выбор элемента главного меню приводит к вызову появляющегося под главным подменю, некоторые из них, в свою очередь, также содержат

подменю. Для удобства элементы подменю визуально объединены при помощи разделителей и имеют пиктограммы, иллюстрирующие опции программы. Выбор элемента главного меню, как и элемента подменю, осуществляется либо щелчком, либо нажатием сочетания клавиш.

Вкладки «Учебный модуль» и «Справка» содержат набор подменю, которые дают возможность всем допущенным к выполнению задания пользователям воспользоваться дополнительными опциями программы (на любом этапе выполнения задания). Например, с помощью этих вкладок доступны такие опции программы, как ознакомление с методическими указаниями, изучение применяемых схем и расчетных формул, а также отмена загруженного учебного модуля и завершение его выполнения. В приложении А поясняется выбор опции программы через главное меню и с помощью сочетания клавиш (таблица А.1).

Остальные подменю, содержащиеся во вкладках «Учебный модуль» и «Справка», а также все подменю, имеющиеся во вкладках «Правка» и «Сервис, для выполнения задания не используются. Они применяются для реализации ряда вспомогательных функций и доступны только для преподавателя учебной дисциплины, обладающего правами администратора.

В центральной области окна выбора задания (см. рисунок 4) имеется перечень из трех пунктов: «1 Глава:», «2 Раздел:» и «3 Тема:». Рядом с каждым из этих пунктов расположен выпадающий (раскрывающийся) список в виде элемента графического интерфейса (виджета), который позволяет осуществить выбор задания путем нажатия либо на сам виджет, либо на значок выпадающего списка, обозначенный треугольником.

В случае недопустимого, неправильного или некорректного заполнения предлагаемых полей программа генерирует сообщения об ошибках, в которых указывается их внутренний код, а также краткая информация об их причине. В приложении Б представлены сведения о возможных сообщениях об ошибках,

включая их внутренние коды, возможные причины, действия, необходимые для их устранения (таблица Б.1), и примеры таких сообщений (рисунок Б.1).

Также в процессе выполнения задания программа может генерировать сообщения информационного характера, которые не имеют внутренних кодов и предназначены для дополнительного разъяснения специфики выполнения отдельных этапов задания. На рисунке Б.2 в качестве примера приведено информационное сообщение, появляющееся при попытке выбора задания пользователем, у которого отсутствует допуск к его выполнению.

Для отмены выбранного задания и/или введенных данных можно либо воспользоваться комбинацией клавиш Ctrl + J, либо подменю «Отменить загруженный блок и выбрать …», содержащееся во вкладке «Учебный модуль» главного меню программы (доступно на любом этапе выполнения задания). В результате на экране появится окно подтверждения, предотвращающее непреднамеренную отмену выбранного задания и введенных данных (рисунок Б.3). При нажатии кнопки «Да» выполнение текущего учебного модуля завершается, все данные, введенные ранее, при этом будут отменены, а на экране появится окно выбора задания (см. рисунок 4). Для возврата в окно выполнения задания и продолжения выполнения текущего учебного модуля без сброса введенных ранее данных в окне подтверждения необходимо нажать кнопку «Нет».

2 Выберите задание «Схема генерации раундовых ключей DES на базе блоков *LS*» и ознакомьтесь с общим планом его выполнения.

Для выбора задания необходимо в окне, показанном на рисунке 4, последовательно указать следующее:

1) пункт «1 Глава:» – «СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ БЛОЧНОГО ТИПА»;

2) пункт «2 Раздел:» – «КРИПТОСИСТЕМА DES»;

3) пункт «3 Тема:» – «СХЕМА ГЕНЕРАЦИИ РАУНДОВЫХ КЛЮЧЕЙ DES НА БАЗЕ БЛОКОВ LS».

Затем нажмите кнопку «Перейти к заданию». В результате появится окно, содержащее общий план выполнения задания по изучению схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига влево *LS*, показанное на рисунке 5.

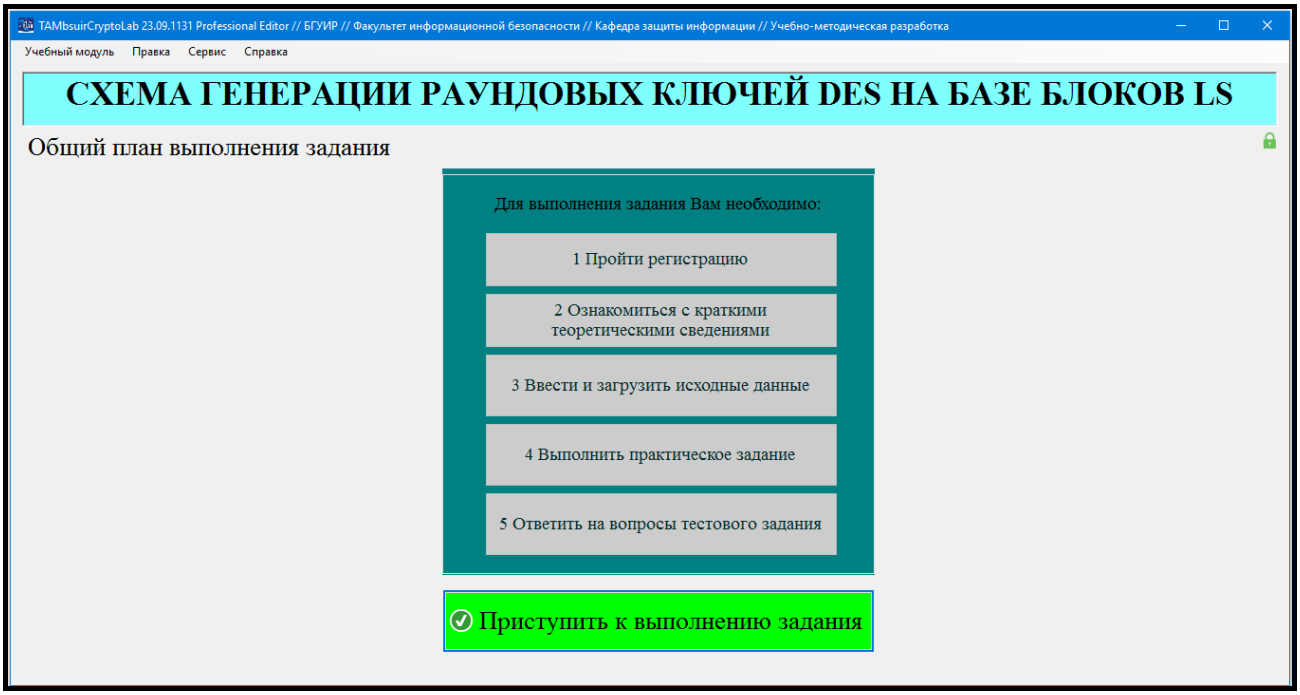


Рисунок 5 – Общий план выполнения задания по изучению схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига влево *LS*

3 Зарегистрируйтесь и ознакомьтесь с краткими теоретическими сведениями по функционированию схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига влево *LS*.

Для того чтобы зарегистрироваться, необходимо в окне с общим планом выполнения задания (см. рисунок 5) нажать кнопку «Приступить к выполнению задания» и в появившемся окне регистрации, приведенном на рисунке 6, указать номер своей группы в поле «1 Номер группы:», ввести свою фамилию и имя в поле «2 Фамилия и имя:» и нажать кнопку «Зарегистрироваться».

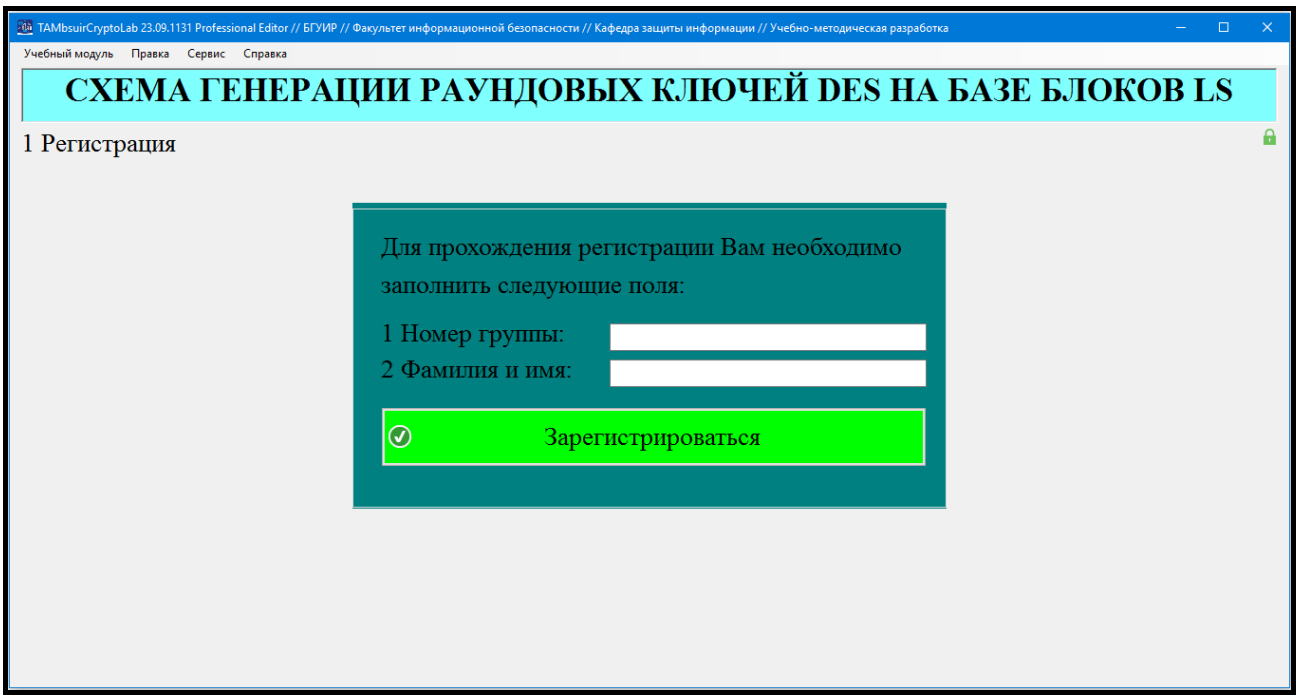


Рисунок 6 – Внешний вид окна регистрации, соответствующего этапу 1 общего плана задания по изучению схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига влево *LS*

После этого появится окно с краткими теоретическими сведениями, показанное на рисунке 7.

4 Загрузите исходные данные в соответствии с индивидуальным вариантом, который определяется преподавателем учебной дисциплины.

Для загрузки исходных данных необходимо в окне с краткими теоретическими сведениями (см. рисунок 7) нажать кнопку «Далее» и в появившемся окне ввода и загрузки исходных данных, приведенном на рисунке 8, ввести исходные данные и нажать кнопку «Загрузить исходные данные».

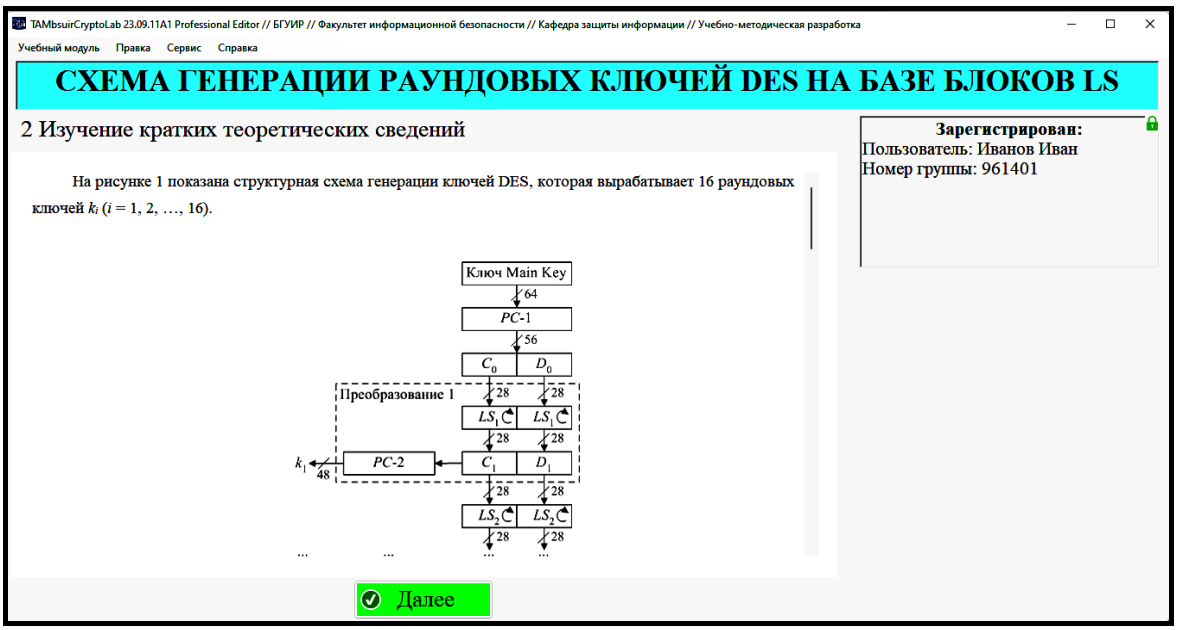


Рисунок 7 – Внешний вид окна с краткими теоретическими сведениями, соответствующего этапу 2 общего плана задания по изучению схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига влево *LS*

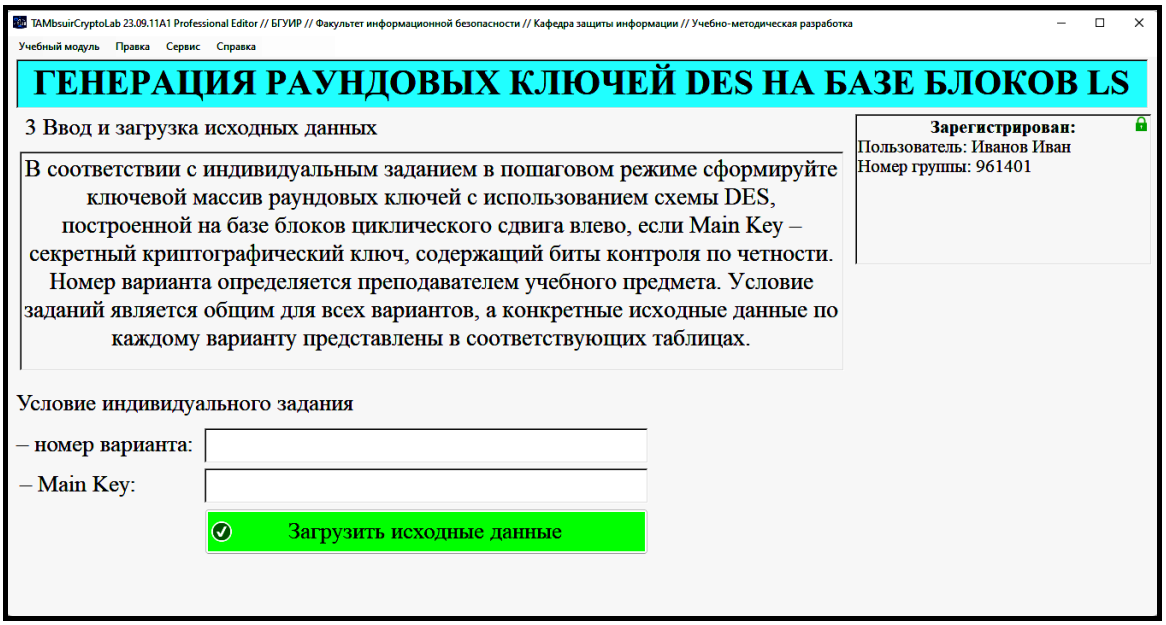


Рисунок 8 – Внешний вид окна ввода и загрузки исходных данных, соответствующего этапу 3 общего плана задания по изучению схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига влево *LS*

В результате на экране появится окно для изучения схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига влево *LS*, соответствующего этапу 4 общего плана задания, показанное на рисунке 9.

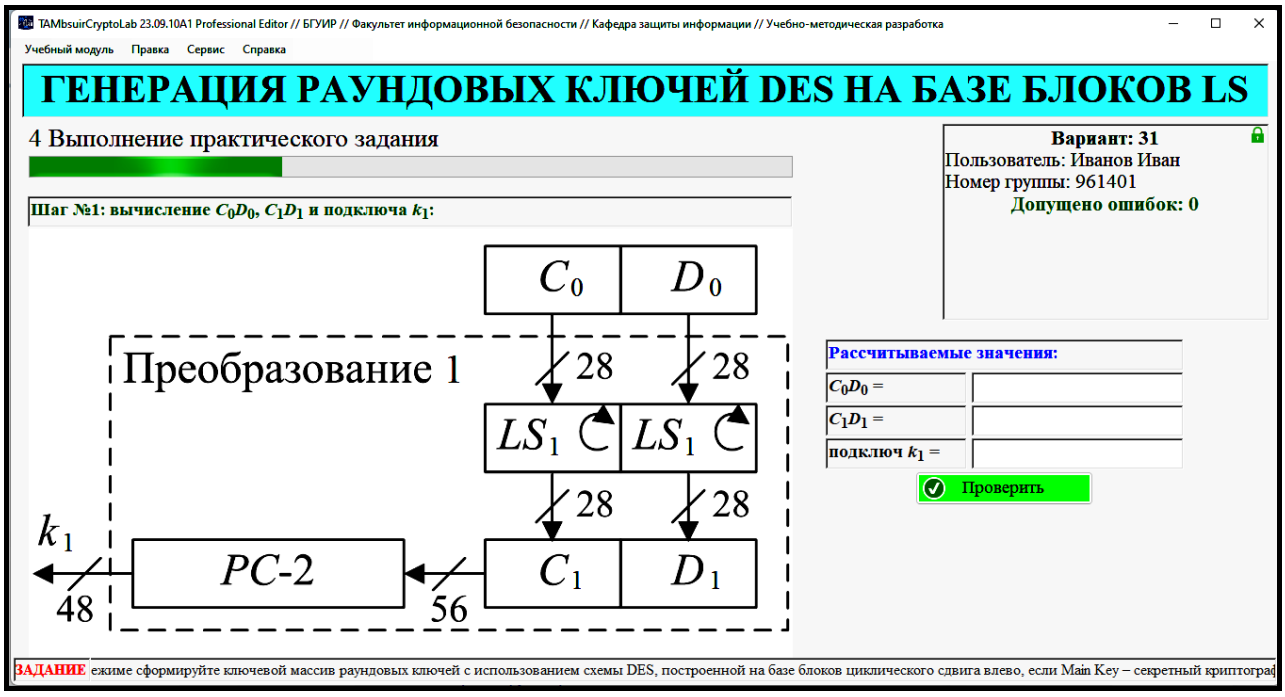


Рисунок 9 – Внешний вид окна для изучения
схемы генерации раундовых ключей DES, построенной
на базе блоков циклического сдвига влево *LS*

5 Выполните предлагаемые задания по изучению схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига влево *LS*.

Исходные данные к заданию приведены в приложении В.

Номер варианта задания определяется преподавателем учебной дисциплины. Условие заданий является общим для всех вариантов, а конкретные исходные данные по каждому варианту представлены в соответствующих таблицах.

Задание выполняется в окне, представленном на рисунке 9, и заключается в пошаговой генерации раундовых ключей DES с использованием схемы, построенной на базе блоков циклического сдвига влево *LS*. Для удобства работы с программой текст задания дублируется в нижней части этого окна в виде «бегущей» строки.

Суть выполнения каждого шага задания заключается в расчете и заполнении C_iD_i, а также раундовых ключей k_i (см. рисунок 9).

Чтобы проверить правильность выполнения каждого шага задания, необходимо нажать кнопку «Проверить».

Если одно или несколько значений рассчитаны неверно, на экран выводится сообщение об ошибке. В этом случае необходимо закрыть окно с сообщением об ошибке и повторно выполнить задание в окне изучения схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига влево *LS* (см. рисунок 9).

Задание по изучению схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига влево *LS*, считается выполненным, если все шаги завершены успешно.

В приложении И приведен пример расчета C_iD_i и раундовых ключей k_i (см. таблицу И.1).

6 Выполните тестовое задание, соответствующее этапу 5 общего плана задания.

Окно с тестовыми заданиями отображается автоматически после завершения этапа 4 общего плана задания. Тест содержит 10 вопросов. Необходимо ответить на все вопросы. Правильных ответов может быть несколько.

Тестовые задания считаются выполненными, если все предлагаемые задания завершены успешно.

7 Продемонстрируйте результаты выполнения задания преподавателю учебной дисциплины.

Задание считается выполненным, если пункты 1 – 6 практического задания завершены успешно. При этом на экран выводится окно, показанное на рисунке 10, а.

а

б

а – задание выполнено; б – задание не выполнено

Рисунок 10 – Заключительные результаты выполнения задания по изучению схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига влево *LS*

Задание считается невыполненным, если на экран выводится окно, показанное на рисунке 10, б. В этом случае необходимо отменить загруженный учебный модуль, нажав комбинацию клавиш «Ctrl + J», в появившемся окне (см. рисунок Б.3) подтвердить отмену, выбрав «Да», и заново выполнить пункты 2 – 7 практического задания.

1.3 Содержание отчета

1 Цель лабораторной работы.

2 Краткие теоретические сведения о работе схемы генерации криптографических подключей DES, построенной на базе блоков циклического сдвига влево *LS*.

3 Выводы по результатам выполнения практических заданий.

4 Ответы на контрольные вопросы.

1.4 Контрольные вопросы

1 Для чего используется схема генерации криптографических подключей DES, построенная на базе блоков циклического сдвига влево *LS*?

2 Какова длина в битах одного подключа DES в схеме генерации криптографических подключей DES, построенной на базе блоков циклического сдвига влево *LS*?

3 Сколько байт имеет основной ключ DES?

4 Какие математические операции используются в схеме генерации криптографических подключей DES, построенной на базе блоков циклического сдвига влево *LS*?

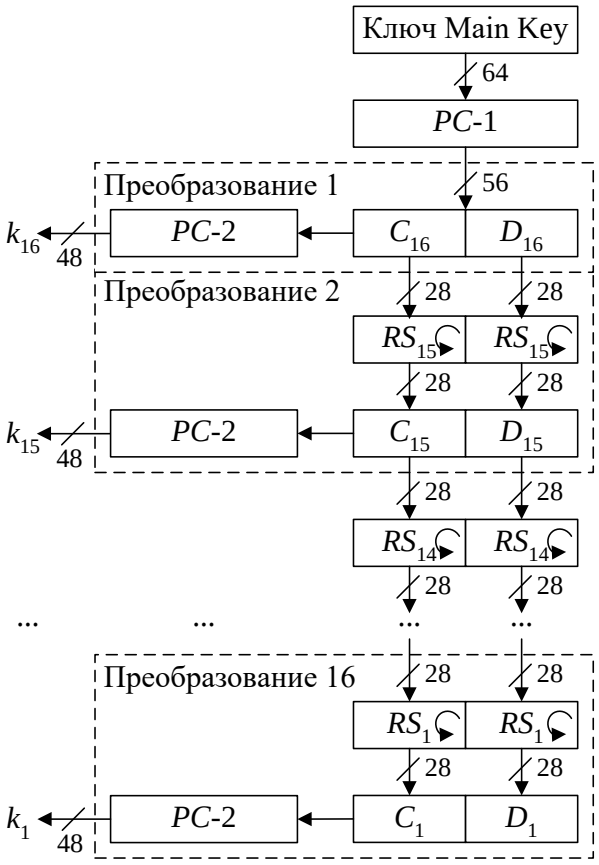
5 Насколько сложными для современных программных и программно-аппаратных средств являются математические операции, используемые в схеме генерации криптографических подключей DES, построенной на базе блоков циклического сдвига влево *LS*?

ЛАБОРАТОРНАЯ РАБОТА 2
СХЕМА ГЕНЕРАЦИИ РАУНДОВЫХ КЛЮЧЕЙ DES НА БАЗЕ БЛОКОВ *RS*

Цель: изучение схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига вправо *RS*.

2.1 Краткие теоретические сведения

На рисунке 11 показана структурная схема генерации ключей DES, которая вырабатывает 16 раундовых ключей.



На *i*-м преобразовании формируется k_{16-i+1} раундовый ключ (i = 1, 2, …, 16)

Рисунок 11 – Структурная схема генерации раундовых ключей DES на базе блоков циклического сдвига вправо *RS*

Каждый раундовый ключ k_{16-i+1} (где i – номер преобразования; i = 1, 2, …, 16, см. рисунок 11) состоит из 48 бит исходного секретного ключа Main Key. Ключ Main Key содержит 56 значащих бит и 8 проверочных бит для контроля на четность, расположенных в позициях 8, 16, 24, 32, 40, 48, 56, 64. Для удаления контрольных битов и подготовки ключа к работе используется функция первоначальной подготовки ключа *PC*-1, поясняемая рисунком 12.

57	49	41	33	25	17	9	C_{16}
1	58	50	42	34	26	18	
10	2	59	51	43	35	27	
19	11	3	60	52	44	36	
63	55	47	39	31	23	15	D_{16}
7	62	54	46	38	30	22	
14	6	61	53	45	37	29	
21	13	5	28	20	12	4	

Рисунок 12 – Функция первоначальной подготовки ключа *PC*-1

Функция первоначальной подготовки ключа *PC*-1, а также функция, завершающая подготовку ключа *PC*-2, в схеме генерации криптографических подключей DES на базе блоков циклического сдвига вправо *RS* выполняют аналогичные преобразования данных, как и в схеме на базе блоков циклического сдвига влево *LS*. При этом используется таблица 1, однако имеются следующие отличительные особенности. Функция *PC*-1, проиллюстрированная на рисунке 12, разделена на две части: C_{16} и D_{16} по 28 бит каждая. Первые четыре строки матрицы *PC*-1 определяют, как выбираются биты последовательности C_{16} (первым битом C_{16} будет бит 57 ключа Main Key, затем бит 49 и т. д., а последними битами – биты 44 и 36), а следующие четыре строки – биты последовательности D_{16} (первым битом D_{16} будет бит 63 ключа Main Key, затем бит 55 и т. д., а последними битами – биты 12 и 4).

Раундовый ключ k_{16}, определяемый на первом преобразовании (см. рисунок 11), есть результат выбора конкретных битов из 56-битовой последовательности $C_{16}D_{16}$ и их перестановки. Для этого используется функция, завершающая подготовку ключа *PC*-2, принцип функционирования которой поясняется рисунком 13.

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Рисунок 13 – Функция, завершающая подготовку ключа *PC*-2

На последующих преобразованиях (i = 2, 3, …, 16, см. рисунок 11) рекурсивно определяются C_{16-i+1} и D_{16-i+1} путем циклического сдвига вправо на один или два бита C_{16-i+2} и D_{16-i+2} соответственно в зависимости от номера преобразования, как показано в таблице 2.

Таблица 2 – Количество сдвигов для вычисления раундовых ключей

Номер преобразования	Количество сдвигов, бит	Номер преобразования	Количество сдвигов, бит
1	–	9	1
2	1	10	2
3	2	11	2
4	2	12	2
5	2	13	2
6	2	14	2
7	2	15	2
8	2	16	1

Операции циклического сдвига вправо выполняются для последовательностей C_{16-i+2} и D_{16-i+2} независимо (см. рисунок 11). Например, последовательность C_3 (преобразование 14) получается посредством циклического сдвига вправо на две позиции последовательности C_4,

последовательность D_3 – посредством циклического сдвига вправо на две позиции последовательности D_4, а C_1 и D_1 (преобразование 16) получаются из C_2 и D_2 посредством циклического сдвига вправо на одну позицию (см. таблицу 2).

Раундовый ключ k_{16-i+1}, определяемый на преобразованиях 2 – 16 (см. рисунок 11), есть результат выбора конкретных битов из 56-битовой последовательности $C_{16-i+1}D_{16-i+1}$ и их перестановки, что реализуется функцией, завершающей подготовку ключа *PC*-2 (см. рисунок 13). Таким образом, первым битом ключа раундового ключа k_{16-i+1}, будет 14-й бит последовательности $C_{16-i+1}D_{16-i+1}$, вторым – 17-й бит, и т. д., а последним – 32-й бит.

2.2 Практическое задание

1 Включите персональный компьютер и запустите файл «TAMbsuirCryptoLab.exe» на выполнение.

После запуска файла «TAMbsuirCryptoLab.exe» активизируется программное обеспечение, и появится окно выбора задания для выполнения (см. рисунок 1).

2 Выберите задание «Схема генерации раундовых ключей DES на базе блоков *RS*» и ознакомьтесь с общим планом его выполнения.

Для выбора задания необходимо в окне, показанном на рисунке 1, последовательно указать следующее:

1) пункт «1 Глава:» – «СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ БЛОЧНОГО ТИПА»;

2) пункт «2 Раздел:» – «КРИПТОСИСТЕМА DES»;

3) пункт «3 Тема:» – «СХЕМА ГЕНЕРАЦИИ РАУНДОВЫХ КЛЮЧЕЙ DES НА БАЗЕ БЛОКОВ RS».

Затем нажмите кнопку «Перейти к заданию». В результате появится окно, содержащее общий план выполнения задания по изучению схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига вправо *RS*, показанное на рисунке 14.

Рисунок 14 – Общий план выполнения задания по изучению схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига вправо *RS*

3 Зарегистрируйтесь и ознакомьтесь с краткими теоретическими сведениями по функционированию схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига вправо *RS*.

Для того чтобы зарегистрироваться, необходимо в окне с общим планом выполнения задания (см. рисунок 14) нажать кнопку «Приступить к выполнению задания» и в появившемся окне регистрации, приведенном на рисунке 15, указать номер своей группы в поле «1 Номер группы:», ввести свою фамилию и имя в поле «2 Фамилия и имя:» и нажать кнопку «Зарегистрироваться».

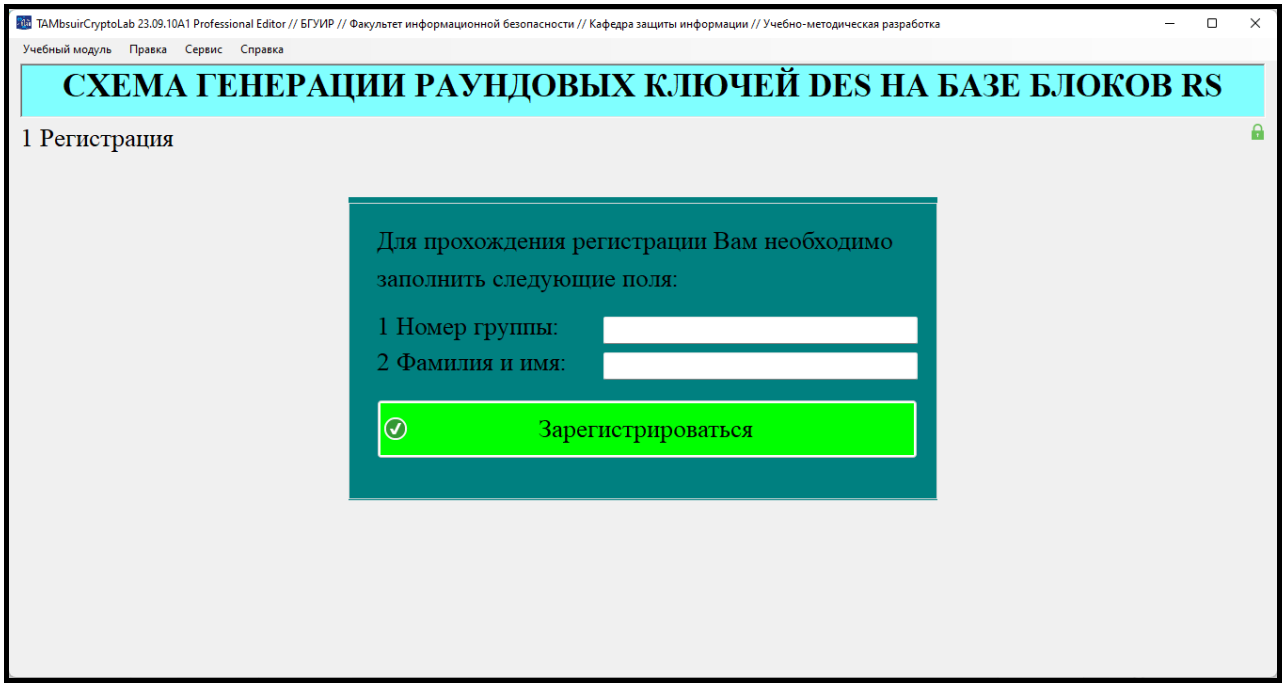


Рисунок 15 – Внешний вид окна регистрации, соответствующего этапу 1 общего плана задания по изучению схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига вправо *RS*

После этого появится окно с краткими теоретическими сведениями, показанное на рисунке 16.

4 Загрузите исходные данные в соответствии с индивидуальным вариантом, который определяется преподавателем учебной дисциплины.

Для загрузки исходных данных необходимо в окне с краткими теоретическими сведениями (см. рисунок 16) нажать кнопку «Далее» и в появившемся окне ввода и загрузки исходных данных, приведенном на рисунке 17, ввести исходные данные и нажать кнопку «Загрузить исходные данные».

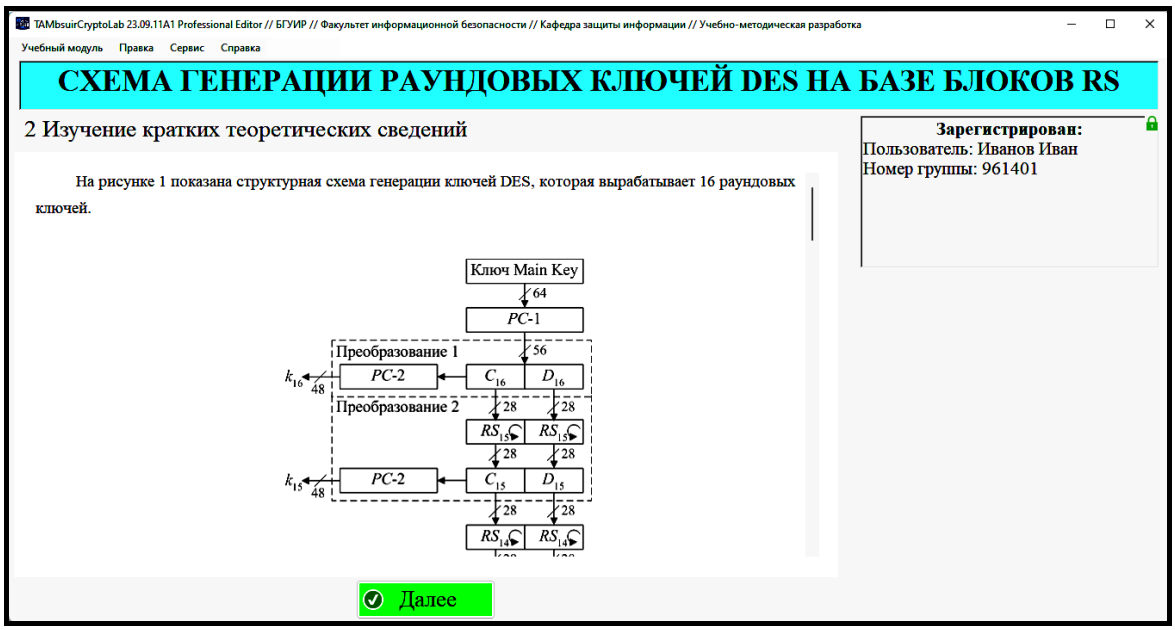


Рисунок 16 – Внешний вид окна с краткими теоретическими сведениями, соответствующего этапу 2 общего плана задания по изучению схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига вправо *RS*

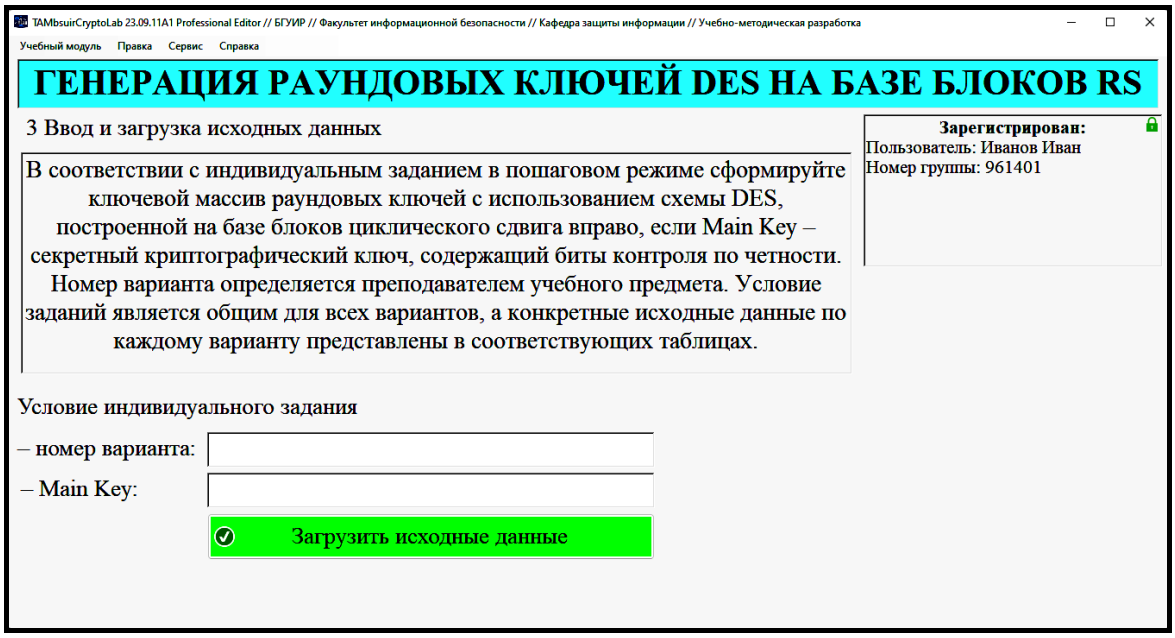


Рисунок 17 – Внешний вид окна ввода и загрузки исходных данных, соответствующего этапу 3 общего плана задания по изучению схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига вправо *RS*

В результате на экране появится окно для изучения схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига вправо *RS*, соответствующего этапу 4 общего плана задания, показанное на рисунке 18.

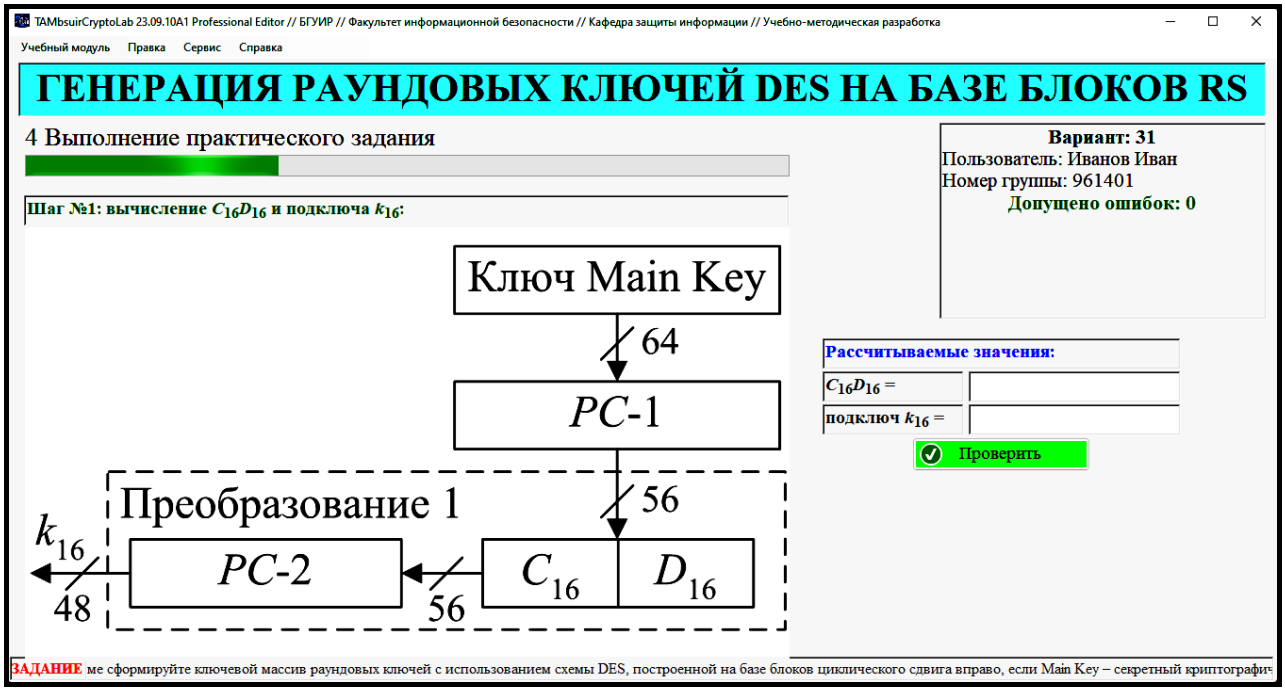


Рисунок 18 – Внешний вид окна для изучения
схемы генерации раундовых ключей DES, построенной
на базе блоков циклического сдвига вправо *RS*

5 Выполните предлагаемые задания по изучению схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига вправо *RS*.

Исходные данные к заданию приведены в приложении Г.

Номер варианта задания определяется преподавателем учебной дисциплины. Условие заданий является общим для всех вариантов, а конкретные исходные данные по каждому варианту представлены в соответствующих таблицах.

Задание выполняется в окне, представленном на рисунке 18, и заключается в пошаговой генерации раундовых ключей DES с использованием схемы, построенной на базе блоков циклического сдвига вправо *RS*. Для удобства работы с программой текст задания дублируется в нижней части этого окна в виде «бегущей» строки.

Суть выполнения каждого шага задания заключается в расчете и заполнении C_iD_i, а также раундовых ключей k_i (см. рисунок 18).

Чтобы проверить правильность выполнения каждого шага задания, необходимо нажать кнопку «Проверить».

Если одно или несколько значений рассчитаны неверно, на экран выводится сообщение об ошибке. В этом случае необходимо закрыть окно с сообщением об ошибке и повторно выполнить задание в окне изучения схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига вправо *RS* (см. рисунок 18).

Задание по изучению схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига вправо *RS*, считается выполненным, если все шаги завершены успешно.

В приложении И приведен пример расчета C_iD_i и раундовых ключей k_i (см. таблицу И.2).

6 Выполните тестовое задание, соответствующее этапу 5 общего плана задания.

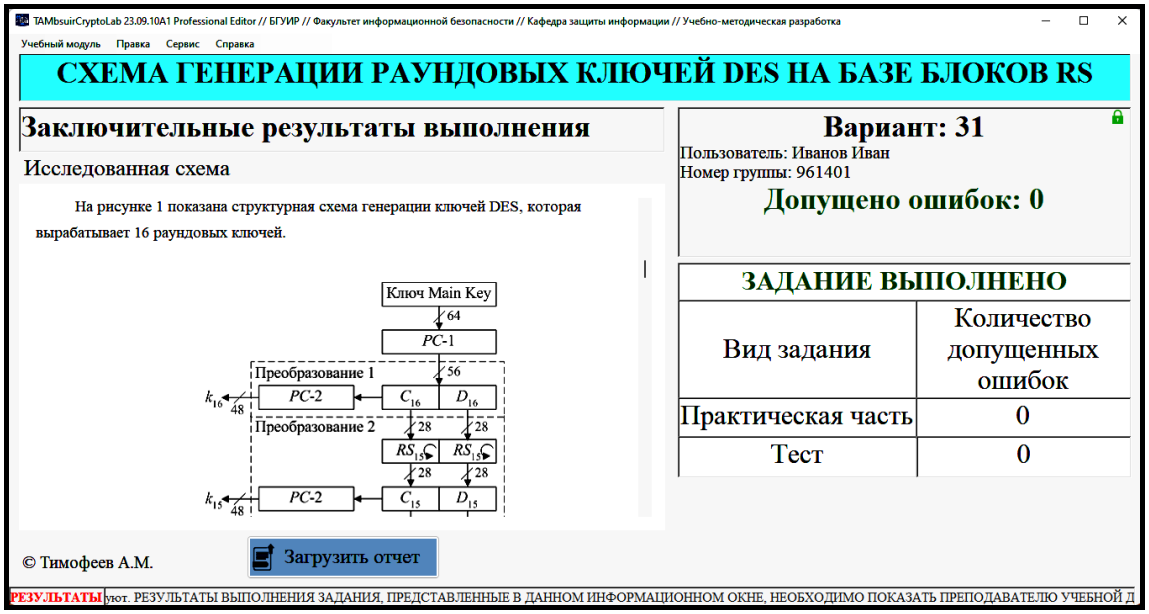
Окно с тестовыми заданиями отображается автоматически после завершения этапа 4 общего плана задания. Тест содержит 10 вопросов. Необходимо ответить на все вопросы. Правильных ответов может быть несколько.

Тестовые задания считаются выполненными, если все предлагаемые задания завершены успешно.

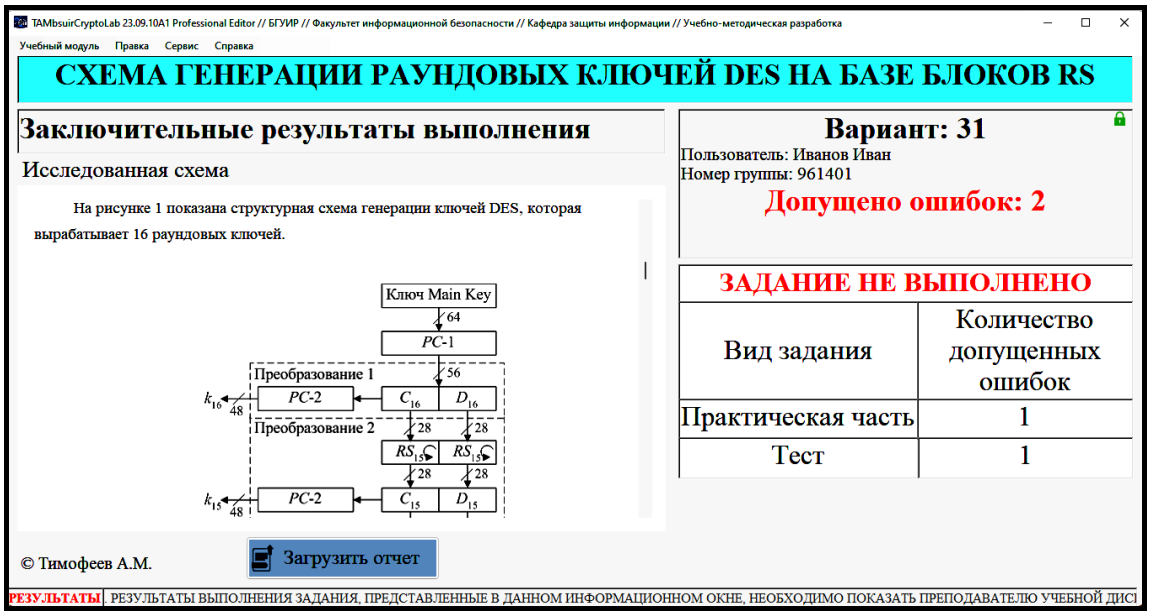
7 Продемонстрируйте результаты выполнения задания преподавателю учебной дисциплины.

Задание считается выполненным, если пункты 1 – 6 практического задания завершены успешно. При этом на экран выводится окно, показанное на рисунке 19, а.

а



б



а – задание выполнено; б – задание не выполнено

Рисунок 19 – Заключительные результаты выполнения задания по изучению схемы генерации раундовых ключей DES, построенной на базе блоков циклического сдвига вправо *RS*

Задание считается невыполненным, если на экран выводится окно, показанное на рисунке 19, б. В этом случае необходимо отменить загруженный учебный модуль, нажав комбинацию клавиш «Ctrl + J», в появившемся окне (см. рисунок Б.3) подтвердить отмену, выбрав «Да», и заново выполнить пункты 2 – 7 практического задания.

2.3 Содержание отчета

1 Цель лабораторной работы.

2 Краткие теоретические сведения о работе схемы генерации криптографических подключей DES, построенной на базе блоков циклического сдвига вправо *RS*.

3 Выводы по результатам выполнения практических заданий.

4 Ответы на контрольные вопросы.

2.4 Контрольные вопросы

1 Для чего используется схема генерации криптографических подключей DES, построенная на базе блоков циклического сдвига вправо *RS*?

2 Какова длина в битах одного подключа DES в схеме генерации криптографических подключей DES, построенной на базе блоков циклического сдвига вправо *RS*?

3 В чем отличия преобразования 1 в схемах генерации криптографических подключей DES, построенных на базе блоков циклического сдвига вправо *RS* и влево *LS*?

4 Какие математические операции используются в схеме генерации криптографических подключей DES, построенной на базе блоков циклического сдвига вправо *RS*?

5 Насколько сложными для современных программных и программно-аппаратных средств являются математические операции, используемые в схеме генерации криптографических подключей DES, построенной на базе блоков циклического сдвига вправо *RS*?

ЛАБОРАТОРНАЯ РАБОТА 3
DES В РЕЖИМЕ ЗАШИФРОВАНИЯ ДАННЫХ

Цель: изучение схемы зашифрования данных DES.

3.1 Краткие теоретические сведения

Структурная схема алгоритма DES в режиме зашифрования данных приведена на рисунке 20.

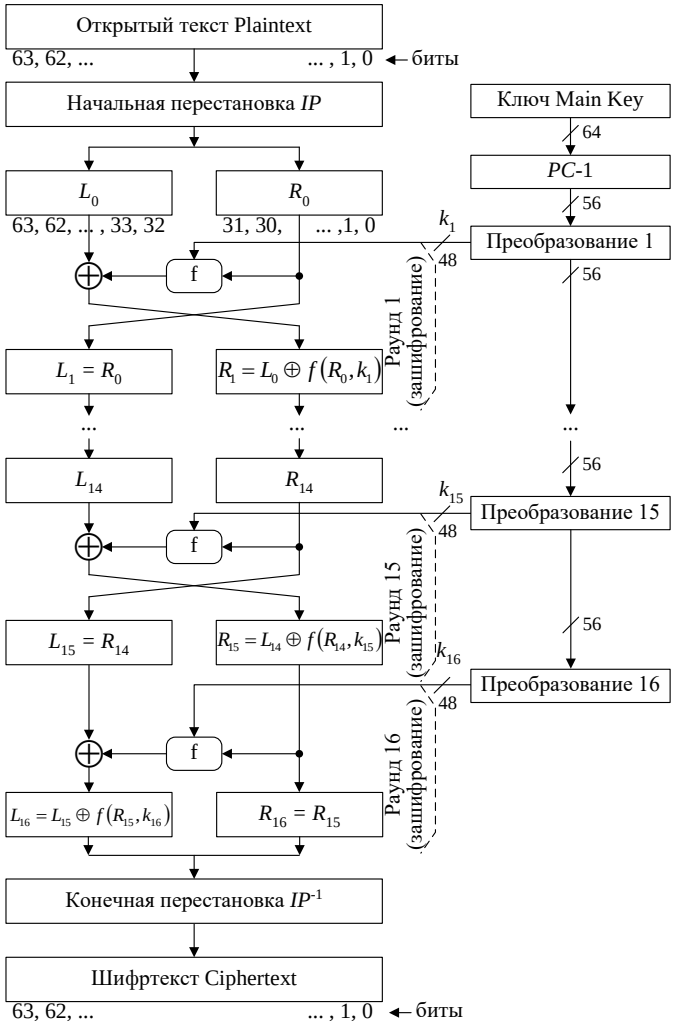


Рисунок 20 – Структурная схема алгоритма DES
в режиме зашифрования данных

Алгоритм DES использует комбинацию подстановок и перестановок и осуществляет шифрование 64-битовых блоков данных с помощью 64-битового ключа, в котором значащими являются 56 бит (см. лабораторную работу 1).

Процесс зашифрования данных DES заключается в следующем.

Данные, подлежащие зашифрованию (биты открытого текста Plaintext), переставляются в соответствии с матрицей начальной перестановки *IP*. Полученная последовательность разделяется на две части: L_0 – левые или старшие биты и R_0 – правые или младшие биты, каждая из которых содержит по 32 бита.

Затем выполняется итеративный процесс зашифрования, состоящий из шестнадцати циклов (раундов). Пусть T_i – результат i-й итерации ($i = 1, 2, \ldots, 16$). Тогда

$$T_i = L_i R_i, \tag{1}$$

где $L_i = t_1, t_2, \ldots, t_{32}$ – первые 32 бита;

$R_i = t_{33}, t_{34}, \ldots, t_{64}$ – последние 32 бита.

Результат i-й итерации L_iR_i описывается следующими системами:

$$\begin{cases} L_i = R_{i-1}, \\ R_i = L_{i-1} \oplus f\left(R_{i-1}, k_i\right), \end{cases} i = 1,2,\ldots,15;$$
$$\begin{cases} L_{16} = L_{15} \oplus f\left(R_{15}, k_{15}\right), \\ R_{16} = R_{15}. \end{cases} \tag{2}$$

Функция f называется функцией шифрования. Ее аргументами являются последовательность R_{i-1}, получаемая на предыдущем шаге итерации, и 48-битовый раундовый ключ k_i, который является результатом

преобразования 64-битового секретного ключа Main Key (см. лабораторную работу 1).

На последнем шаге итерации получают последовательности R_{16} и L_{16} (без перестановки местами), которые конкатенируются в 64-битовую последовательность $R_{16}L_{16}$.

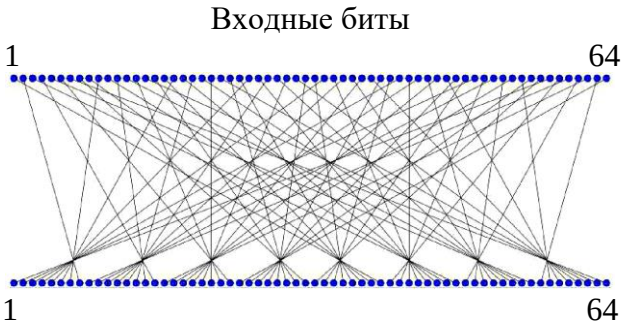
По окончании шифрования осуществляется восстановление позиций битов с помощью матрицы конечной перестановки IP^{-1}, в результате чего формируется шифртекст Ciphertext (см. рисунок 20).

Матрицы начальной IP и конечной IP^{-1} перестановки битов.

Матрицы начальной и конечной перестановки битов поясняются рисунком 21.

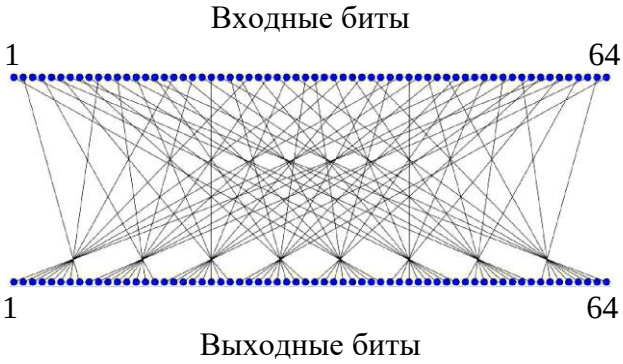
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

а



40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

б



а – начальная перестановка *IP*; б – конечная (обратная) перестановка IP^{-1}

Рисунок 21 – Матрицы начальной и конечной перестановки битов

Биты входного блока Plaintext (64 бита) переставляются в соответствии с матрицей *IP*: бит 58 Plaintext становится битом 1, бит 50 – битом 2 и т. д. По окончании шестнадцати раундов шифрования осуществляется восстановление позиций битов с помощью матрицы обратной перестановки IP^{-1}, показанной на рисунке 21, б: бит 40 становится битом 1, бит 8 – битом 2 и т. д.

Функция шифрования f.

Схема вычисления функции шифрования $f(R_{i-1}, k_i)$ показана на рисунке 22.

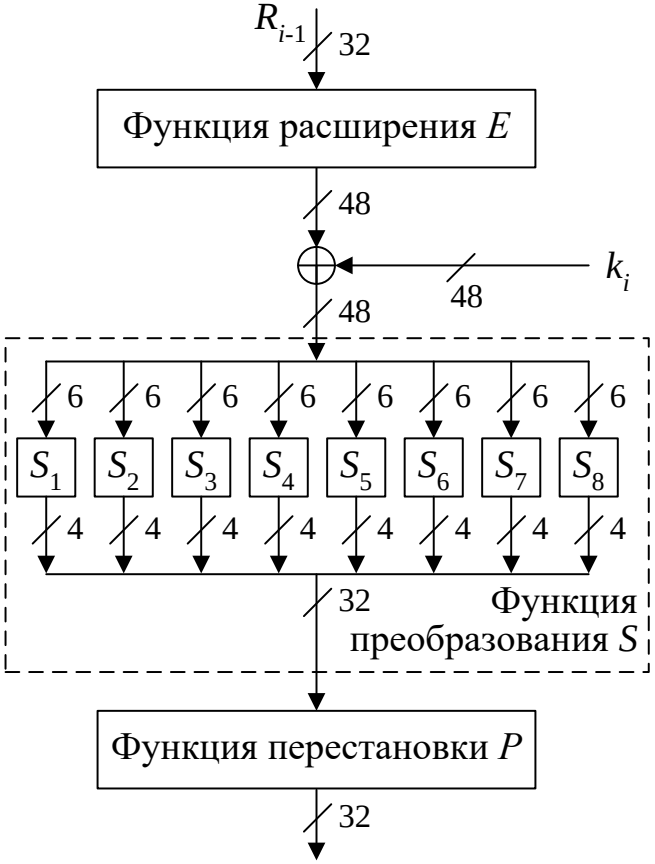


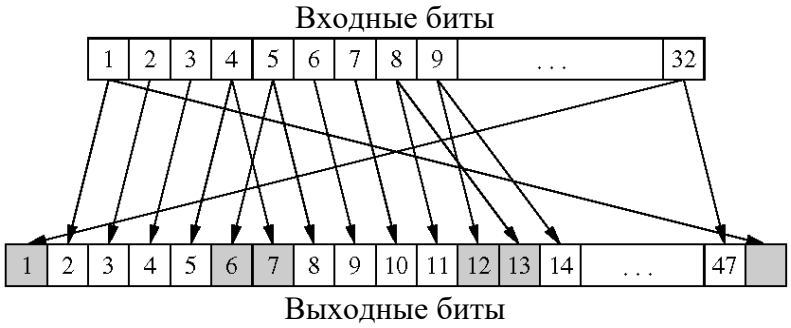
Рисунок 22 – Схема вычисления функции шифрования *f*

Аргументами функции шифрования f являются R_{i-1} (32 бита) и k_i (48 бит). Функция f, в свою очередь, содержит три функции: расширения E, преобразования S и перестановки P.

Функция расширения E увеличивает количество битов правой части R_{i-1} с 32-х до 48 в соответствии с правилами, иллюстрируемыми рисунком 23.

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

а



б

а – матрица функции E; б – пример преобразования входных битов в выходные

Рисунок 23 – Вычисление функции расширения E

Полученный результат $E(R_{i-1})$ складывается по модулю 2 с текущим значением раундового ключа k_i и затем разбивается на восемь 6-битовых блоков B_1, B_2,…, B_8 (см. рисунок 22). Далее каждый из этих блоков используется как номер элемента в функции преобразования S, содержащей восемь матриц S_1, S_2,…, S_8. Вычисление функции преобразования S поясняется рисунком 24.

Номер столбца

Номер строки	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S_1
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	S_2
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	S_3
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	S_4
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	S_5
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	S_6
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	S_7
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	S_8
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

Значения приведены в десятичном коде

Рисунок 24 – Функция преобразования *S*

Пусть на вход матрицы S_j поступает 6-битовый блок $B_j = b_1\ b_2\ b_3\ b_4\ b_5\ b_6$. Тогда 2-битовое число $b_1\ b_6$ указывает номер строки матрицы, а 4-битовое число $b_2\ b_3\ b_4\ b_5$ – номер столбца. В результате получаем $S_1(B_1)\ S_2(B_2)\ \ldots\ S_8(B_8)$ в виде 32-битового блока, поскольку матрицы S_1 – S_8 содержат 4-битовые элементы. Этот 32-битовый блок преобразуется с помощью функции перестановки P, приведенной на рисунке 25.

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Рисунок 25 – Функция перестановки P

Как видно из рисунка 25, бит 16 становится первым выходным битом функции перестановки P, бит 7 – вторым и т. д. Выходное значение функции перестановки P является результатом функции шифрования $f(R_{i-1}, k_i)$.

3.2 Практическое задание

1 Включите персональный компьютер и запустите файл «TAMbsuirCryptoLab.exe» на выполнение.

После запуска файла «TAMbsuirCryptoLab.exe» активизируется программное обеспечение, и появится окно выбора задания для выполнения (см. рисунок 1).

2 Выберите задание «DES в режиме зашифрования данных» и ознакомьтесь с общим планом его выполнения.

Для выбора задания необходимо в окне, показанном на рисунке 1, последовательно указать следующее:

1) пункт «1 Глава:» – «СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ БЛОЧНОГО ТИПА»;

2) пункт «2 Раздел:» – «КРИПТОСИСТЕМА DES»;

3) пункт «3 Тема:» – «DES В РЕЖИМЕ ЗАШИФРОВАНИЯ ДАННЫХ».

Затем нажмите кнопку «Перейти к заданию». В результате появится окно, содержащее общий план выполнения задания по изучению схемы зашифрования данных DES, показанное на рисунке 26.

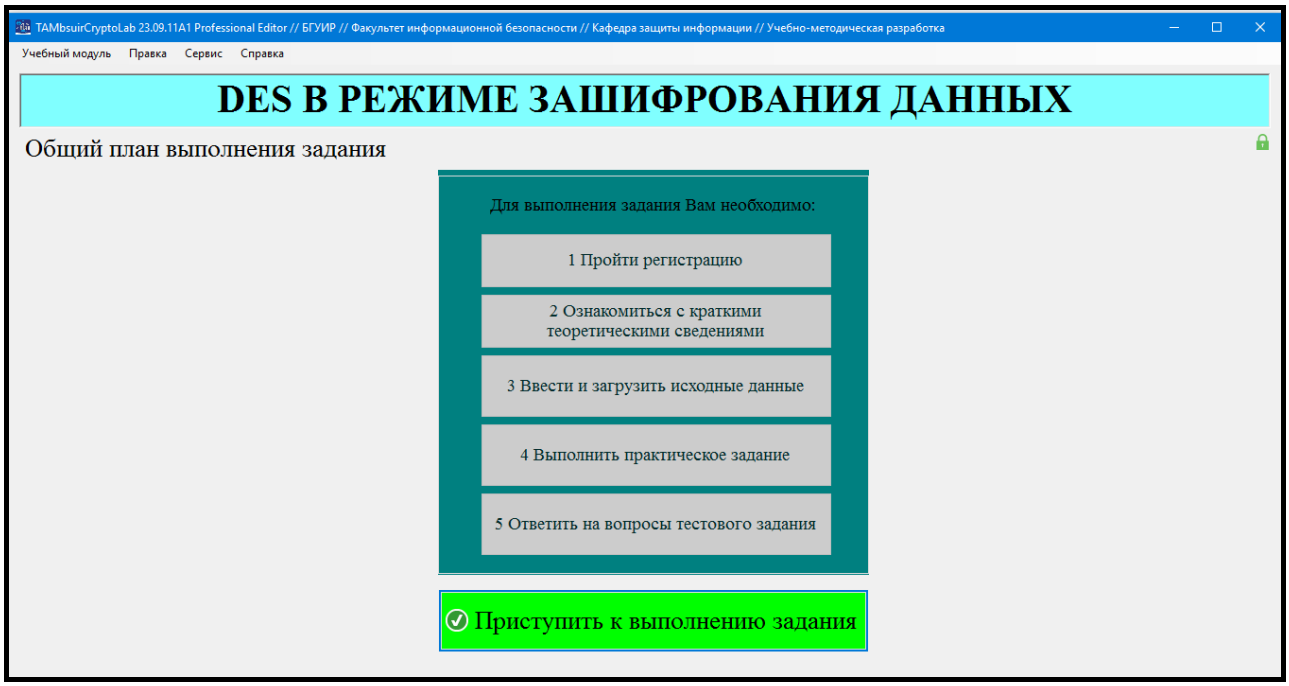


Рисунок 26 – Общий план выполнения задания
по изучению схемы зашифрования данных DES

3 Зарегистрируйтесь и ознакомьтесь с краткими теоретическими сведениями по функционированию схемы зашифрования данных DES.

Для того чтобы зарегистрироваться, необходимо в окне с общим планом выполнения задания (см. рисунок 26) нажать кнопку «Приступить к выполнению задания» и в появившемся окне регистрации, приведенном на рисунке 27, указать номер своей группы в поле «1 Номер группы:», ввести свою фамилию и имя в поле «2 Фамилия и имя:» и нажать кнопку «Зарегистрироваться».

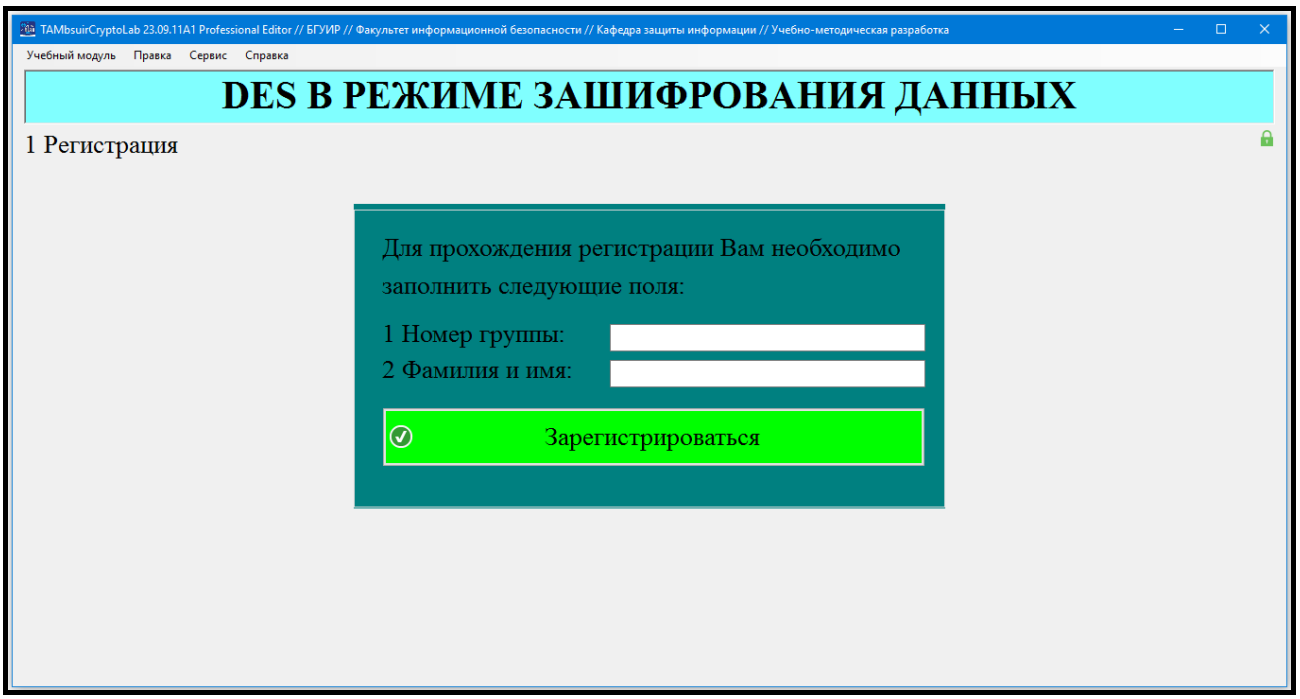


Рисунок 27 – Внешний вид окна регистрации,
соответствующего этапу 1 общего плана задания
по изучению схемы зашифрования данных DES

После этого появится окно с краткими теоретическими сведениями, показанное на рисунке 28.

4 Загрузите исходные данные в соответствии с индивидуальным вариантом, который определяется преподавателем учебной дисциплины.

Для загрузки исходных данных необходимо в окне с краткими теоретическими сведениями (см. рисунок 28) нажать кнопку «Далее» и в появившемся окне ввода и загрузки исходных данных, приведенном на рисунке 29, ввести исходные данные и нажать кнопку «Загрузить исходные данные».

Рисунок 28 – Внешний вид окна с краткими теоретическими сведениями, соответствующего этапу 2 общего плана задания по изучению схемы зашифрования данных DES

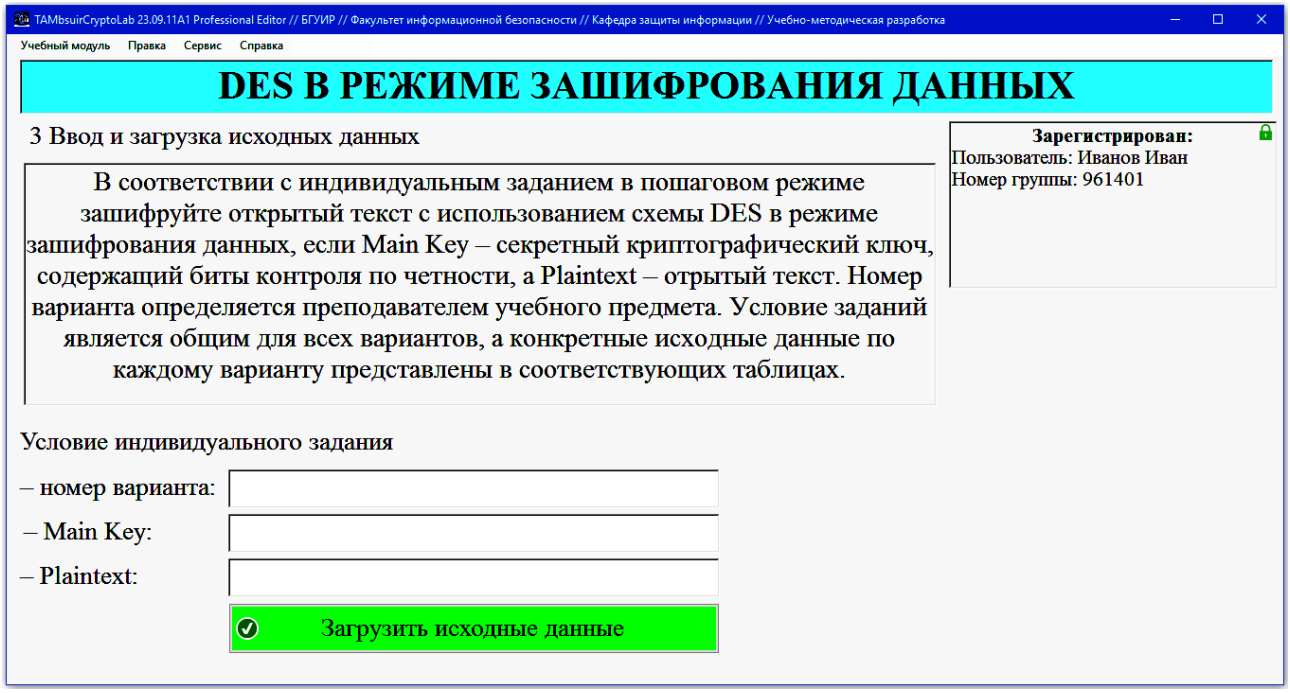


Рисунок 29 – Внешний вид окна ввода и загрузки исходных данных, соответствующего этапу 3 общего плана задания по изучению схемы зашифрования данных DES

В результате на экране появится окно для изучения схемы зашифрования данных DES, соответствующего этапу 4 общего плана задания, показанное на рисунке 30.

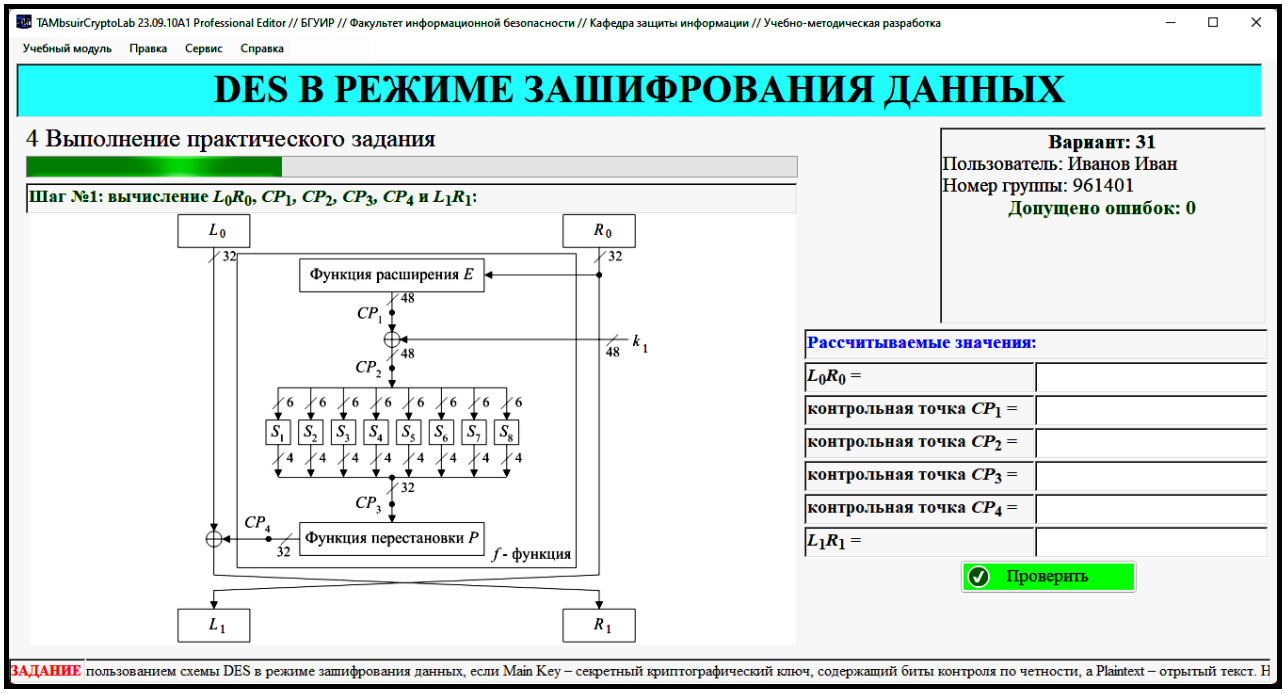


Рисунок 30 – Внешний вид окна по изучению
схемы зашифрования данных DES

5 Выполните предлагаемые задания по изучению схемы зашифрования данных DES.

Исходные данные к заданию приведены в приложении Д.

Номер варианта задания определяется преподавателем учебной дисциплины. Условие заданий является общим для всех вариантов, а конкретные исходные данные по каждому варианту представлены в соответствующих таблицах.

Задание выполняется в окне, представленном на рисунке 30, и заключается в пошаговом зашифровании данных с использованием стандарта

DES. Для удобства работы с программой текст задания дублируется в нижней части этого окна в виде «бегущей» строки.

Суть выполнения каждого шага задания заключается в расчете и заполнении L_iR_i, контрольных точек CP_1 – CP_4, а также шифртекста Ciphertext (см. рисунки 20 и 30).

Чтобы проверить правильность выполнения каждого шага задания, необходимо нажать кнопку «Проверить».

Если одно или несколько значений рассчитаны неверно, на экран выводится сообщение об ошибке. В этом случае необходимо закрыть окно с сообщением об ошибке и повторно выполнить задание в окне изучения схемы зашифрования данных DES (см. рисунок 30).

Задание по изучению схемы зашифрования данных DES считается выполненным, если все шаги завершены успешно.

В приложении И приведен пример расчета L_iR_i и шифртекста Ciphertext (см. таблицу И.3).

6 Выполните тестовое задание, соответствующее этапу 5 общего плана задания.

Окно с тестовыми заданиями отображается автоматически после завершения этапа 4 общего плана задания. Тест содержит 10 вопросов. Необходимо ответить на все вопросы. Правильных ответов может быть несколько.

Тестовые задания считаются выполненными, если все предлагаемые задания завершены успешно.

7 Продемонстрируйте результаты выполнения задания преподавателю учебной дисциплины.

Задание считается выполненным, если пункты 1 – 6 практического задания завершены успешно. При этом на экран выводится окно, показанное на рисунке 31, а.

а

б

а – задание выполнено; б – задание не выполнено

Рисунок 31 – Заключительные результаты выполнения задания по изучению схемы схемы зашифрования данных DES

Задание считается невыполненным, если на экран выводится окно, показанное на рисунке 31, б. В этом случае необходимо отменить загруженный учебный модуль, нажав комбинацию клавиш «Ctrl + J», в появившемся окне (см. рисунок Б.3) подтвердить отмену, выбрав «Да», и заново выполнить пункты 2 – 7 практического задания.

3.3 Содержание отчета

1 Цель лабораторной работы.

2 Краткие теоретические сведения о работе схемы зашифрования данных DES.

3 Выводы по результатам выполнения практических заданий.

4 Ответы на контрольные вопросы.

3.4 Контрольные вопросы

1 Сколько раундов шифрования данных выполняется схемой DES?

2 Что выполняет функция Expansion Function *E*?

3 Какие данные подаются на вход *f*-Function?

4 Как работают блоки *S*-boxes?

5 Что выполняет блок *P*?

ЛАБОРАТОРНАЯ РАБОТА 4
DES В РЕЖИМЕ РАСШИФРОВАНИЯ ШИФРТЕКСТОВ

Цель: изучение схемы расшифрования шифртекстов DES.

4.1 Краткие теоретические сведения

Структурная схема алгоритма DES в режиме расшифрования шифртекстов приведена на рисунке 32.

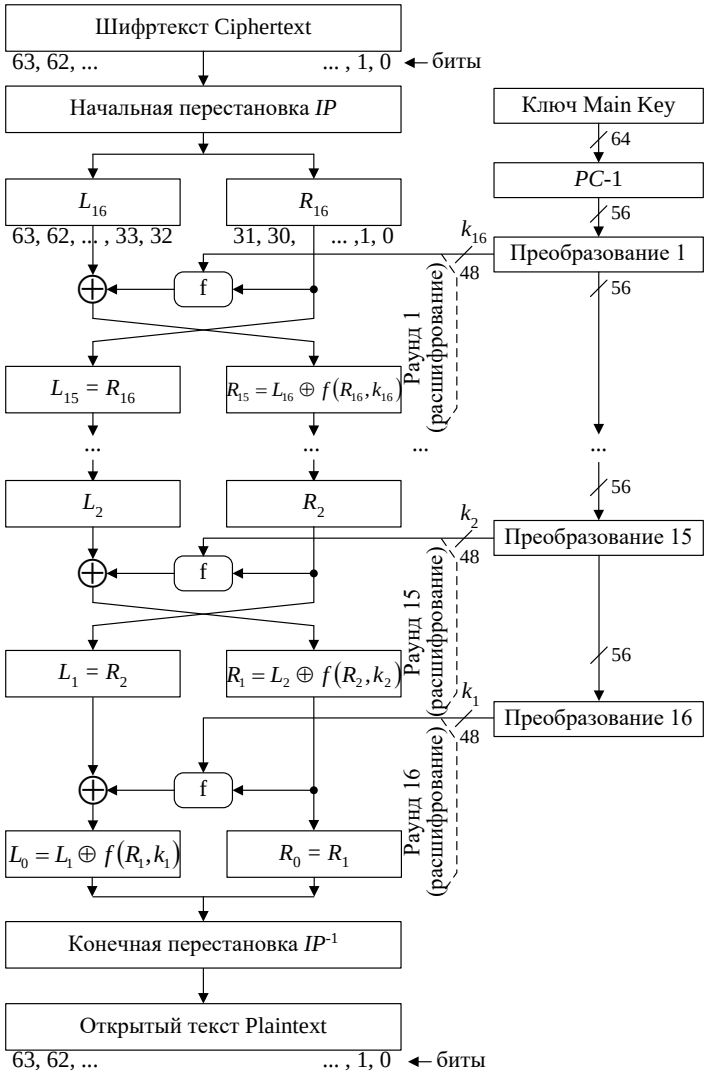


Рисунок 32 – Структурная схема алгоритма DES
в режиме расшифрования шифртекстов

По сравнению со схемой зашифрования данных алгоритм DES в режиме расшифрования шифртекстов является инверсным. С учетом логики работы алгоритма DES это означает, что расшифровываемые данные (биты шифртекста Ciphertext) сначала переставляются в соответствии с матрицей начальной перестановки *IP*, а затем над полученной последовательностью битов $R_{16}L_{16}$ выполняются те же действия, что и в процессе зашифрования данных над последовательностью R_0L_0 при зашифровании данных.

Таким образом, итеративный процесс расшифрования шифртекстов DES может быть описан следующими системами:

$$\begin{cases} L_{i-1} = R_i, \\ R_{i-1} = L_i \oplus f\left(R_i, k_i\right). \end{cases}, i = 16,15,\ldots,2;$$
$$\begin{cases} L_0 = L_1 \oplus f\left(R_1, k_1\right), \\ R_0 = R_1. \end{cases} \quad (3)$$

Как видно из рисунка 32, на первой итерации используется раундовый ключ k_{16}, на второй итерации – k_{15} и т. д., а на шестнадцатой итерации – k_1.

На последнем шаге итерации получают последовательности R_0 и L_0 (без перестановки местами), которые конкатенируются в 64-битовую последовательность R_0L_0.

По окончании расшифрования осуществляется восстановление позиций битов с помощью матрицы конечной перестановки IP^{-1}, в результате чего формируются биты открытого текста Plaintext (см. рисунок 32).

4.2 Практическое задание

1 Включите персональный компьютер и запустите файл «TAMbsuirCryptoLab.exe» на выполнение.

После запуска файла «TAMbsuirCryptoLab.exe» активизируется программное обеспечение, и появится окно выбора задания для выполнения (см. рисунок 1).

2 Выберите задание «DES в режиме расшифрования шифртекстов» и ознакомьтесь с общим планом его выполнения.

Для выбора задания необходимо в окне, показанном на рисунке 1, последовательно указать следующее:

1) пункт «1 Глава:» – «СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ БЛОЧНОГО ТИПА»;

2) пункт «2 Раздел:» – «КРИПТОСИСТЕМА DES»;

3) пункт «3 Тема:» – «DES В РЕЖИМЕ РАСШИФРОВАНИЯ ШИФРТЕКСТОВ».

Затем нажмите кнопку «Перейти к заданию». В результате появится окно, содержащее общий план выполнения задания по изучению схемы расшифрования шифртекстов DES, показанное на рисунке 33.

3 Зарегистрируйтесь и ознакомьтесь с краткими теоретическими сведениями по функционированию схемы расшифрования шифртекстов DES.

Для того чтобы зарегистрироваться, необходимо в окне с общим планом выполнения задания (см. рисунок 33) нажать кнопку «Приступить к выполнению задания» и в появившемся окне регистрации, приведенном на рисунке 34, указать номер своей группы в поле «1 Номер группы:»,

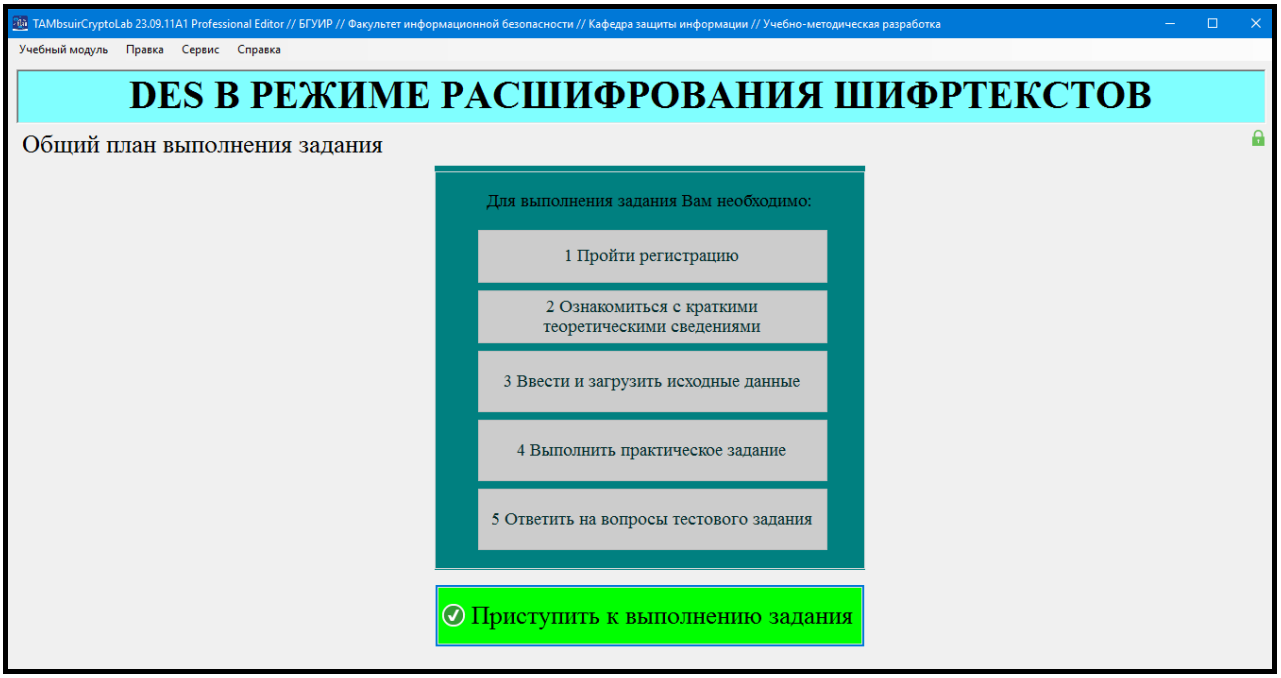


Рисунок 33 – Общий план выполнения задания
по изучению схемы расшифрования шифртекстов DES

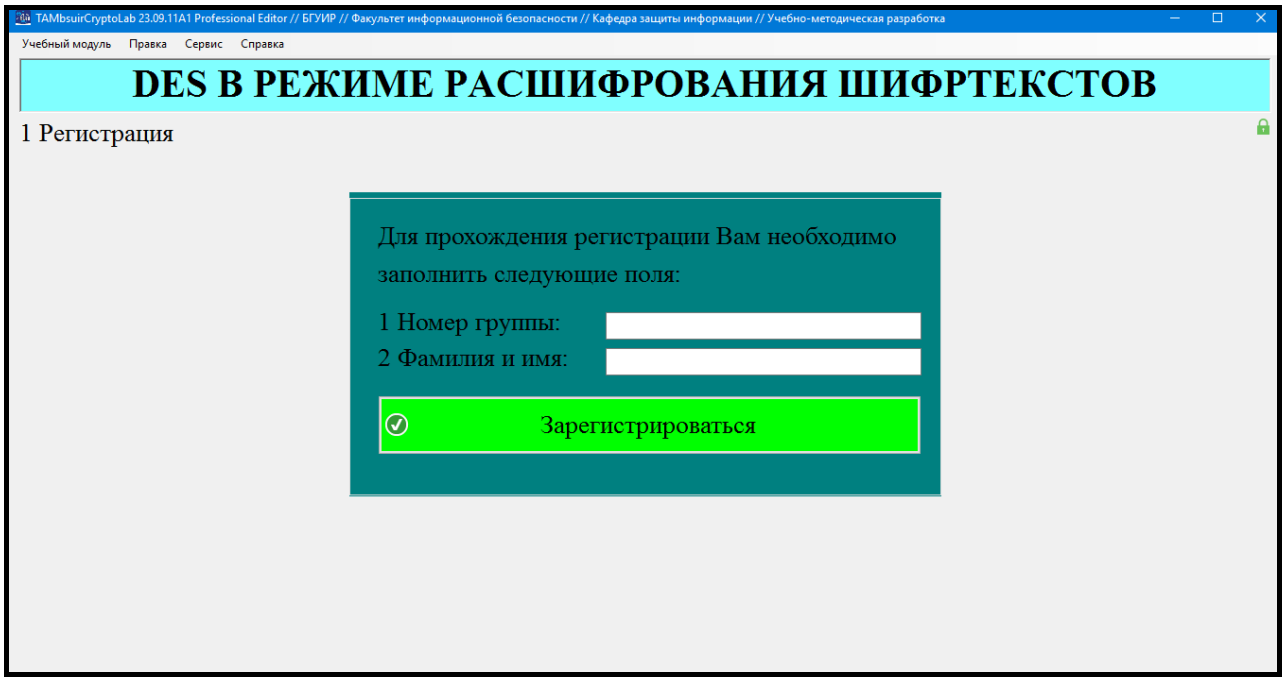


Рисунок 34 – Внешний вид окна регистрации,
соответствующего этапу 1 общего плана задания
по изучению схемы расшифрования шифртекстов DES

ввести свою фамилию и имя в поле «2 Фамилия и имя:» и нажать кнопку «Зарегистрироваться».

После этого появится окно с краткими теоретическими сведениями, показанное на рисунке 35.

Рисунок 35 – Внешний вид окна с краткими теоретическими сведениями, соответствующего этапу 2 общего плана задания по изучению схемы расшифрования шифртекстов DES

4 Загрузите исходные данные в соответствии с индивидуальным вариантом, который определяется преподавателем учебной дисциплины.

Для загрузки исходных данных необходимо в окне с краткими теоретическими сведениями (см. рисунок 35) нажать кнопку «Далее» и в появившемся окне ввода и загрузки исходных данных, приведенном на рисунке 36, ввести исходные данные и нажать кнопку «Загрузить исходные данные».

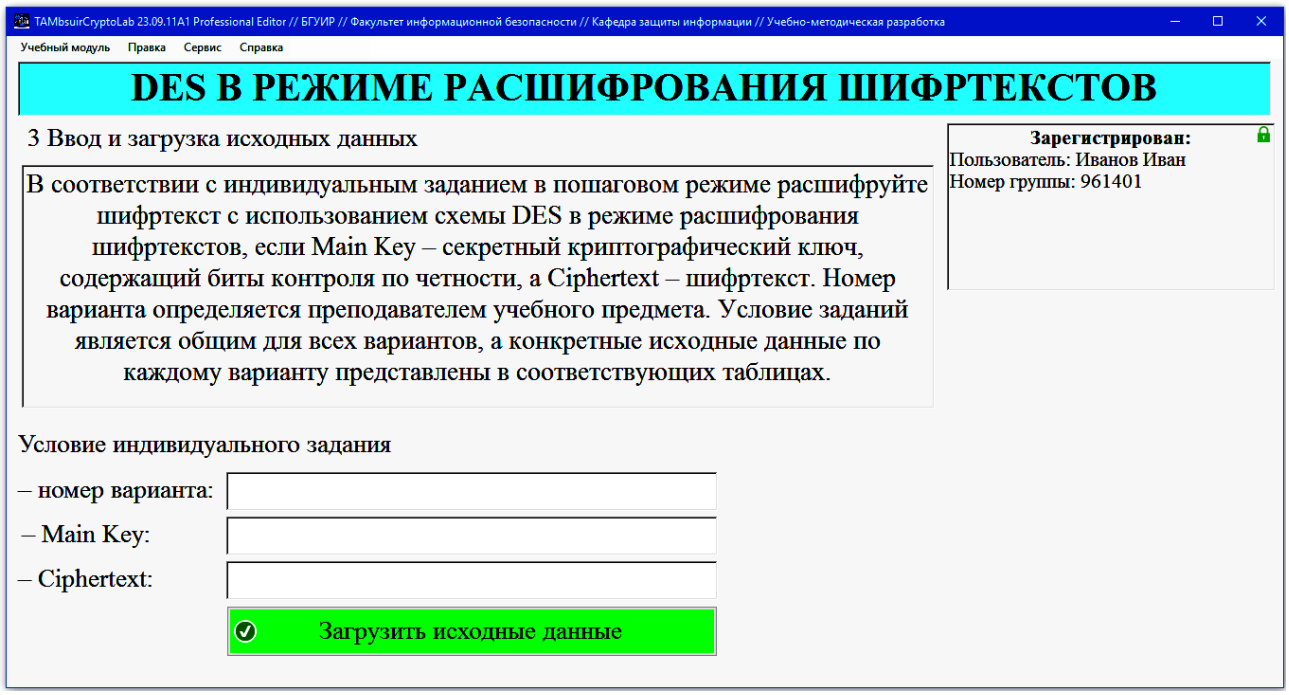


Рисунок 36 – Внешний вид окна ввода и загрузки исходных данных, соответствующего этапу 3 общего плана задания по изучению схемы расшифрования шифртекстов DES

В результате на экране появится окно для изучения схемы расшифрования шифртекстов DES, соответствующего этапу 4 общего плана задания, показанное на рисунке 37.

5 Выполните предлагаемые задания по изучению схемы расшифрования шифртекстов DES.

Исходные данные к заданию приведены в приложении Е.

Номер варианта задания определяется преподавателем учебной дисциплины. Условие заданий является общим для всех вариантов, а конкретные исходные данные по каждому варианту представлены в соответствующих таблицах.

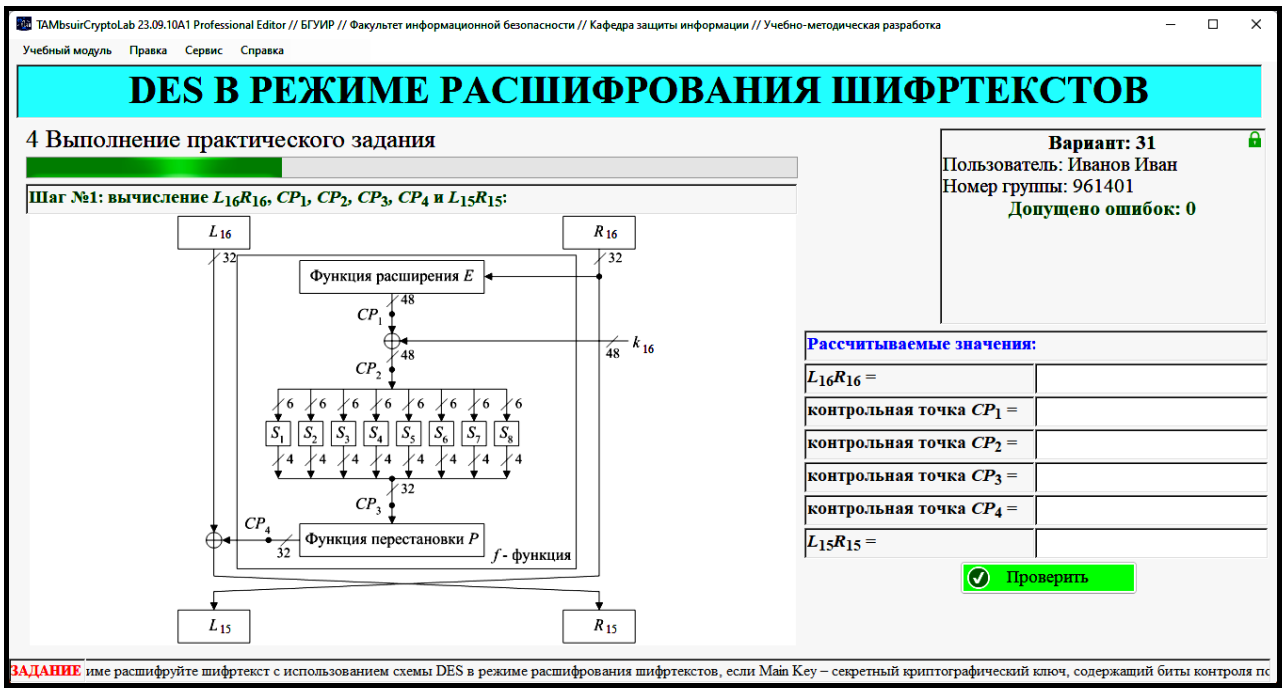


Рисунок 37 – Внешний вид окна для изучения
схемы расшифрования шифртекстов DES

Задание выполняется в окне, представленном на рисунке 37, и заключается в пошаговом расшифровании шифртекстов с использованием стандарта DES. Для удобства работы с программой текст задания дублируется в нижней части этого окна в виде «бегущей» строки.

Суть выполнения каждого шага задания заключается в расчете и заполнении L_iR_i, контрольных точек CP_1 – CP_4, а также открытого текста Plaintext (см. рисунки 32 и 37).

Чтобы проверить правильность выполнения каждого шага задания, необходимо нажать кнопку «Проверить».

Если одно или несколько значений рассчитаны неверно, на экран выводится сообщение об ошибке. В этом случае необходимо закрыть окно с сообщением об ошибке и повторно выполнить задание в окне изучения схемы расшифрования шифртекстов DES (см. рисунок 37).

Задание по изучению схемы расшифрования шифртекстов DES считается выполненным, если все шаги завершены успешно.

В приложении И приведен пример расчета L_iR_i и открытого текста Plaintext (см. таблицу И.4).

6 Выполните тестовое задание, соответствующее этапу 5 общего плана задания.

Окно с тестовыми заданиями отображается автоматически после завершения этапа 4 общего плана задания. Тест содержит 10 вопросов. Необходимо ответить на все вопросы. Правильных ответов может быть несколько.

Тестовые задания считаются выполненными, если все предлагаемые задания завершены успешно.

7 Продемонстрируйте результаты выполнения задания преподавателю учебной дисциплины.

Задание считается выполненным, если пункты 1 – 6 практического задания завершены успешно. При этом на экран выводится окно, показанное на рисунке 38, а.

Задание считается невыполненным, если на экран выводится окно, показанное на рисунке 38, б. В этом случае необходимо отменить загруженный учебный модуль, нажав комбинацию клавиш «Ctrl + J», в появившемся окне (см. рисунок Б.3) подтвердить отмену, выбрав «Да», и заново выполнить пункты 2 – 7 практического задания.

а

б

а – задание выполнено; б – задание не выполнено

Рисунок 38 – Заключительные результаты выполнения задания по изучению схемы расшифрования шифртекстов DES

4.3 Содержание отчета

1 Цель лабораторной работы.

2 Краткие теоретические сведения о работе схемы расшифрования шифртекстов DES.

3 Выводы по результатам выполнения практических заданий.

4 Ответы на контрольные вопросы.

4.4 Контрольные вопросы

1 Сколько раундов расшифрования шифртекстов выполняется схемой DES?

2 Какие данные подаются на вход *f*-Function в схеме DES в режиме расшифрования?

3 В каком порядке используются раундовые подключи при расшифрования шифртекстов DES?

4 Какие данные подаются на вход блока *IP* в схеме DES в режиме расшифрования шифртекстов?

5 Что выполняется блоком IP^{-1} в стандарте DES в режиме расшифрования шифртекстов?

ЛАБОРАТОРНАЯ РАБОТА 5
РЕЖИМЫ РАБОТЫ СИММЕТРИЧНЫХ КРИПТОСИСТЕМ БЛОЧНОГО ТИПА НА БАЗЕ DES

Цель: изучение основных режимов работы симметричных криптосистем, построенных на базе DES: режима электронной кодовой книги ECB, режима сцепления блоков шифра CBC, режима распространяющегося сцепления блоков шифра PCBC, режима обратной связи по шифртексту CFB, режима обратной связи по выходу OFB, режима счетчика CTR, а также режимов (схем) трехкратного применения DES (3DES) и режима (метода) отбеливания ключа DESX.

5.1 Краткие теоретические сведения

Структурная схема криптосистемы в режиме электронной кодовой книги ECB (Electronic Code Book, ECB), который также называют режимом прямого шифрования, показана на рисунке 39.

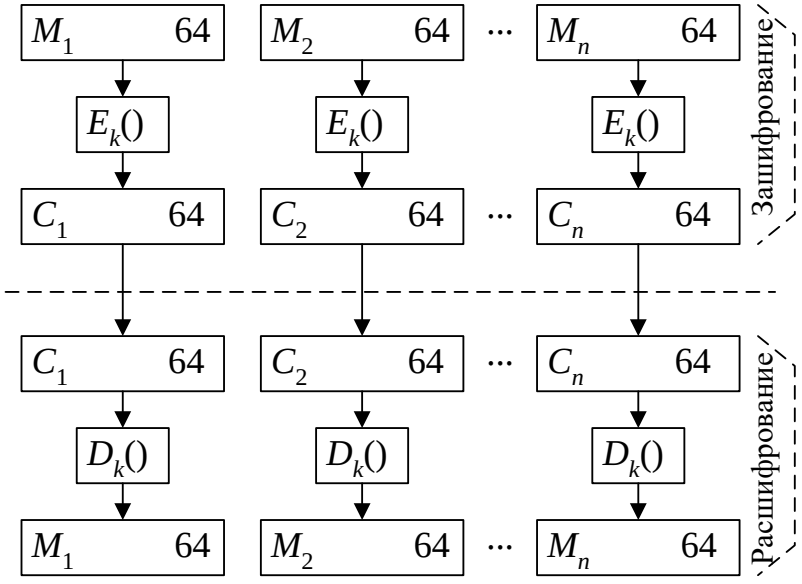


Рисунок 39 – Структурная схема криптосистемы в режиме ECB

В дальнейшем будем полагать, что в качестве базового алгоритма криптографического преобразования данных использован DES.

В режиме ECB исходный файл M (открытый текст) разбивается на 64-битовые блоки: $M = \{M_1, M_2, \ldots, M_n\}$. Если общая длина данных, подлежащих зашифрованию, не кратна 64 битам, то M_n-й блок будет иметь размер меньше 64 бит, поэтому его дополняют двоичными символами «0» со стороны старших двоичных разрядов до полного размера блока. Например, если общая длина данных, подлежащих зашифрованию, равна 1000 бит, то 16-й блок дополняется двадцатью четырьмя двоичными символами «0» со стороны старших двоичных разрядов. Затем каждый блок $\{M_1, M_2, \ldots, M_n\}$ шифруется отдельно. Результат зашифрования M_i и получение шифртекста C_i может быть представлен выражением

$$C_i = E_k\left(M_i\right), \tag{4}$$

где E_k – базовый алгоритм зашифрования данных;

M_i – i-й блок открытого текста,

k – секретный ключ;

i – количество шифруемых блоков данных ($i = 1 - n$).

На рисунке 39 в качестве базового алгоритма зашифрования данных и расшифрования шифртекстов выбран DES, как отмечалось ранее, поэтому секретным ключом будет являться Main Key k. На основе этого ключа Main Key k (разрядностью 64 бита с учетом битов контроля по четности) по схеме генерации раундовых ключей DES, построенной на базе блоков циклического сдвига влево LS, формируют 16 раундовых ключей DES, каждый из которых имеет разрядность 48 бит (см. лабораторную работу 1). Далее с помощью полученных раундовых ключей осуществляют итерационный процесс зашифрования данных DES (см. лабораторную работу 3), применяя его

к каждому M_i-му блоку (независимо), как видно из рисунка 39. В результате формируют шифртекст $C = \{C_1, C_2, \ldots, C_n\}$, который затем передается получателю по незащищенному каналу связи.

Для расшифрования шифртекста C его разделяют на 64-битовые блоки: $C = \{C_1, C_2, \ldots, C_n\}$. Как видно из рисунка 39, после этого каждый блок $\{C_1, C_2, \ldots, C_n\}$ расшифровывается отдельно (независимо). Результат расшифрования шифртекста C_i и получение M_i может быть представлен выражением

$$M_i = D_k\left(C_i\right), \tag{5}$$

где D_k – базовый алгоритм расшифрования шифртекстов;

C_i – i-й блок шифртекста;

k – секретный ключ;

i – количество расшифровываемых блоков ($i = 1 - n$).

Процесс расшифрования шифртекстов выполняется в обратном порядке по отношению с процессу зашифрования данных с учетом логики работы схемы. Поскольку в качестве базового алгоритма зашифрования данных выбран DES, то для расшифрования шифртекстов необходимо также использовать DES. Однако с учетом логики работы схемы и особенностей DES при расшифровании шифртекстов важно учитывать следующее:

– секретный ключ Main Key k необходимо использовать тот же, что и при зашифровании данных;

– схема генерации раундовых ключей DES должна быть выполнена на базе блоков циклического сдвига вправо *RS* (см. лабораторную работу 2);

– итерационный процесс расшифрования шифртекстов DES реализуется с использованием схемы, показанной на рисунке 32 (см. лабораторную работу 4).

Важно отметить, что режим ECB, как другие режимы, которые будут описаны ниже, может быть выполнен не только на базе DES, но и с

использованием любых других алгоритмов (стандартов) блочного типа. Причем разрядность одного шифруемого блока может отличаться от 64 бит. В этом случае принципы функционирования схемы останутся теми же, за исключением следующего:

– при формировании данных, подлежащих зашифрованию, получают блоки, размер которых соответствует размеру одного блока данных выбранного алгоритма (стандарта) блочного типа;

– если общая длина данных, подлежащих зашифрованию, не кратна размеру одного блока данных выбранного алгоритма (стандарта) блочного типа, то M_n-й блок дополняют двоичными символами «0» со стороны старших двоичных разрядов до полного размера одного блока соответствующего алгоритма (стандарта) блочного типа.

Например, на схеме, показанной на рисунке 39, в качестве базового алгоритма зашифрования данных E_k вместо DES может быть выбран стандарт AES [10, 11]. В этом случае размер одного блока составит 128 бит.

Режим ECB характеризуется постоянной скоростью обработки блоков, возможностью распараллеливания вычислений и наиболее прост в реализации. Однако при этом имеется существенный недостаток – сохранение статистических особенностей открытого текста [1 – 5]. Обусловлено это тем, что одинаковым блокам шифртекста соответствуют одинаковые блоки открытого текста. В результате режим ECB оказывается относительно слабо устойчивым против квалифицированных криптоаналитиков.

От указанного недостатка свободен режим сцепления блоков шифра (Cipher Block Chaining, CBC). Реализация этого режима работы поясняется рисунком 40, на котором приведена структурная схема криптосистемы.

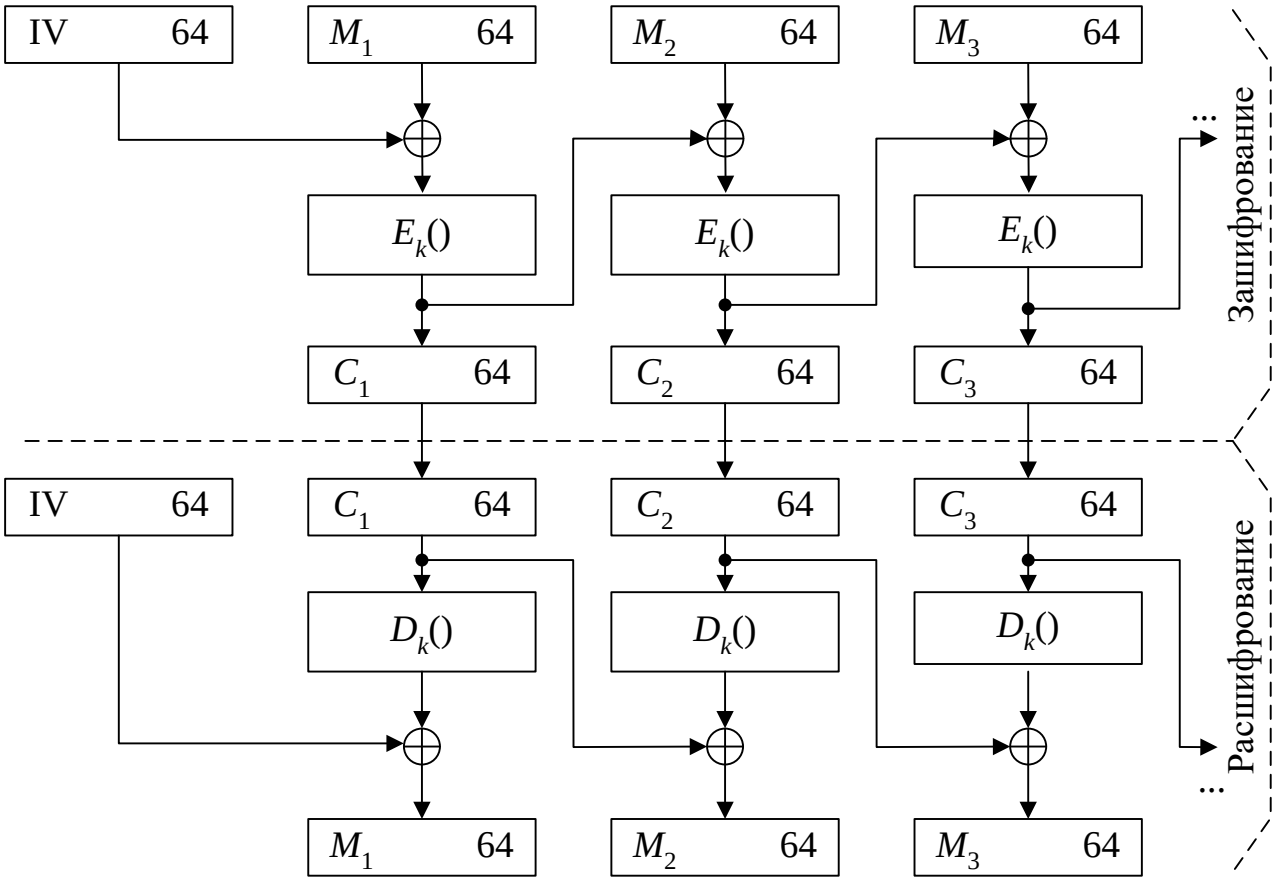


Рисунок 40 – Структурная схема криптосистемы в режиме CBC

Для зашифрования исходного файла M его вначале разделяют на 64-битовые блоки $M = \{M_1, M_2, \ldots, M_n\}$, как и в режиме ECB. Однако итерационный процесс зашифрования выполняется в соответствии с системой

$$\begin{cases} C_i = E_k\left(M_i \oplus IV\right), \ i = 1, \\ C_i = E_k\left(M_i \oplus C_{i-1}\right), \ i = 2 - n, \end{cases} \quad (6)$$

где E_k – базовый алгоритм зашифрования данных;

M_i – i-й блок открытого текста;

IV – начальный вектор (вектор инициализации);

C_{i-1} – (i–1)-й блок шифртекста;

k – секретный ключ;

i – количество шифруемых блоков данных (i = 1 – n).

Расширование шифртекстов осуществляется в соответствии с системой

$$\begin{cases} M_i = D_k\left(C_i\right) \oplus IV, \ i = 1, \\ M_i = D_k\left(C_i\right) \oplus C_{i-1}, \ i = 2 - n, \end{cases} \tag{7}$$

где D_k – базовый алгоритм расшифрования шифртекстов;

C_i – i-й блок шифртекста;

IV – начальный вектор (вектор инициализации);

C_{i-1} – (i–1)-й блок шифртекста;

k – секретный ключ;

i – количество шифруемых блоков данных (i = 1 – n).

К достоинствам режима CBC можно отнести постоянную скорость обработки блоков, отсутствие статистических особенностей, свойственных режиму ECB. Кроме того, режим CBC позволяет осуществлять распараллеливание расшифровки и может использоваться для формирования кода аутентификации сообщения (КАС) [5; 11]. КАСом является последний 64-битовый блок шифртекста C_n, который является функцией секретного ключа Main Key k, начального вектора IV и каждого бита открытого текста $M = \{M_1, M_2, \ldots, M_n\}$.

Режим CBC был усовершенствован, в результате чего появился режим распространяющегося сцепления блоков шифра PCBC (Propagating Cipher Block Chaining). На рисунке 41 приведена структурная схема криптосистемы в режиме PCBC.

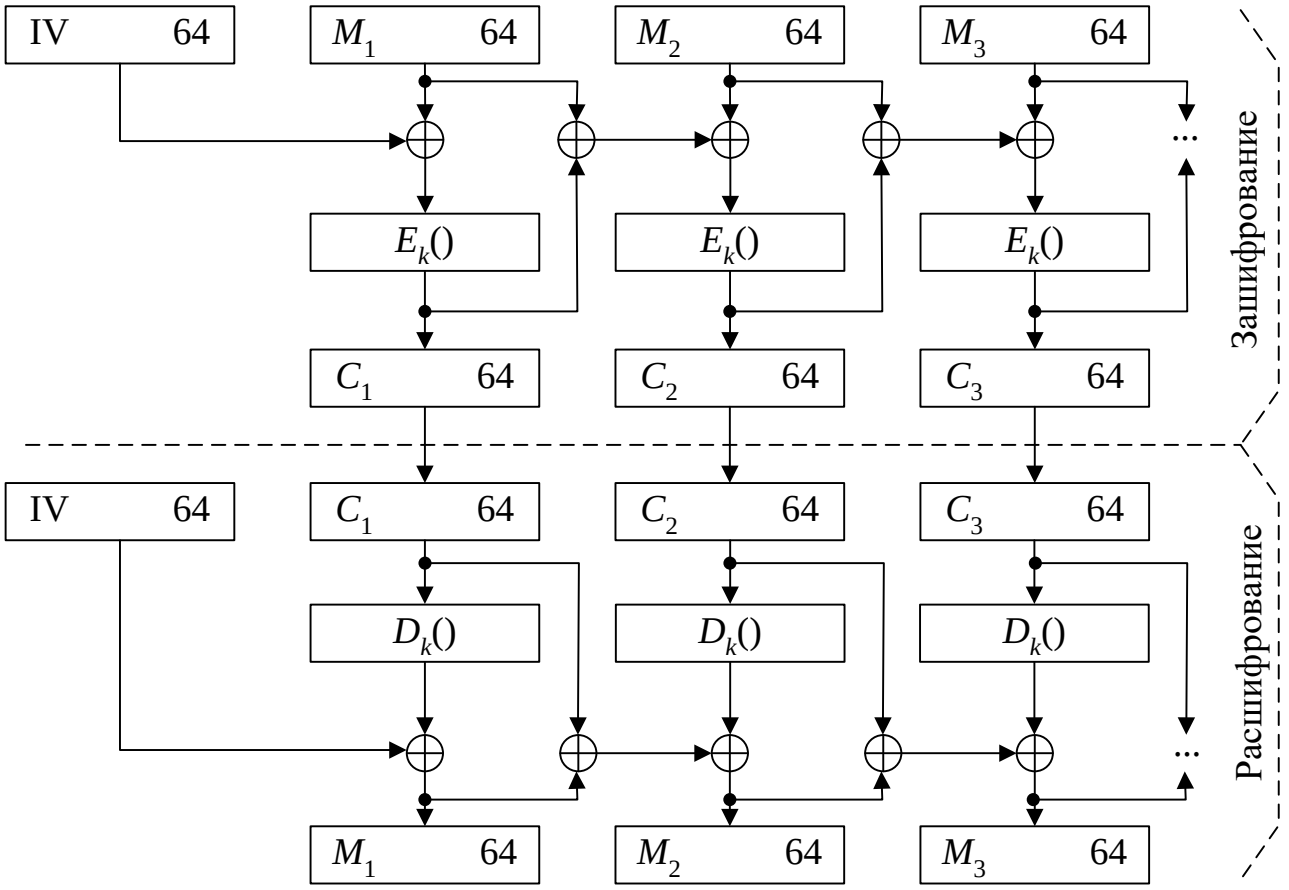


Рисунок 41 – Структурная схема криптосистемы в режиме PCBC

В данном режиме первый блок шифртекста формируется так же, как и в режиме CBC, а все остальные блоки шифртекста получают следующим образом. Вначале суммируют по модулю два предыдущий блок открытого текста и предыдущий блок шифртекста. Результат суммирования снова подвергается операции суммирования по модулю два с текущим шифруемым блоком открытого текста. После зашифрования полученного числа формируют текущий блок шифртекста (см. рисунок 41).

Таким образом, результат шифрования C_i и расшифрования M_i определяется системами соответственно:

$$\begin{cases} C_i = E_k\left(M_i \oplus IV\right), \ i = 1, \\ C_i = E_k\left(M_i \oplus M_{i-1} \oplus C_{i-1}\right), \ i = 2 - n, \end{cases} \tag{8}$$

$$\begin{cases} M_i = D_k\left(C_i\right) \oplus IV,\ i = 1, \\ M_i = D_k\left(C_i\right) \oplus C_{i-1} \oplus M_{i-1},\ i = 2 - n, \end{cases} \quad (9)$$

где E_k – базовый алгоритм зашифрования данных;

M_i – i-й блок открытого текста;

IV – начальный вектор (вектор инициализации);

M_{i-1} – (i–1)-й блок открытого текста;

C_{i-1} – (i–1)-й блок шифртекста;

D_k – базовый алгоритм расшифрования шифртекстов;

C_i – i-й блок шифртекста;

k – секретный ключ;

i – количество шифруемых блоков данных (i = 1 – n).

В режиме PCBC ошибка при приеме шифртекста приводит к неправильному расшифрированию всех последующих блоков. Следовательно, формирование КАС на передающей стороне криптосистемы и его проверка на принимающей стороне могут быть использованы для аутентификации отправителя данных и самих данных, как и в режиме CBC.

Режимы CBC и PCBC в настоящее время используют в сетевом протоколе аутентификации Kerberos, который включает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними и поддерживается ОС Windows 10 и 11, а также ОС UNIX и UNIX подобными ОС (Apple Mac OS X, Red Hat Enterprise Linux 4, FreeBSD, Solaris, AIX, OpenVMS) [12 – 14].

Для некоторых приложений существует необходимость зашифрования открытого текста произвольной длины с помощью стандартного блочного алгоритма таким образом, чтобы избыточность в полученном шифртексте была минимальной либо вовсе отсутствовала. Такая избыточность имеет место, когда общая длина данных, подлежащих зашифрованию, не кратна размеру одного блока (в случае DES – не кратна 64 битам). При этом M_n-й блок будет иметь

размер меньше 64 бит. В ранее рассмотренных режимах работы M_n-й блок необходимо дополнять двоичными символами «0» со стороны старших двоичных разрядов до полного размера блока, как отмечалось выше. Однако дополненные биты никакой значащей информации не несут, поэтому они вносят избыточность в полученном шифртексте и снижают эффективность использования пропускной способности канала связи.

Для устранения избыточности в полученном шифртексте может быть использован режим обратной связи по шифртексту CFB (Cipher Feed Back). Структурная схема криптосистемы, реализующей этот режим, показана на рисунке 42.

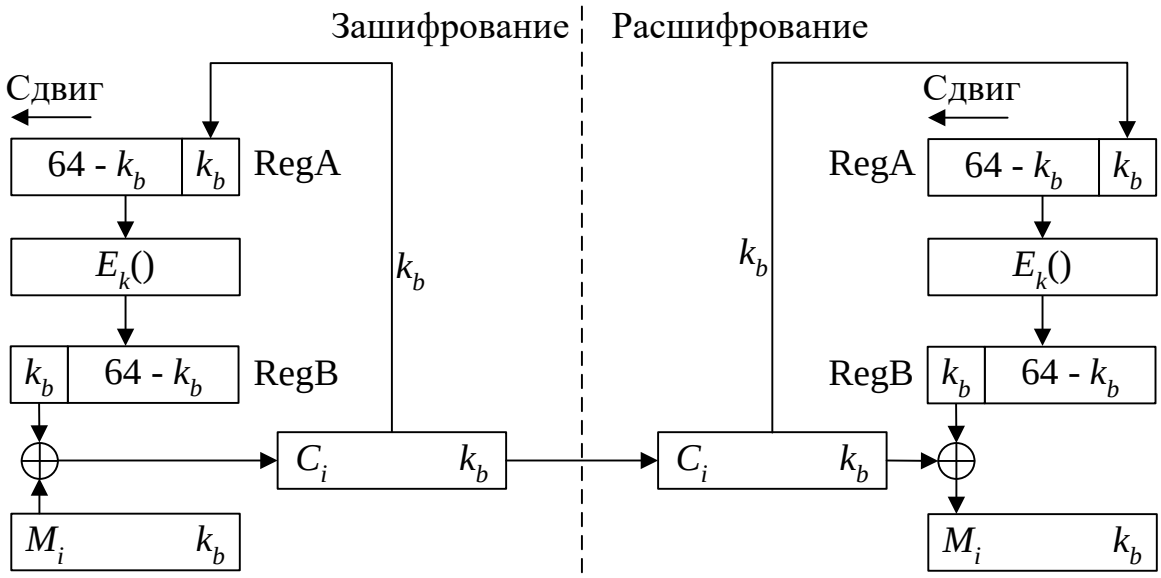


Рисунок 42 – Структурная схема криптосистемы в режиме CFB

В этом режиме размер блока может отличаться от 64 бит. Файл, подлежащий зашифрованию (расшифрованию), считывается последовательными блоками длиной k_b бит (для DES k_b = 1, 2, ..., 64). Входной блок (64-битовый входной регистр сдвига RegA) вначале содержит вектор инициализации *IV*, выровненный по правому краю. Предположим, что в результате разбиения на блоки получено *n* блоков длиной k_b бит каждый (при наличии остатка он дополняется двоичными символами «0» со стороны

старших двоичных разрядов до полного размера k_b; k_b целесообразно подбирать таким, чтобы остаток был равен нулю). Тогда для любого i = 1...n (n – число блоков) блок шифртекста равен

$$C_i = M_i \oplus P_{i-1}, \tag{10}$$

где M_i – i-й блок открытого текста,

$P_{i\text{-}1}$ – k_b старших битов предыдущего зашифрованного блока, взятых из 64-битового выходного регистра RegB.

Обновление входного сдвигового регистра RegA для всех последующих блоков осуществляется следующим образом. Содержимое RegA сдвигается влево на k_b бит. В высвободившиеся k_b бит младшие биты записывают C_i.

Восстановление зашифрованных данных выполняется аналогичным образом (см. рисунок 42):

$$M_i = C_i \oplus P_{i-1}, \tag{11}$$

где C_i – i-й блок шифртекста,

$P_{i\text{-}1}$ – k_b старших битов предыдущего зашифрованного блока, взятых из 64-битового выходного регистра RegB.

Важно отметить, что при расшифровании шифртекстов обновление сдвигового регистра RegA осуществляют так же, как и при зашифровании открытых данных.

Если обновление сдвигового регистра RegA выполнять путем сдвига влево на k_b бит и записи в его высвободившиеся младшие k_b биты старших k_b битов выходного 64-битового регистра RegB, то такой режим работы называют режимом обратной связи по выходу OFB (Output Feed Back). На рисунке 43 приведена структурная схема криптосистемы в режиме OFB.

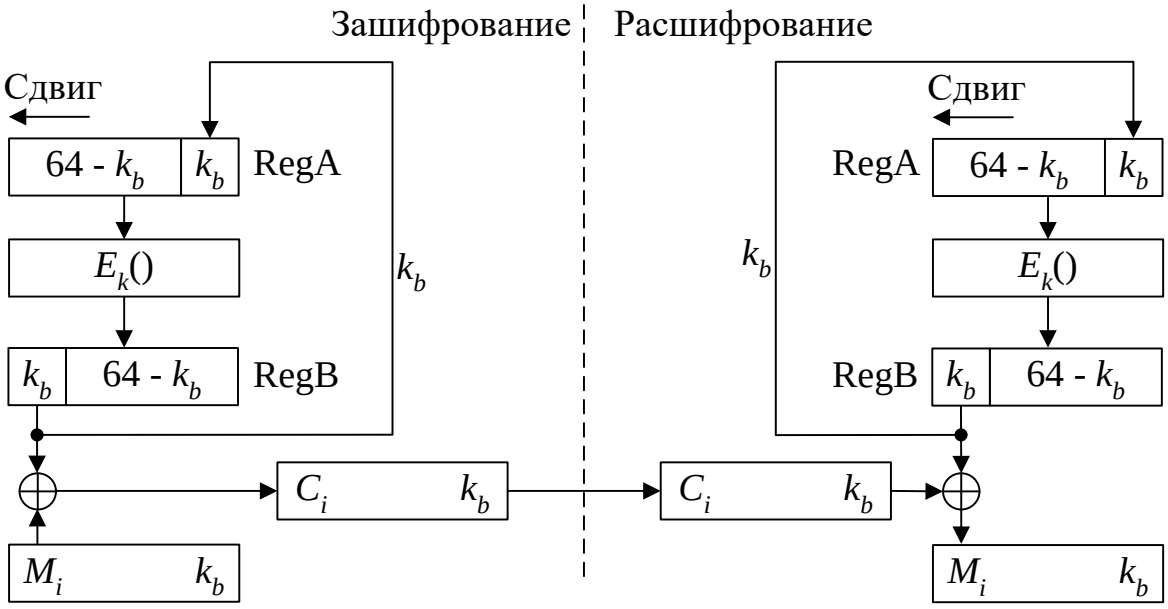


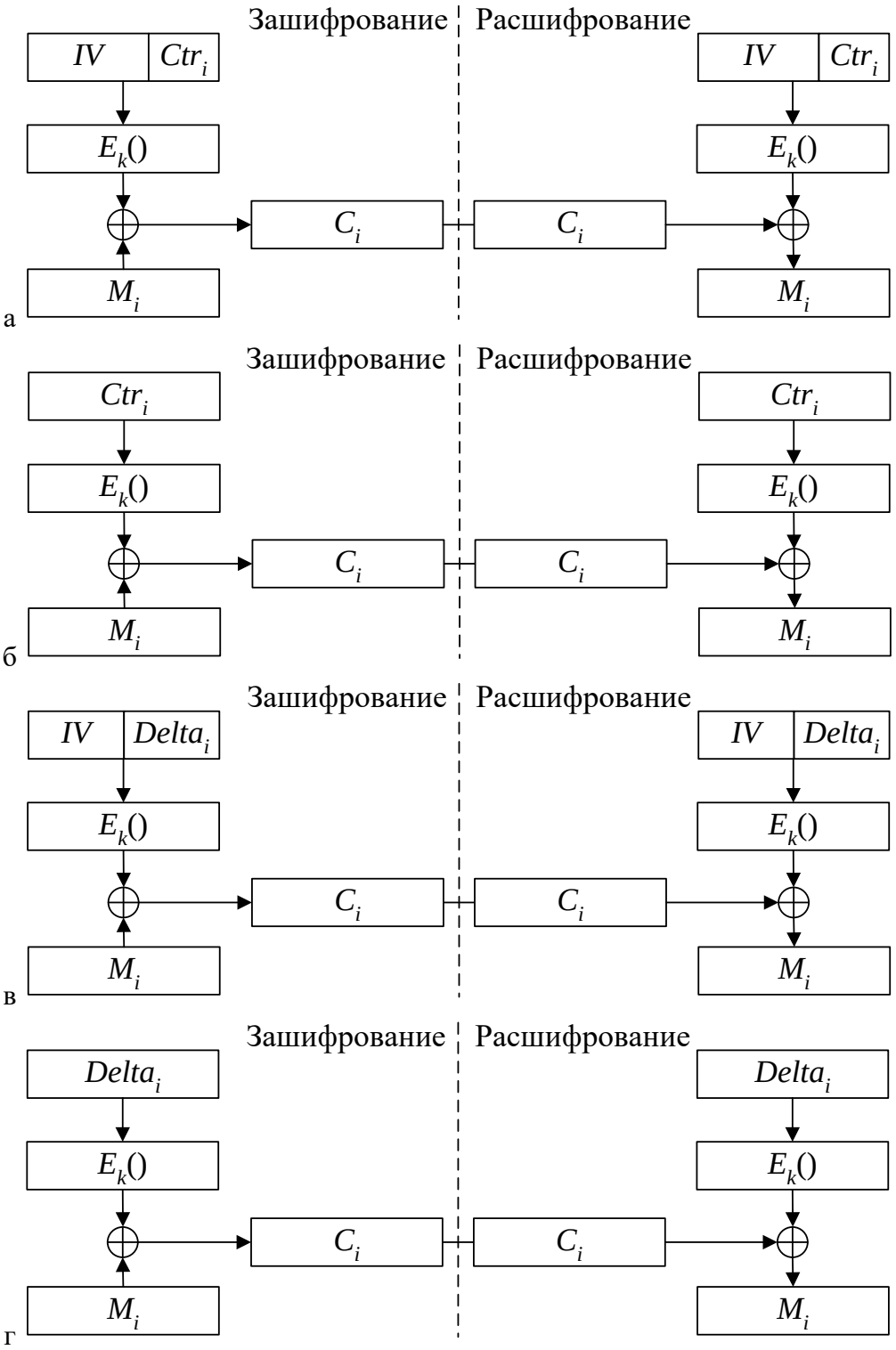
Рисунок 43 – Структурная схема криптосистемы в режиме OFB

Шифртекст C_i и открытый текст M_i определяются соответственно по формулам (10) и (11).

Существует возможность получения из блочного шифра потокового. Это может быть выполнено на базе режима счетчика CTR (Counter Mode). На рисунке 44 приведены структурные схемы криптосистем в режиме счетчика CTR различных версий.

В режиме счетчика CTR исходный файл M разбивается на 64-битовые блоки: $M = \{M_1, M_2, \ldots, M_n\}$. Также имеется начальный вектор IV, который записывают во входной регистр.

В версиях режима счетчика с разбиением входного регистра на две части (см. рисунок 44, а и в) начальный вектор IV содержит две части: левую (старшие биты) L разрядностью (64–b)-бит и правую R (младшие биты) разрядностью b-бит. Левая часть IV постоянна и не изменяется, а правая часть увеличивается либо на единицу (для версии Ctr_i, см. рисунок 44, а), либо на случайную величину (для версии Random Delta, см. рисунок 44, в) с приведением по модулю 2^b каждый раз при зашифровании очередного блока открытого текста.



а – версия *Ctr*$_i$ с разбиением входного регистра на две части;
б – версия *Ctr*$_i$ без разбиения входного регистра на две части;
в – версия Random Delta с разбиением входного регистра на две части;
г – версия Random Delta без разбиения входного регистра на две части

Рисунок 44 – Структурные схемы криптосистем в режиме счетчика CTR

В версиях режима счетчика без разбиения входного регистра на две части (см. рисунок 44, б и г) увеличение либо на единицу (для версии Ctr_i), либо на случайную величину (для версии Random Delta) с приведением по модулю 2^{64} осуществляют каждый раз при зашифровании очередного блока открытого текста. Причем такую операцию выполняют по отношению ко всему значению входного регистра.

Первый блок шифртекста C_1 в режиме счетчика CTR получают после зашифрования входного регистра и последующим сложением по модулю два полученного значения с первым блоком открытого текста M_1. Последующие блоки шифртекста C_2, …, C_n вычисляют аналогичным образом, обновляя значения входного регистра, увеличивая его значение либо на единицу (для версии Ctr_i), либо на случайную величину (для версии Random Delta) с приведением по модулю 2^b или 2^{64} соответственно для версии CTR с разбиением входного регистра на две части и без разбиения входного регистра на две части.

При расшифровании шифртекстов выполняют такие же операции, как и при зашифровании открытых текстов, за исключением того, что при расшифровании шифртекстов суммирование по модулю два зашифрованного значения входного регистра выполняют с 64-битовыми блоками шифртекстов $C = \{C_1, C_2, \ldots, C_n\}$.

Таким образом, в режиме счетчика CTR для $i = 1...n$ (где n – число блоков) результаты зашифрования расшифрования определяются уравнениями:

– для режима счетчика Ctr_i с разбиением входного регистра на две части:

$$C_i = E_k\left(IV \mid Ctr_i\right) \oplus M_i, \tag{12}$$

$$M_i = E_k\left(IV \mid Ctr_i\right) \oplus C_i; \tag{13}$$

– для режима счетчика Ctr_i без разбиения входного регистра на две части:

$$C_i = E_k\left(Ctr_i\right) \oplus M_i, \tag{14}$$

$$M_i = E_k\left(Ctr_i\right) \oplus C_i; \tag{15}$$

– для режима счетчика Random Delta с разбиением входного регистра на две части:

$$C_i = E_k\left(IV \mid Delta_i\right) \oplus M_i, \tag{16}$$

$$M_i = E_k\left(IV \mid Delta_i\right) \oplus C_i; \tag{17}$$

– для режима счетчика Random Delta без разбиения входного регистра на две части:

$$C_i = E_k\left(Delta_i\right) \oplus M_i, \tag{18}$$

$$M_i = E_k\left(Delta_i\right) \oplus C_i, \tag{19}$$

где E_k – базовый алгоритм зашифрования данных;

IV – начальный вектор (вектор инициализации);

Ctr_i – значение счетчика для i-го блока;

M_i – i-й блок открытого текста;

C_i – i-й блок шифртекста;

| – функция конкатенации;

$Delta_i$ – значение приращения для i-го блока.

Для повышения криптостойкости DES были разработаны дополнительные режимы (схемы) – многократного применения DES и DESX [8–11].

Вначале рассмотрим режимы (схемы) многократного применения DES. Эти режимы (схемы) имеют несколько версий: 2DES, 3DES-EEE3, 3DES-EDE3, 3DES-EEE2 и 3DES-EDE2, которые так же, как и DESX, могут применяться в сочетаниях с другими режимами, рассмотренными ранее (ECB, CBC, PCBC, CFB, OFB и CTR).

Далее в качестве примера будут приведены реализации режимов (схем) многократного применения DES в сочетании с режимом ECB.

Структурная схема криптосистемы, реализующей режим 2DES, приведена на рисунке 45.

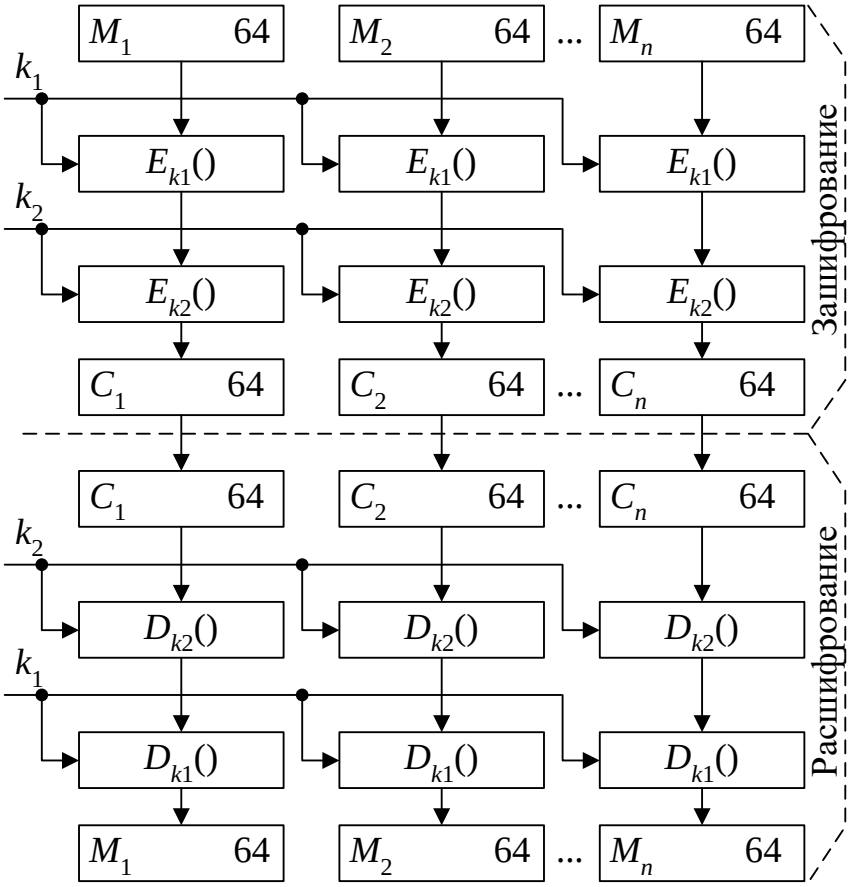


Схема выполнена в сочетании с режимом ECB

Рисунок 45 – Структурная схема криптосистемы в режиме 2DES

В режиме 2DES зашифрование DES выполняют вначале с использованием секретного ключа Main Key k_1, а затем полученный результат зашифровывают на секретном ключе Main Key k_2. Для расшифрования шифртекстов выполняют действия, обратные по отношению к зашифрованию с учетом логики работы схемы, т. е. шифртекст расшифровывают на секретном ключе Main Key k_2 и полученный результат расшифровывают на секретном ключе Main Key k_1.

Результаты зашифрования открытого текста M_i и расшифрования шифртекста C_i для $i = 1...n$ (где n – число блоков) могут быть описаны выражениями соответственно

$$C_i = E_{k_2}\left(E_{k_1}\left(M_i\right)\right), \tag{20}$$

$$M_i = D_{k_1}\left(D_{k_2}\left(C_i\right)\right), \tag{21}$$

где E_{k1}, E_{k2} и D_{k1}, D_{k2} – базовые алгоритмы зашифрования данных и расшифрования шифртекстов соответственно;

M_i – i-й блок открытого текста;

C_i – i-й блок шифртекста;

k_1 и k_2 – секретные ключи.

Если блочный алгоритм не является группой, то результирующий двукратно шифрованный блок текста окажется намного сложнее взломать методом полного перебора всех вариантов ключа. Например, для DES количество всех возможных секретных ключей Main Key k равно 2^{56}, а для 2DES – 2^{112}. Однако если блочный алгоритм обладает свойствами группы [2], то всегда найдется такой ключ k_3, что

$$C_i = E_{k_2}\left(E_{k_1}\left(M_i\right)\right) = E_{k_3}\left(M_i\right). \tag{22}$$

Это означает, что

$$M_i = D_{k_1}\left(D_{k_2}\left(C_i\right)\right) = D_{k_3}\left(C_i\right), \tag{23}$$

и является недостатком режима 2DES.

В этой связи целесообразно применять режимы (схемы) трехкратного использования алгоритма DES, структурные схемы которых иллюстрируются рисунками 46–49.

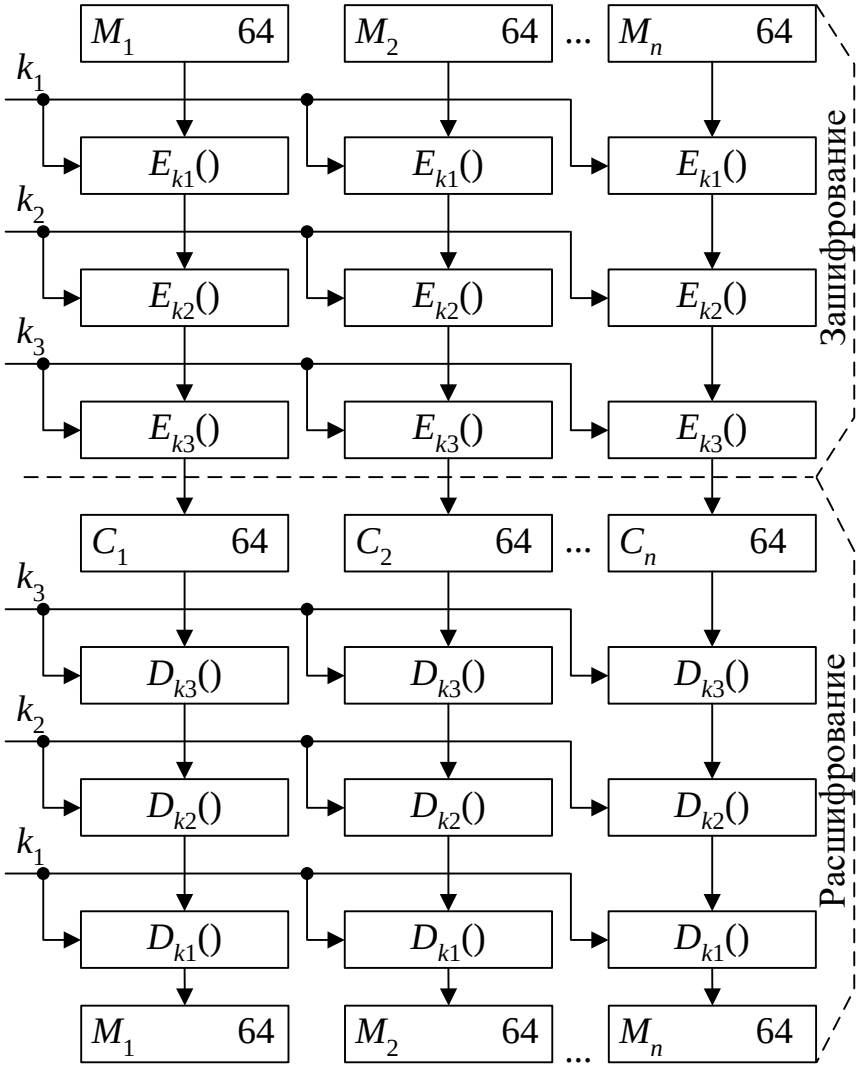


Схема выполнена в сочетании с режимом ECB

Рисунок 46 – Структурная схема криптосистемы в режиме 3DES-EEE3

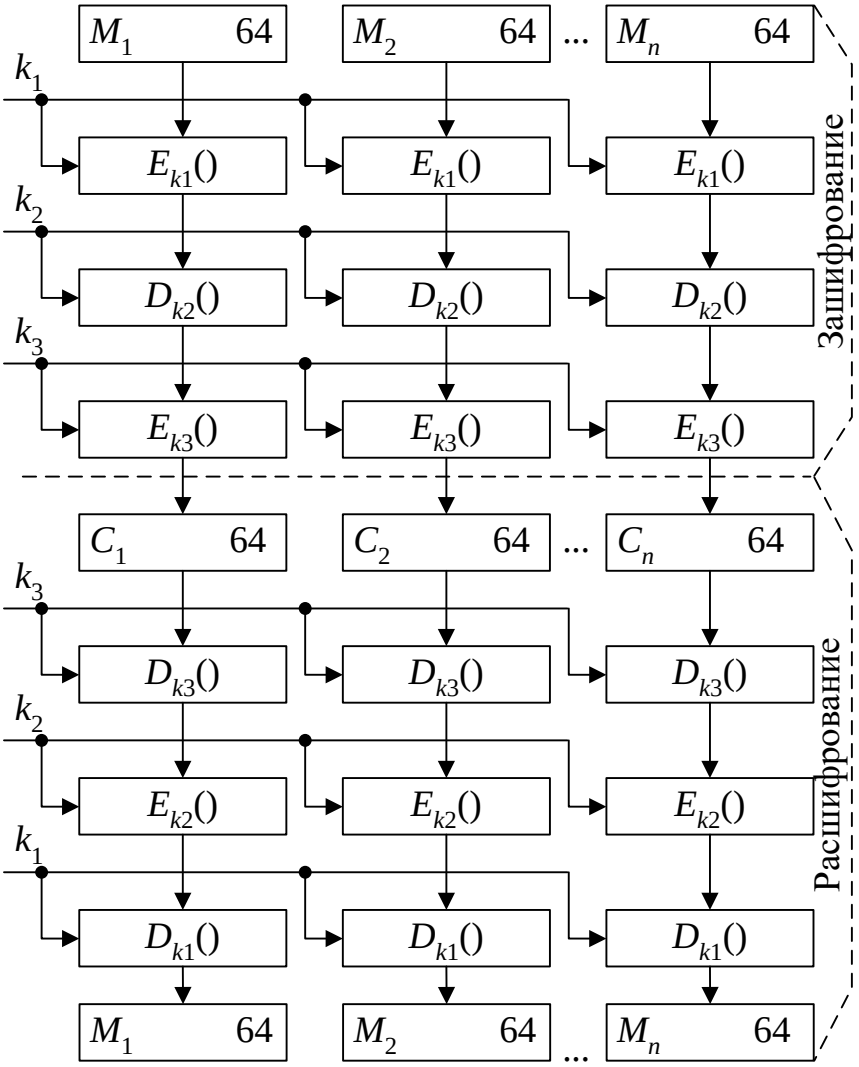


Схема выполнена в сочетании с режимом ECB

Рисунок 47 – Структурная схема криптосистемы в режиме 3DES-EDE3

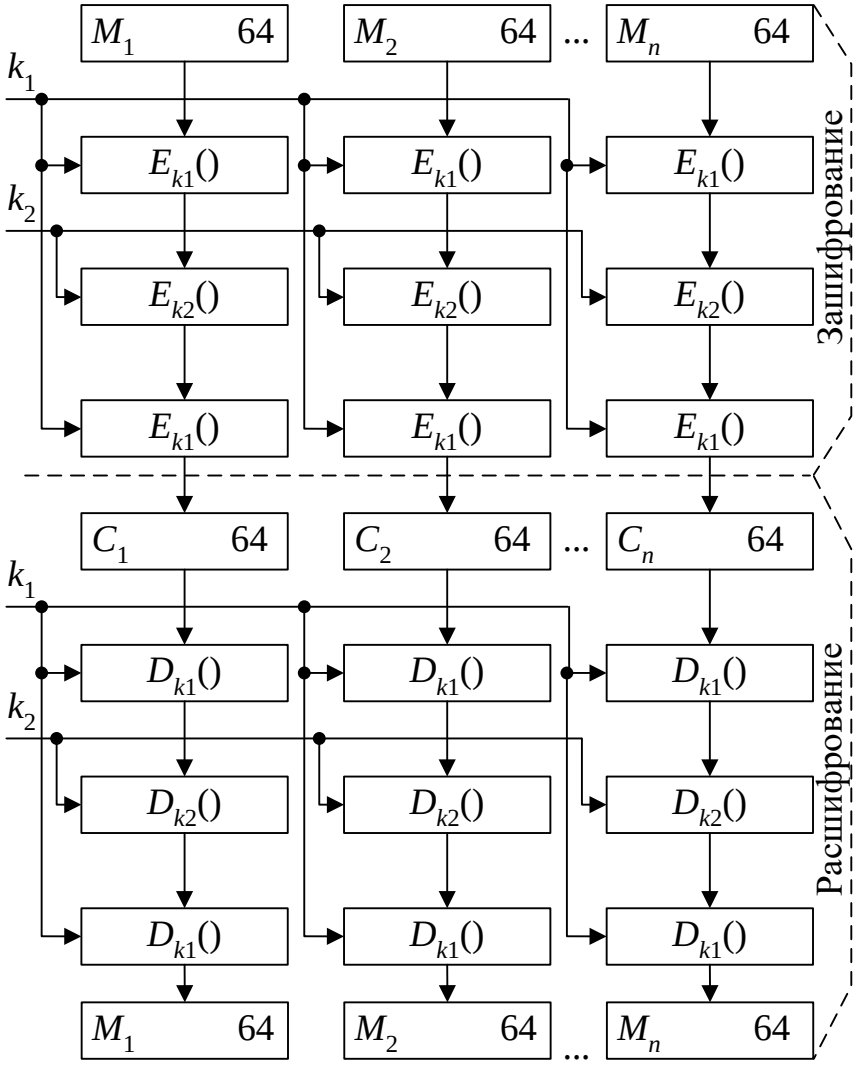


Схема выполнена в сочетании с режимом ECB

Рисунок 48 – Структурная схема криптосистемы в режиме 3DES-EEE2

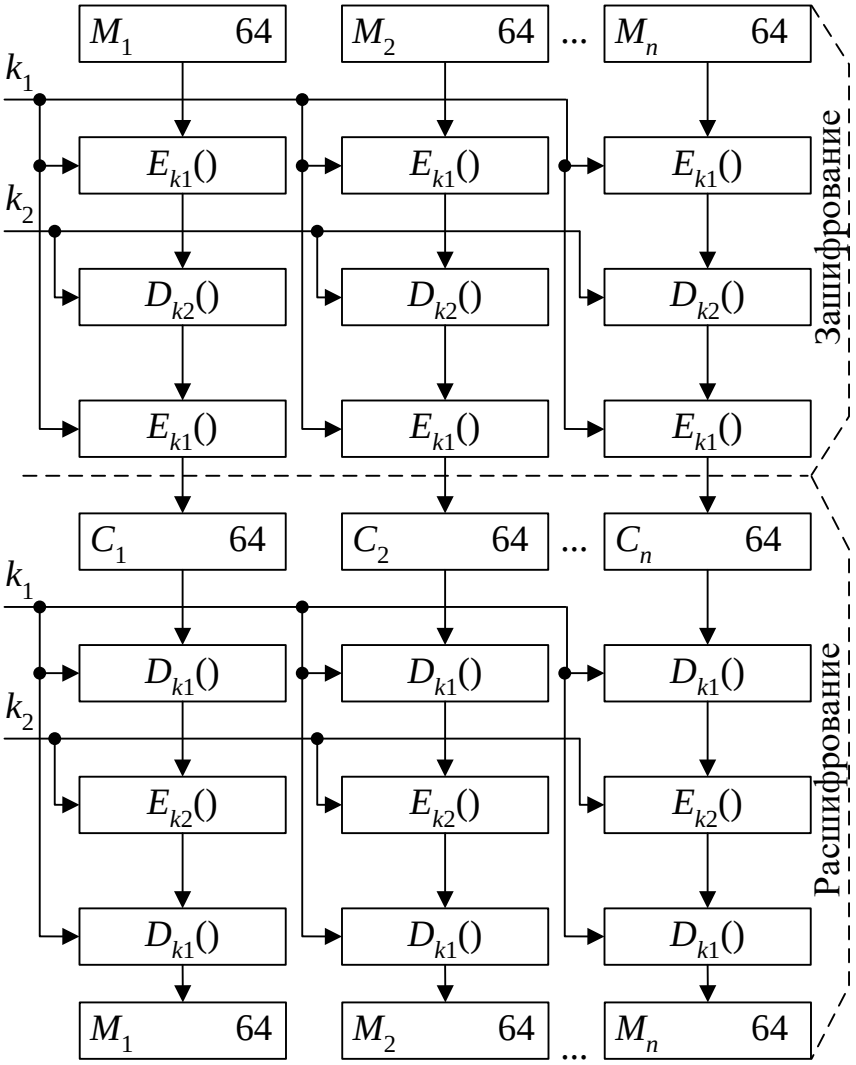


Схема выполнена в сочетании с режимом ECB

Рисунок 49 – Структурная схема криптосистемы в режиме 3DES-EDE2

Для схем, представленных на рисунках 46–49, результаты зашифрования и расшифрования при i = 1...n (где n – число блоков) определяются выражениями:

– для режима 3DES-EEE3 (схема на рисунке 46)

$$C_i = E_{k_3}\left(E_{k_2}\left(E_{k_1}\left(M_i\right)\right)\right), \tag{24}$$

$$M_i = D_{k_1}\left(D_{k_2}\left(D_{k_3}\left(C_i\right)\right)\right); \tag{25}$$

– для режима 3DES-EDE3 (схема на рисунке 47)

$$C_i = E_{k_3}\left(D_{k_2}\left(E_{k_1}\left(M_i\right)\right)\right), \tag{26}$$

$$M_i = D_{k_3}\left(E_{k_2}\left(D_{k_1}\left(C_i\right)\right)\right); \tag{27}$$

– для режима 3DES-EEE2 (схема на рисунке 48)

$$C_i = E_{k_1}\left(E_{k_2}\left(E_{k_1}\left(M_i\right)\right)\right), \tag{28}$$

$$M_i = D_{k_1}\left(D_{k_2}\left(D_{k_1}\left(C_i\right)\right)\right); \tag{29}$$

– для режима 3DES-EDE2 (схема на рисунке 49)

$$C_i = E_{k_1}\left(D_{k_2}\left(E_{k_1}\left(M_i\right)\right)\right), \tag{30}$$

$$M_i = D_{k_1}\left(E_{k_2}\left(D_{k_1}\left(C_i\right)\right)\right), \tag{31}$$

где E_{k1}, E_{k2}, E_{k3} и D_{k1}, D_{k2}, D_{k3} – базовые алгоритмы зашифрования данных и расшифрования шифртекстов соответственно;

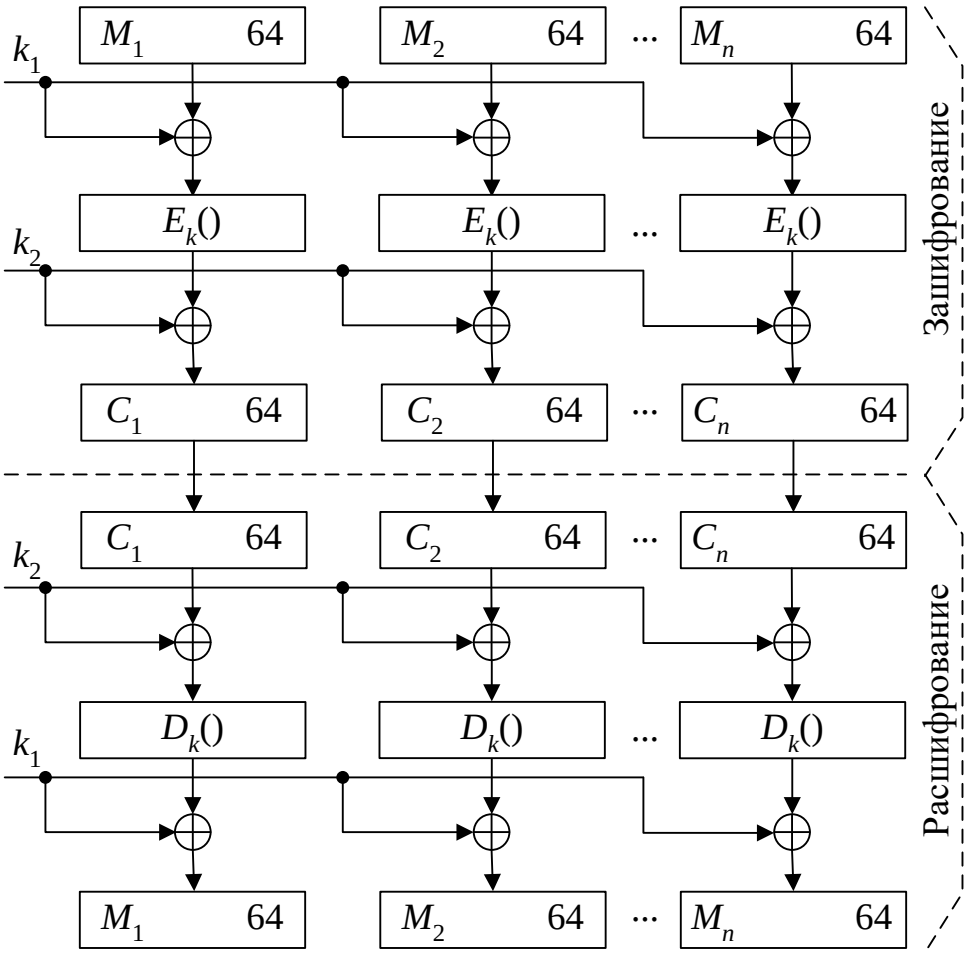
M_i – i-й блок открытого текста;

C_i – i-й блок шифртекста;

k_1, k_2 и k_3 – секретные ключи.

Среди всех версий режимов (схем) 3DES самой широко используемой является версия 3DES-EDE2 (см. рисунок 49), которая весьма эффективна при аппаратной реализации и применяется во многих финансовых приложениях (для эмиссии и обработки кредитных карт VISA, EuroPay и пр.), а также для защиты информации, содержащейся в биометрических паспортах [15].

Далее рассмотрим структурную схему криптосистемы в режиме DESX, которая показана на рисунке 50.



DESX выполнен в сочетании с режимом ECB

Рисунок 50 – Структурная схема криптосистемы в режиме DESX

Эта схема использует метод отбеливания ключа, который позволяет увеличить криптостойкость алгоритма к атакам на основе полного перебора всех возможных ключей.

Сущность режима DESX заключается в том, что перед выполнением однократного DES и после него на данные операцией суммирования по модулю два накладываются различные 64-битные ключи k_1 и k_2 (см. рисунок 50), в результате чего общая длина ключа увеличивается до $56 + 2 \times 64 = 184$ бит.

Для схемы, представленной на рисунке 50, результаты зашифрования и расшифрования для $i = 1...n$ (где n – число блоков) определяются выражениями:

$$C_i = E_k\left(M_i \oplus k_1\right) \oplus k_2, \tag{32}$$

$$M_i = D_k\left(C_i \oplus k_2\right) \oplus k_1, \tag{33}$$

где E_k и D_k – базовые алгоритмы зашифрования данных и расшифрования шифртекстов соответственно;

M_i – i-й блок открытого текста;

C_i – i-й блок шифртекста;

k_1 и k_2 – секретные ключи.

DESX полностью совместим с алгоритмом DES при $k_1 = k_2 = 0$. Существует несколько версий алгоритма DESX, основными из которых являются:

– DESX с переменным размером ключа шифрования, который получают с предварительным применением к нему хеширования по алгоритму SHA-1;

– DESX с длиной ключа шифрования 120 бит, когда в DESX выбирают $k_1 = k_2$;

– DESX, в которой вместо обеих операций XOR выполняется сложение по модулю 2^{64}.

Важно отметить, что режим DESX может применяться в сочетаниях с другими режимами, рассмотренными ранее (ECB, CBC, PCBC, CFB, OFB и CTR), а также в сочетании со схемами (режимами) двукратных и трехкратных DES. На рисунке 50 режим DESX выполнен в сочетании с режимом ECB.

Скорость алгоритма DESX приблизительно равна скорости DES. DESX характеризуется высокой криптостойкостью, имеет аппаратную и программную реализации и в настоящее время достаточно широко

используется. Реализация DESX включена в криптографические библиотеки BSAFE компании RSA Security с конца 80-х годов [16].

5.2 Практическое задание

1 Включите персональный компьютер и запустите файл «TAMbsuirCryptoLab.exe» на выполнение.

После запуска файла «TAMbsuirCryptoLab.exe» активизируется программное обеспечение, и появится окно выбора задания для выполнения (см. рисунок 1).

2 Выберите задание «Режимы работы DES» и ознакомьтесь с общим планом его выполнения.

Для выбора задания необходимо в окне, показанном на рисунке 1, последовательно указать следующее:

1) пункт «1 Глава:» – «СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ БЛОЧНОГО ТИПА»;

2) пункт «2 Раздел:» – «КРИПТОСИСТЕМА DES»;

3) пункт «3 Тема:» – «РЕЖИМЫ РАБОТЫ DES».

Затем нажмите кнопку «Перейти к заданию». В результате появится окно, содержащее общий план выполнения задания по изучению режимов работы симметричных криптосистем, построенных на базе DES, которое показано на рисунке 51.

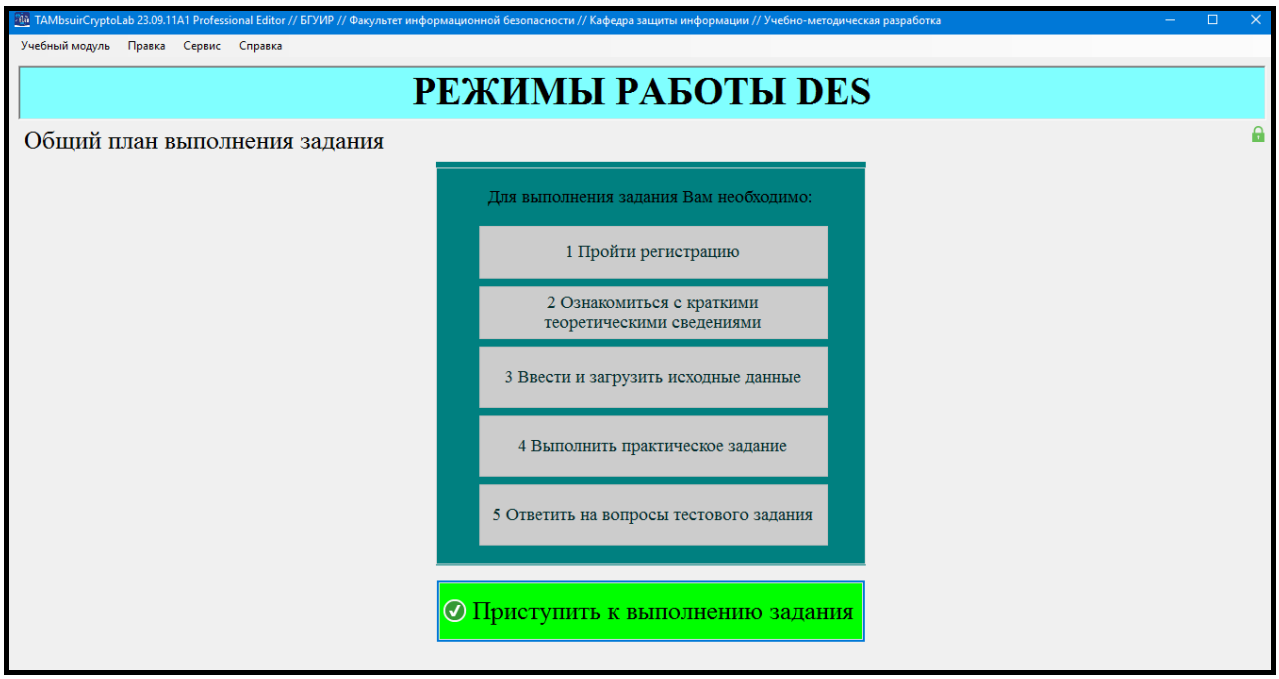


Рисунок 51 – Общий план выполнения задания по изучению режимов работы симметричных криптосистем, построенных на базе DES

3 Зарегистрируйтесь и ознакомьтесь с краткими теоретическими сведениями по функционированию схем, реализующих основные режимы работы симметричных криптосистем, построенных на базе DES.

Для того чтобы зарегистрироваться, необходимо в окне с общим планом выполнения задания (см. рисунок 51) нажать кнопку «Приступить к выполнению задания» и в появившемся окне регистрации, приведенном на рисунке 52, указать номер своей группы в поле «1 Номер группы:», ввести свою фамилию и имя в поле «2 Фамилия и имя:» и нажать кнопку «Зарегистрироваться».

После этого появится окно с краткими теоретическими сведениями, показанное на рисунке 53.

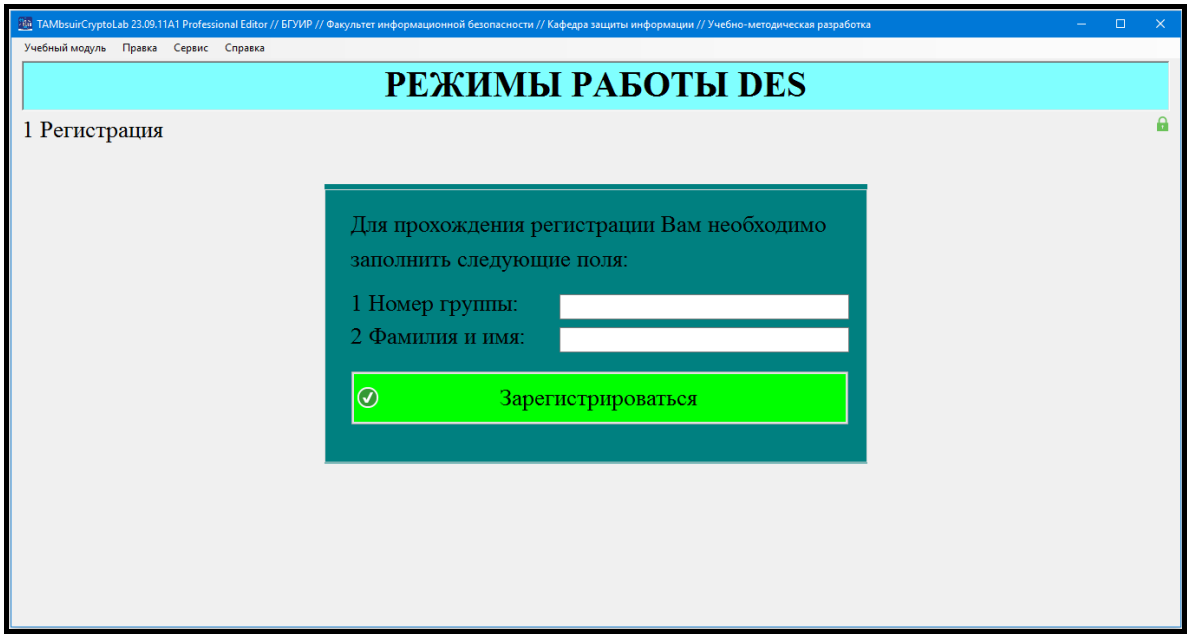


Рисунок 52 – Внешний вид окна регистрации, соответствующего этапу 1 общего плана задания по изучению режимов работы симметричных криптосистем, построенных на базе DES

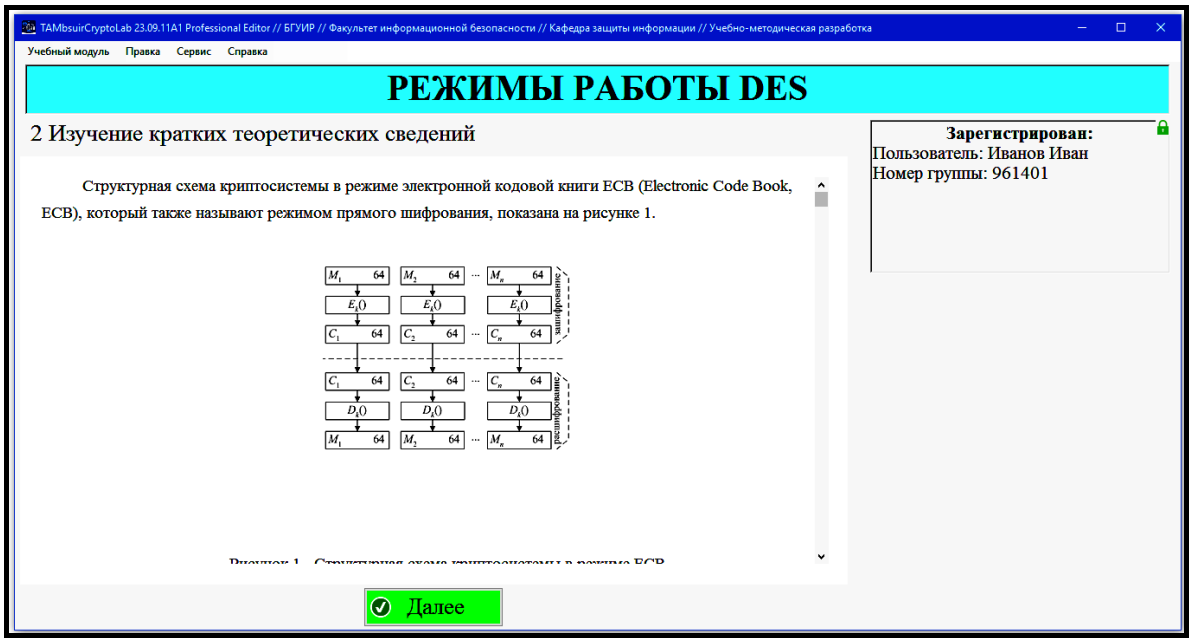


Рисунок 53 – Внешний вид окна с краткими теоретическими сведениями, соответствующего этапу 2 общего плана задания по изучению режимов работы симметричных криптосистем, построенных на базе DES

4 Загрузите исходные данные в соответствии с индивидуальным вариантом, который определяется преподавателем учебной дисциплины.

Для загрузки исходных данных необходимо в окне с краткими теоретическими сведениями (см. рисунок 53) нажать кнопку «Далее» и в появившемся окне ввода и загрузки исходных данных, приведенном на рисунке 54, ввести исходные данные и нажать кнопку «Загрузить исходные данные».

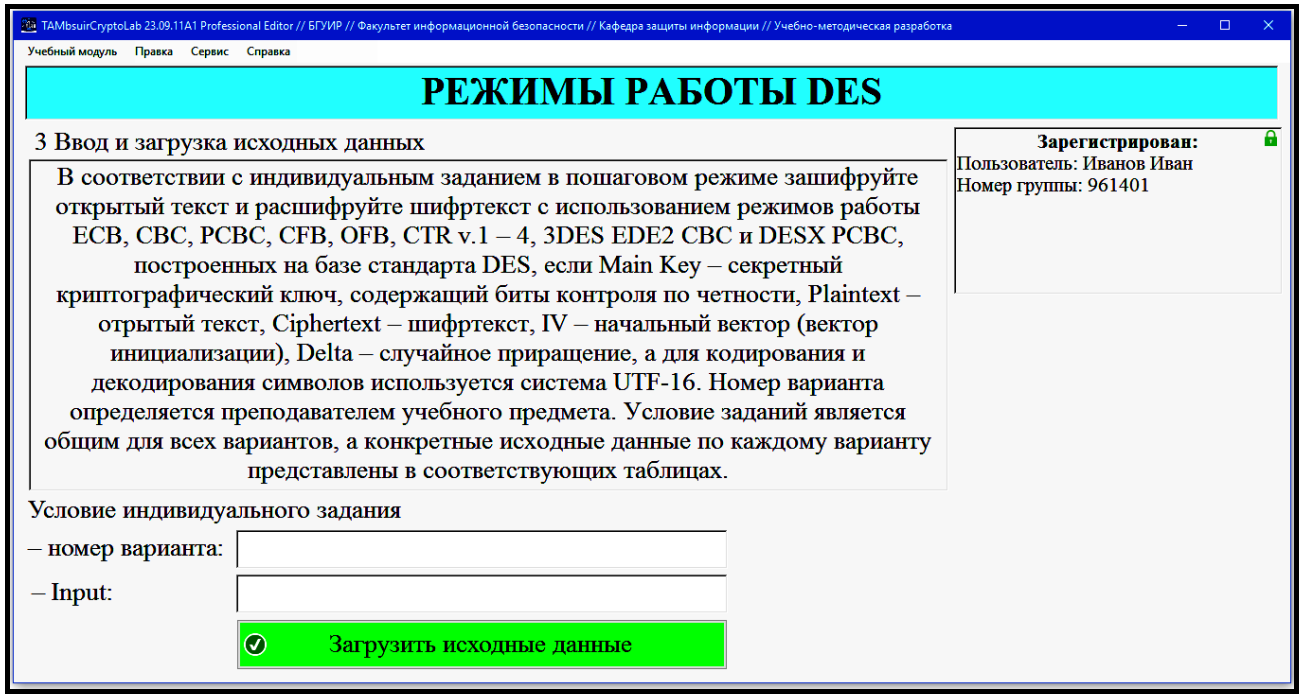
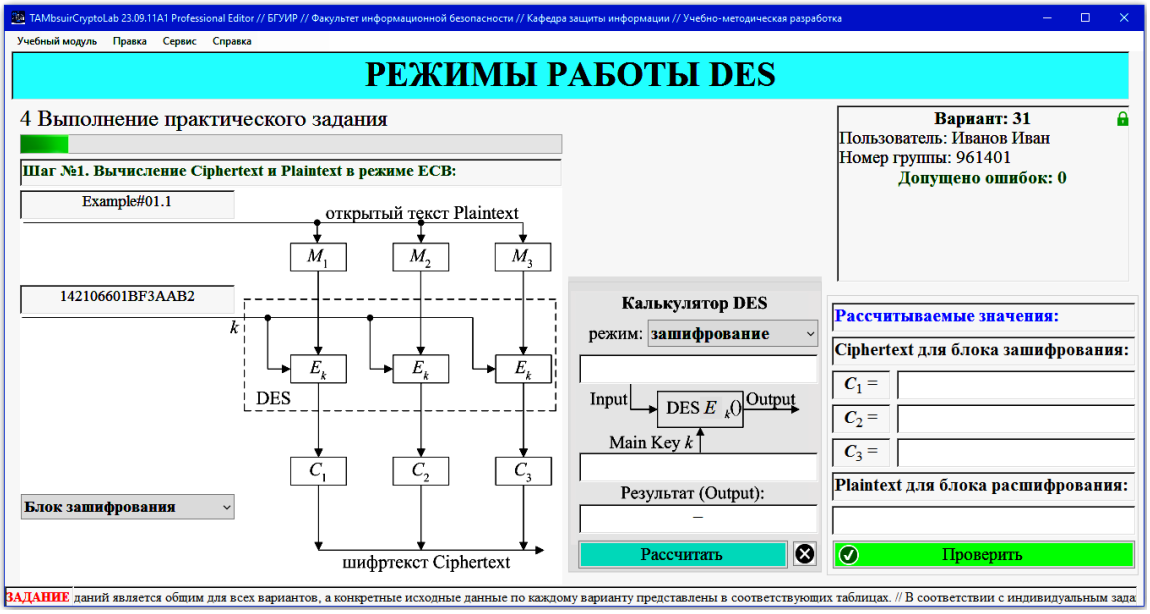
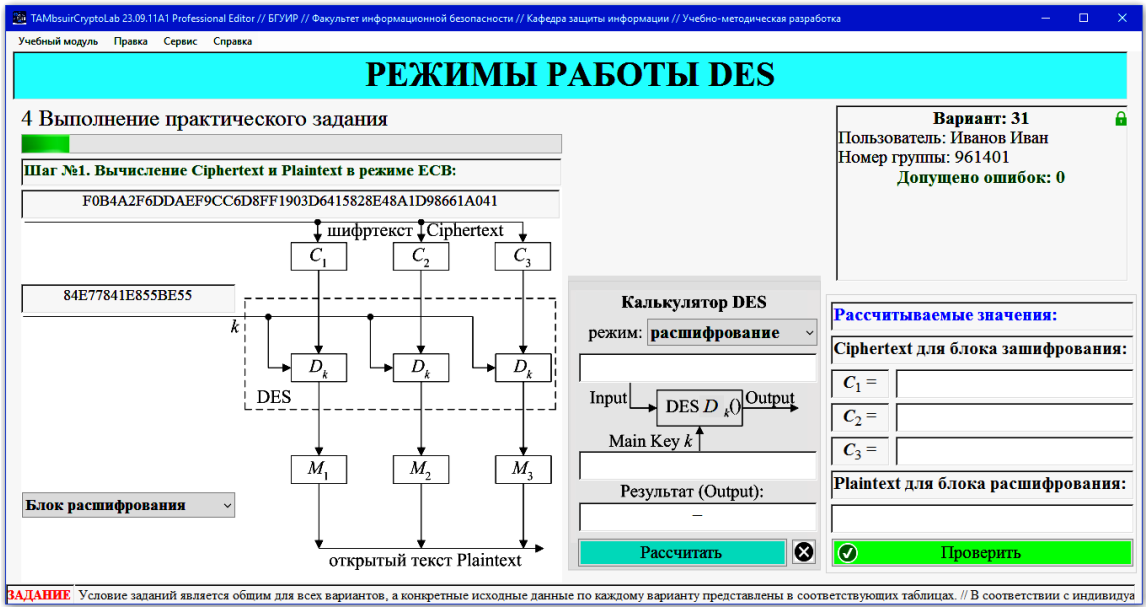


Рисунок 54 – Внешний вид окна ввода и загрузки исходных данных, соответствующего этапу 3 общего плана задания по изучению режимов работы симметричных криптосистем, построенных на базе DES

В результате на экране появится окно для изучения режимов работы симметричных криптосистем, построенных на базе DES, которое соответствует этапу 4 общего плана задания и показано на рисунке 55.



а



б

а – блок зашифрования данных; б – блок расшифрования шифртекстов

Рисунок 55 – Внешний вид окна для изучения режимов работы симметричных криптосистем, построенных на базе DES

5 Выполните предлагаемые задания по изучению режимов работы симметричных криптосистем, построенных на базе DES.

Исходные данные к заданию приведены в приложении Е.

Номер варианта задания определяется преподавателем учебной дисциплины. Условие заданий является общим для всех вариантов, а

конкретные исходные данные по каждому варианту представлены в соответствующих таблицах.

Задание выполняется в окне, представленном на рисунке 55, и заключается в пошаговом изучении основных режимов работы симметричных криптосистем, построенных на базе DES:

– режима электронной кодовой книги ECB;

– режима сцепления блоков шифра CBC;

– режима распространяющегося сцепления блоков шифра PCBC;

– режима обратной связи по шифртексту CFB;

– режима обратной связи по выходу OFB;

– режима счетчика CTR;

– режимов (схем) трехкратного применения DES (3DES);

– режима (метода) отбеливания ключа DESX.

Для удобства работы с программой текст задания дублируется в нижней части этого окна в виде «бегущей» строки.

Суть выполнения каждого шага задания заключается в расчете и заполнении шифртекстов C_1 – C_3 для блока зашифрования, а также открытого текста Plaintext для блока расшифрования (см. рисунок 55).

Чтобы проверить правильность выполнения каждого шага задания, необходимо нажать кнопку «Проверить».

Если одно или несколько значений рассчитаны неверно, на экран выводится сообщение об ошибке. В этом случае необходимо закрыть окно с сообщением об ошибке и повторно выполнить задание в окне изучения режимов работы симметричных криптосистем, построенных на базе DES (см. рисунок 55).

Задание по изучению режимов работы симметричных криптосистем, построенных на базе DES, считается выполненным, если все шаги завершены успешно.

В приложении И приведены примеры расчетов шифртекстов и открытых текстов для исследуемых режимов работы симметричных криптосистем, построенных на базе DES (см. таблицы И.5–И.9).

6 Выполните тестовое задание, соответствующее этапу 5 общего плана задания.

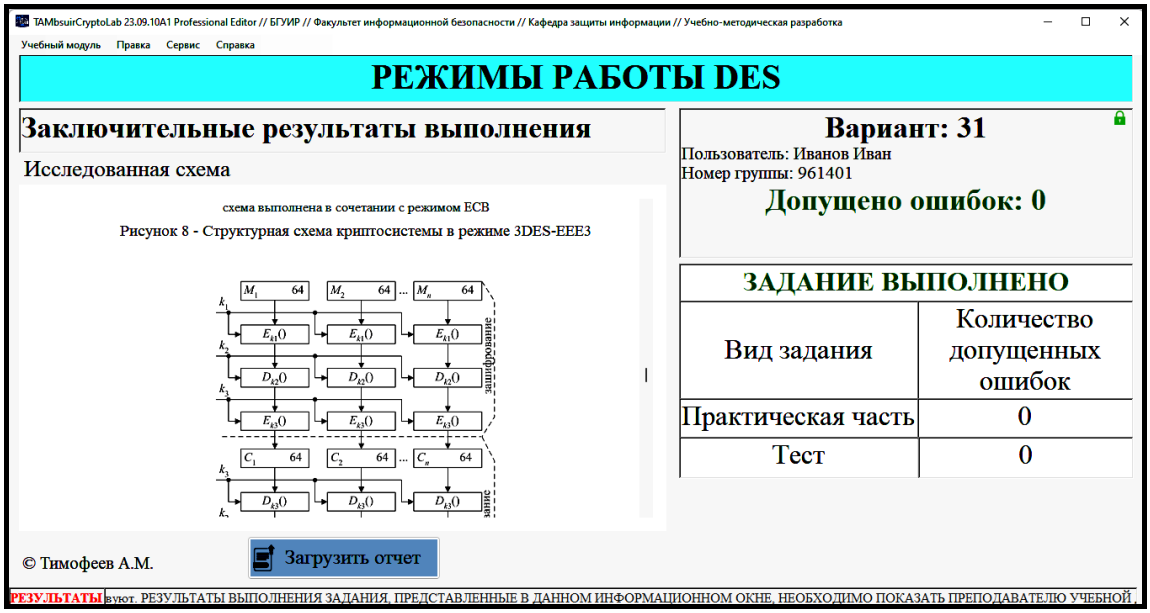
Окно с тестовыми заданиями отображается автоматически после завершения этапа 4 общего плана задания. Тест содержит 10 вопросов. Необходимо ответить на все вопросы. Правильных ответов может быть несколько.

Тестовые задания считаются выполненными, если все предлагаемые задания завершены успешно.

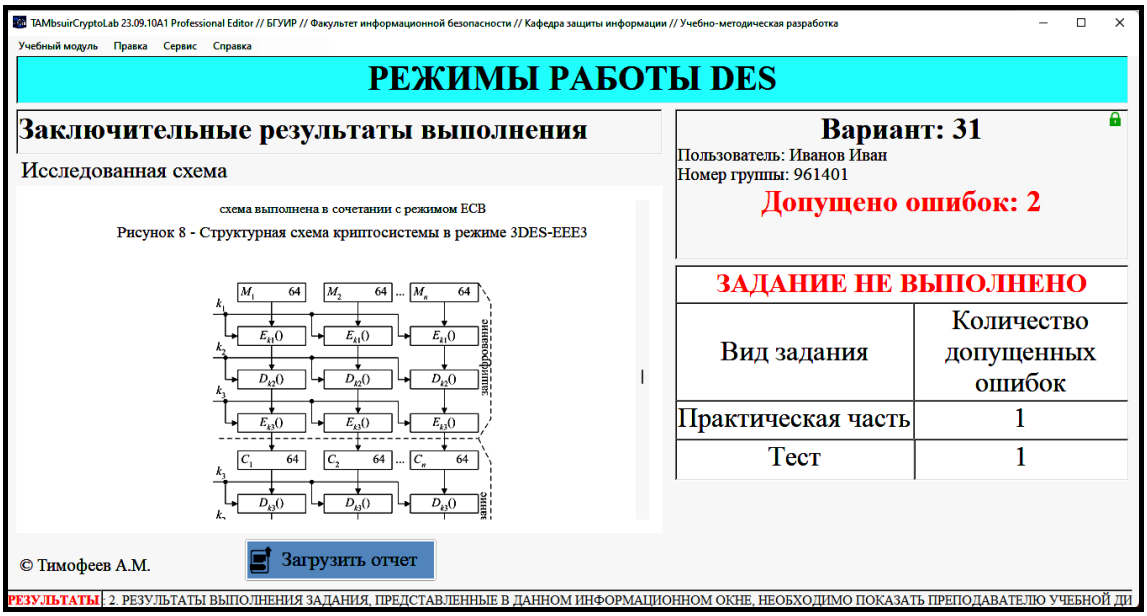
7 Продемонстрируйте результаты выполнения задания преподавателю учебной дисциплины.

Задание считается выполненным, если пункты 1 – 6 практического задания завершены успешно. При этом на экран выводится окно, показанное на рисунке 56, а.

Задание считается невыполненным, если на экран выводится окно, показанное на рисунке 38, б. В этом случае необходимо отменить загруженный учебный модуль, нажав комбинацию клавиш «Ctrl + J», в появившемся окне (см. рисунок Б.3) подтвердить отмену, выбрав «Да», и заново выполнить пункты 2 – 7 практического задания.



а



б

а – задание выполнено; б – задание не выполнено

Рисунок 56 – Заключительные результаты выполнения задания по изучению режимов работы симметричных криптосистем, построенных на базе DES

5.3 Содержание отчета

1 Цель лабораторной работы.

2 Краткие теоретические сведения об основных режимах работы DES.

3 Выводы по результатам выполнения практических заданий.

4 Ответы на контрольные вопросы.

5.4 Контрольные вопросы

1 Какое практическое применение находят режимы работы DES?

2 Каким образом режимы работы DES могут реализовываться с использованием других алгоритмов (стандартов) блочного типа?

3 Какой режим работы DES позволяет повысить криптостойкость на основе метода отбеливания ключа?

4 С какой целью могут использоваться на практике коды аутентификации сообщения (КАС), формируемые в режимах работы CBC и PCBC?

5 Какие режимы работы DES имеют наибольшую криптостойкость?

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Тимофеев, А. М. Криптографическая защита информации : учеб.-метод. пособие / А. М. Тимофеев. – Минск : БГУИР, 2020. – 118 с.

2 Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия / О. Р. Лапонина. – М. : НОУ «Интуит», 2016. – 244 с.

3 Радько, Н. М. Основы криптографической защиты информации : учеб. пособие / Н. М. Радько, А. Н. Мокроусов. – Воронеж : ФГБОУ ВПО ВГУ, 2014. – 109 с.

4 Милославская, Н. Г. Научные основы построения центров управления сетевой безопасностью в информационно-телекоммуникационных сетях / Н. Г. Милославская. – М. : Горячая линия-Телеком, 2021. – 432 с.

5 Бутакова, Н. Г. Криптографические методы и средства защиты информации: учеб. пособие / Н. Г. Бутакова, Н. В. Федоров. – СПб. : Интермедия, 2020. – 380 с.

6 Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 26 августа 2013 г. № 60 «Об утверждении Положения о порядке проведения государственной экспертизы средств технической и криптографической защиты информации» [Электронный ресурс]. – Режим доступа : https://pravo.by/document/?guid=12551&p0=T61302557&p1=1. – Дата доступа: 1.09.2023.

7 Информационные ресурсы. Стандарты в области защиты информации [Электронный ресурс]. – Режим доступа : https://rlst.org.by/informational-resources/virtualnye-vystavki/arhiv-tematicheskih-vystavok-normativno-tehnicheskih-dokumentov/standarty-v-oblasti-zashhity-informatsii/. – Дата доступа: 1.09.2023.

8 Data Encryption Standard (DES). Federal Information Processing Standards Publication 46-3 [Электронный ресурс]. – Режим доступа : https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf. – Дата доступа: 1.09.2023.

9 FOX Specifications [Электронный ресурс]. – Режим доступа : https://crypto.junod.info//fox_spec_v1.2.pdf. – Дата доступа: 1.09.2023.

10 Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197 [Электронный ресурс]. – Режим доступа : https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf. – Дата доступа: 1.09.2023.

11 Recommendation for Block Cipher Modes of Operation. Methods and Techniques. NIST Special Publication 800-38A [Электронный ресурс]. – Режим доступа : https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38a.pdf. – Дата доступа: 1.09.2023.

12 Kerberos 5 Release 1.20.1 [Электронный ресурс]. – Режим доступа : https://web.mit.edu/kerberos/krb5-1.20/. – Дата доступа: 1.09.2023.

13 Kerberos Authentication Overview. Описание компонента [Электронный ресурс]. – Режим доступа : https://learn.microsoft.com/ru-ru/windows-server/security/kerberos/kerberos-authentication-overview. – Дата доступа: 1.09.2023.

14 Kerberos V5 UNIX User's Guide. Kerberos V5 Tutorial [Электронный ресурс]. – Режим доступа : https://web.mit.edu/kerberos/krb5-1.9/krb5-1.9.1/doc/krb5-user.html. – Дата доступа: 1.09.2023.

15 Микроконтроллер MIK51AB72D для паспортно-визовых документов. Основные характеристики: [Электронный ресурс]. – Режим доступа : https://habr.com/ru/news/t/687486/. – Дата доступа: 1.09.2023.

16 RSA Security Inc. BSAFE: [Электронный ресурс]. – Режим доступа : http://support.aficio.com/bb_v1oi/pub_e/oi_view/0001035/0001035948/view/NETWORK/unv/0149.htm. – Дата доступа: 1.09.2023.

ПРИЛОЖЕНИЕ А

Дополнительные опции программы

Таблица А.1 – Доступ к дополнительным опциям программы

Опция программы	Выбор опции программы	
	нажатием сочетания клавиш	с помощью меню
Получение методических указаний по выполнению задания	Ctrl + M	Учебный модуль → Методические указания по выполнению
Ознакомление с краткими теоретическими сведениями	–	Справка → Краткая теория → 1 Описание
Доступ к изучаемым схемам	–	Справка → Краткая теория → 2 Схемы → «*выбрать требуемую схему из предлагаемого перечня*»
Ознакомление с формулами, используемыми для расчета контролируемых значений	–	Справка → Краткая теория → Расчетные формулы
Отмена загруженного учебного модуля	Ctrl + J	Учебный модуль → Отменить загруженный блок и выбрать …
Завершение выполнения учебного модуля	Alt + F4	Учебный модуль → Выход

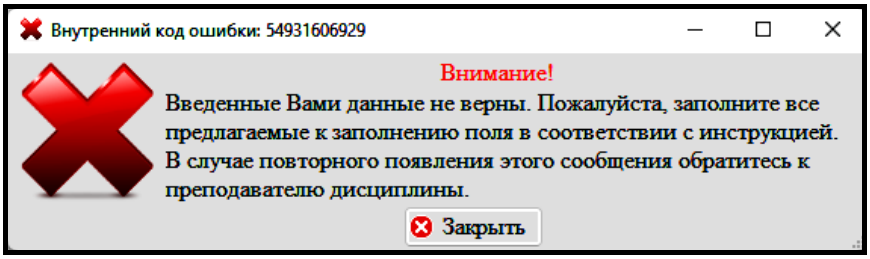
ПРИЛОЖЕНИЕ Б

Сведения о возможных сообщениях программы

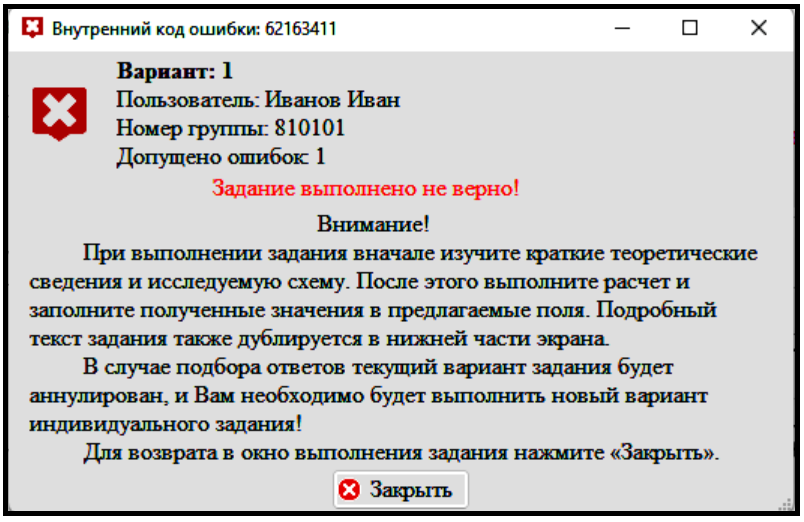
Таблица Б.1 – Сообщения об ошибках

Код ошибки	Возможная причина	Устранение
54XXXXXXXXX	Данные введены некорректно	Заполните предлагаемые поля в соответствии с инструкцией для текущего окна
6XXXXXXX	Расчет по практическому заданию выполнен неверно	Пересчитайте контролируемые значения для заданного шага практического задания в соответствии с инструкцией для текущего окна и нажмите «Проверить»
17XXXXXX	Выбранное действие либо не может быть выполнено, либо может привести к сбою в работе программного обеспечения	Обратитесь к преподавателю учебной дисциплины

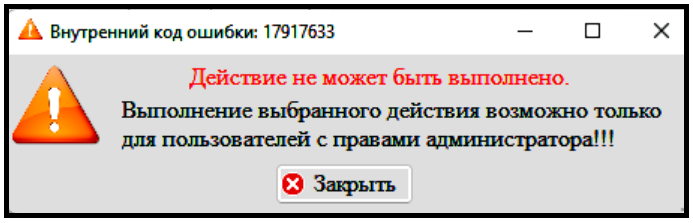
Примечание – Число X представлено в десятичной системе счисления и определяет тип ошибки и ее причину.



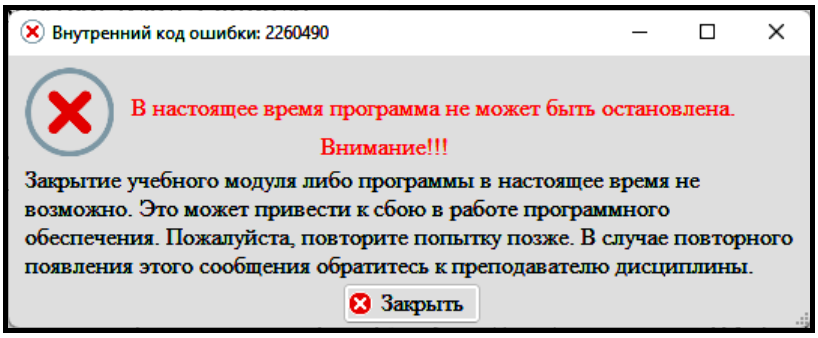
а



б



в



г

а – данные введены некорректно; б – расчет выполнен неверно; в – действие не может быть выполнено; г – действие может привести к сбою в работе программного обеспечения

Рисунок Б.1 – Примеры возможных сообщений об ошибках

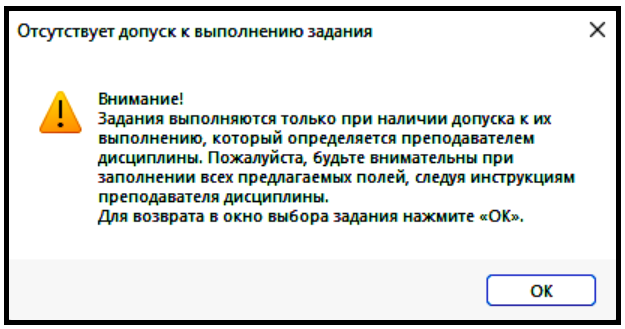


Рисунок Б.2 – Пример информационного сообщения

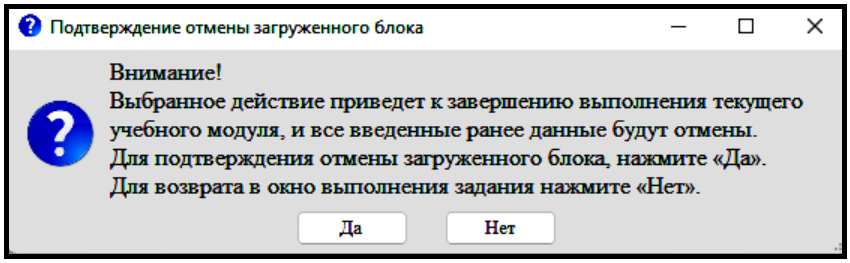


Рисунок Б.3 – Информационное сообщение
для подтверждения отмены загруженного блока

ПРИЛОЖЕНИЕ В

Исходные данные к лабораторной работе 1

Таблица В.1 – Исходные данные к лабораторной работе 1

Вариант	Секретный ключ Main Key
1	DDA55C0AF5F3BED2
2	356A4E66C6BDF5D8
3	5A5FE2D147360022
4	C6B14E2B12A6C024
5	47F0F32D17B70CD4
6	C548115FD4C08B63
7	AA06F0EB1DD195A5
8	A3BB63118EBE7DC9
9	397BED71C95396BD
10	60A099AFE2A39660
11	2BB4748DF6C97406
12	9F1E2B007224397D
13	1D530A6F59ACB22B
14	7E7EF5D4A311DBC5
15	3FCC50692EF6A66F
16	71DBF009B1AF71EB
17	D1DDCFF566F081C9
18	937803186ADD7E27
19	B7A58ED48147691E
20	7EA96C773596D250
21	710550AAAFE477CA
22	2817ED4D992477E7
23	2E6AB409786CF3D7
24	6C36146FF3DB785A
25	65AACCE46C3CF977
26	0059E7BD60DEDB60
27	4859B881E700775F
28	39EDE269A34D44D4
29	9077E89530EB81AA
30	FA17282B0CD4FCD2

Примечание – Значения указаны в шестнадцатеричной системе счисления.

ПРИЛОЖЕНИЕ Г

Исходные данные к лабораторной работе 2

Таблица Г.1 – Исходные данные к лабораторной работе 2

Вариант	Секретный ключ Main Key
1	4DFF4B35A36A8282
2	65F09C8B35FAE169
3	B118DD953FDBD118
4	479560EB87F66C1D
5	2E30B7446A4EB805
6	6C9324CC1777BE96
7	B8CF874E2B111DFC
8	FFA6ED479A5C4BED
9	E888A648567E427B
10	48B74769BBB12222
11	5C0CB460C6425342
12	56CFFA3CA942C960
13	D866E2F559EEBD0C
14	D1DEEE5CACC51860
15	817B0663BEE7CCC5
16	96BDD1D1B7357B6C
17	9FD4E7112D7EA927
18	055A5911E2186C09
19	90E178F98B0A7172
20	770F84CFACF5DD63
21	6FE75627E78BCC65
22	4481CF0956176C0A
23	FABEEEB4306C392D
24	2E306CFCD8061742
25	0CE7B17BC56387FA
26	9C6A550F2728B818
27	DEF018337D9C8199
28	212E359F229359C3
29	3F351BC5BD0A727D
30	D22B5FEE7795058B

Примечание – Значения указаны в шестнадцатеричной системе счисления.

ПРИЛОЖЕНИЕ Д

Исходные данные к лабораторной работе 3

Таблица Д.1 – Исходные данные к лабораторной работе 3

Вариант	Секретный ключ Main Key	Открытый текст Plaintext
1	DDA55C0AF5F3BED2	365B6E6F256B8247
2	356A4E66C6BDF5D8	CCF27CFBAB0FF035
3	5A5FE2D147360022	77112DCE01714AC3
4	C6B14E2B12A6C024	F4B45258FB637542
5	47F0F32D17B70CD4	7368554296FC2073
6	C548115FD4C08B63	6C5D799B7E86E9EA
7	AA06F0EB1DD195A5	68AAB9E7776AC571
8	A3BB63118EBE7DC9	B4EFF1F39A46FB85
9	397BED71C95396BD	1ABCD25783E3DD32
10	60A099AFE2A39660	7CE6CE9AE0D10E42
11	2BB4748DF6C97406	9B5FE30C1E2C99FA
12	9F1E2B007224397D	4E504450295E4290
13	1D530A6F59ACB22B	AEEA40DF3291FAA3
14	7E7EF5D4A311DBC5	CA17051BF7CFACE9
15	3FCC50692EF6A66F	0D81347CA9B328DD
16	71DBF009B1AF71EB	ED6B5AE92BA0F773
17	D1DDCFF566F081C9	AF97BA71ECA77E7B
18	937803186ADD7E27	94BB63E01F46CFAB
19	B7A58ED48147691E	13470DAC8418317A
20	7EA96C773596D250	1908483DDFEFF293
21	710550AAAFE477CA	367B3ABD695969F5
22	2817ED4D992477E7	BB09D645AF85DDC2
23	2E6AB409786CF3D7	25378B5F8821F3B1
24	6C36146FF3DB785A	1FC3C5F9AEED9610
25	65AACCE46C3CF977	905809BFC57147EE
26	0059E7BD60DEDB60	9570BC97AEE0CB55
27	4859B881E700775F	52992342B6A764C1
28	39EDE269A34D44D4	A63984CF0D16EC20
29	9077E89530EB81AA	F3EBAA54EC1905A5
30	FA17282B0CD4FCD2	4BF404E82C03FBB1

Примечание – Значения указаны в шестнадцатеричной системе счисления.

ПРИЛОЖЕНИЕ Е

Исходные данные к лабораторной работе 4

Таблица Е.1 – Исходные данные к лабораторной работе 4

Вариант	Секретный ключ Main Key	Шифртекст Ciphertext
1	4DFF4B35A36A8282	F3C116A2F89843C9
2	65F09C8B35FAE169	D6BE6DC8A4D74C2A
3	B118DD953FDBD118	28F9C102B627AD62
4	479560EB87F66C1D	31F0B4A44157C999
5	2E30B7446A4EB805	EE56D6AFC8B4DA1C
6	6C9324CC1777BE96	6B1782960F7198B2
7	B8CF874E2B111DFC	71E6395BDA8D3F74
8	FFA6ED479A5C4BED	60C33257296761BD
9	E888A648567E427B	766979598912953B
10	48B74769BBB12222	470F7E12BD120540
11	5C0CB460C6425342	F66DE84E9B182A92
12	56CFFA3CA942C960	536A93360BD68285
13	D866E2F559EEBD0C	6B9C8088BF47696B
14	D1DEEE5CACC51860	1405B4B883E39E9A
15	817B0663BEE7CCC5	C825066795FE1B3D
16	96BDD1D1B7357B6C	C715E4B52F3DE39F
17	9FD4E7112D7EA927	C9911F5D2804A2B0
18	055A5911E2186C09	5A677C9A3113B1BC
19	90E178F98B0A7172	7F997DB1DFD23140
20	770F84CFACF5DD63	5EA1627FC47FE8D4
21	6FE75627E78BCC65	C13EF3B3A0A4160E
22	4481CF0956176C0A	071D66CFD4AFF2A8
23	FABEEEB4306C392D	2E18C7538F6551DA
24	2E306CFCD8061742	FA2FC8E0BA616F69
25	0CE7B17BC56387FA	D26F7801FD0B1B38
26	9C6A550F2728B818	92667A0FBF44F849
27	DEF018337D9C8199	C44A4A46F4CFE555
28	212E359F229359C3	D602AB3EE2352EDA
29	3F351BC5BD0A727D	EFBD5238D03AFEEF
30	D22B5FEE7795058B	B93E0BAA231BFC02

Примечание – Значения указаны в шестнадцатеричной системе счисления.

ПРИЛОЖЕНИЕ Ж

Исходные данные к лабораторной работе 5

Таблица Ж.1 – Исходные данные к лабораторной работе 5. Часть 1

Вариант	Значение Input для окна ввода и загрузки исходных данных
1	80EE7EE0474A746BF987C314AB0BB86B
2	D78A07C656F123A6BEC1D9DFC645EE64
3	C7E0E5C42F2676B11DD127FCD07C3EB7
4	D123382C28EB508ECAD722857095A5B3
5	995F4DCA26F33BB01455A884C927D642
6	83220EA20CC13BDB9056FA5704F04187
7	2C7362712F7390DDE88718D242CBC4A2
8	01DF024D8602A7D724713ACFF9E3AB23
9	14215855C464120F9131BA84A96899C4
10	91575625EEF30029CC8A4DBE39C0E304
11	DCF4BE21736FDD9DCCF2BC5548222DBB
12	D8753EA28D863521202E883A1754D6D1
13	4DB5A8B5AA77502279B958FC37AAE0AA
14	5D91E5C382417755BF9C0045E6A38578
15	1BEB089379781160251B29D32E38EA75
16	4DDEDD856E134E0C3D53F60D770B3CD5
17	33E0E04CA24D30E480859E6717A32786
18	B28BF707C60009089CFB55268204E919
19	DF53A04E589DD2FFADF805E874E7F499
20	2B6F5AEB13340E32D6D7AFA6F80A627C
21	9C8488C303D82D14B8F75ACEFB2094B5
22	06BCFA12A9FD05AA456E7781EE2C07A3
23	95894CEF5F3196534145331CDA4037B6
24	43FAA03C0F50D29F7EDD7E9461AC268C
25	F0B73872D4A456D525A7D063C9E9CF05
26	36C03DF38BCB9345B6AC7081B201F195
27	1FA72C2307C5E29FA4CA16687F6FD595
28	0E795EA06F32002423F2BB2733D42224
29	B53B4422BDACFD71DD9E4FC1B42BC646
30	D6DB7339A35026ECA607FF1409BB6CCF

Примечание – Значения указаны в шестнадцатеричной системе счисления.

Таблица Ж.2 – Исходные данные к лабораторной работе 5. Часть 2.1

Вариант	Открытый текст Plaintext для блока зашифрования		
	в режиме ECB	в режиме CBC	в режиме PCBC
1	#26826705BYN	#43613286BYN	#93856937BYN
2	#69594840BYN	#21103837BYN	#95085966BYN
3	#19778030BYN	#17494877BYN	#19537200BYN
4	#55953469BYN	#19122751BYN	#38277344BYN
5	#25664317BYN	#30328430BYN	#48351451BYN
6	#49207401BYN	#66426776BYN	#49306116BYN
7	#97255135BYN	#51458428BYN	#99044408BYN
8	#84916941BYN	#43292420BYN	#57331301BYN
9	#39199279BYN	#17772123BYN	#45110782BYN
10	#25173419BYN	#41925158BYN	#13604981BYN
11	#48918683BYN	#50990928BYN	#70665573BYN
12	#23763159BYN	#27555921BYN	#97585198BYN
13	#55412867BYN	#51830364BYN	#22377442BYN
14	#34350611BYN	#92347474BYN	#81862691BYN
15	#40663109BYN	#42222703BYN	#67687929BYN
16	#42852563BYN	#56920447BYN	#47097180BYN
17	#79932819BYN	#41440899BYN	#57446503BYN
18	#20515041BYN	#20742867BYN	#11956148BYN
19	#73109973BYN	#53684700BYN	#69024485BYN
20	#16384144BYN	#10774516BYN	#15413906BYN
21	#54747462BYN	#72599165BYN	#98012140BYN
22	#35301860BYN	#33418517BYN	#56519596BYN
23	#70043698BYN	#19953172BYN	#87596474BYN
24	#91491720BYN	#89965059BYN	#84710463BYN
25	#88182197BYN	#97009724BYN	#99748744BYN
26	#36905469BYN	#76276614BYN	#93935036BYN
27	#82074910BYN	#62853303BYN	#78144745BYN
28	#85283838BYN	#21743944BYN	#43503421BYN
29	#91599797BYN	#89828256BYN	#28104301BYN
30	#44148003BYN	#52034884BYN	#75135504BYN

Примечание – Значения указаны в символьном виде.

Таблица Ж.3 – Исходные данные к лабораторной работе 5. Часть 2.2

Вариант	Открытый текст Plaintext для блока зашифрования		
	в режиме CFB	в режиме OFB	в режиме CTR v.1
1	#83598840BYN	#16217123BYN	#43409264BYN
2	#88482340BYN	#33090976BYN	#31933025BYN
3	#84761850BYN	#34519798BYN	#59705377BYN
4	#15371045BYN	#76712035BYN	#80718841BYN
5	#57582211BYN	#76057316BYN	#65790981BYN
6	#60320485BYN	#50085195BYN	#53610904BYN
7	#35509194BYN	#69041335BYN	#96095796BYN
8	#18325879BYN	#69917491BYN	#15777911BYN
9	#54014364BYN	#34703016BYN	#59981263BYN
10	#74030434BYN	#51575011BYN	#30078102BYN
11	#40450703BYN	#31777275BYN	#95104911BYN
12	#52885525BYN	#74456397BYN	#22768186BYN
13	#84344345BYN	#59496067BYN	#71605906BYN
14	#79308643BYN	#16905074BYN	#64642750BYN
15	#75965746BYN	#38771364BYN	#17346324BYN
16	#18073250BYN	#85204824BYN	#21395602BYN
17	#63217875BYN	#65851899BYN	#72206054BYN
18	#75392711BYN	#41481806BYN	#45241128BYN
19	#78298064BYN	#63777597BYN	#98924091BYN
20	#85616989BYN	#56311830BYN	#85922497BYN
21	#82140277BYN	#90418556BYN	#43676297BYN
22	#18404131BYN	#25363637BYN	#54936016BYN
23	#71203850BYN	#79186515BYN	#25824865BYN
24	#46763260BYN	#89121029BYN	#19059483BYN
25	#59515732BYN	#48071825BYN	#48631679BYN
26	#34538034BYN	#73411506BYN	#11676646BYN
27	#88461118BYN	#16985885BYN	#51322953BYN
28	#53921774BYN	#50637072BYN	#76771782BYN
29	#79169640BYN	#50224611BYN	#75651150BYN
30	#92778099BYN	#48851856BYN	#19276646BYN

Примечание – Значения указаны в символьном виде.

Таблица Ж.4 – Исходные данные к лабораторной работе 5. Часть 2.3

Вариант	Открытый текст Plaintext для блока зашифрования		
	в режиме CTR v.2	в режиме CTR v.3	в режиме CTR v.4
1	#70303083BYN	#22470916BYN	#97152010BYN
2	#95205258BYN	#74927685BYN	#23165487BYN
3	#55875320BYN	#51406847BYN	#38801904BYN
4	#38704239BYN	#28527971BYN	#16870577BYN
5	#61845969BYN	#48459403BYN	#22347900BYN
6	#79269069BYN	#25938734BYN	#69042259BYN
7	#36071613BYN	#23369892BYN	#16025282BYN
8	#95574068BYN	#96644021BYN	#92253684BYN
9	#25259453BYN	#72674061BYN	#86269240BYN
10	#97351613BYN	#96843542BYN	#28756443BYN
11	#43144318BYN	#56514350BYN	#65188276BYN
12	#88252982BYN	#16128581BYN	#12020073BYN
13	#47969647BYN	#64180565BYN	#10239744BYN
14	#29328806BYN	#45869014BYN	#15000004BYN
15	#35882205BYN	#33895610BYN	#58902479BYN
16	#10212193BYN	#44099295BYN	#75631852BYN
17	#57905105BYN	#82958879BYN	#81956699BYN
18	#80757683BYN	#65416561BYN	#71451126BYN
19	#86903120BYN	#24171085BYN	#66988412BYN
20	#27456204BYN	#78621103BYN	#47894629BYN
21	#52202775BYN	#61792578BYN	#99387477BYN
22	#59486089BYN	#60857428BYN	#71761331BYN
23	#44231465BYN	#91123322BYN	#89790830BYN
24	#23139426BYN	#52061965BYN	#40002884BYN
25	#89536746BYN	#49204895BYN	#27616275BYN
26	#60013515BYN	#33541664BYN	#18766665BYN
27	#86615666BYN	#95164773BYN	#41829291BYN
28	#41449964BYN	#85879967BYN	#94296443BYN
29	#50895103BYN	#68560561BYN	#39454376BYN
30	#65014198BYN	#82932714BYN	#86242898BYN

Примечание – Значения указаны в символьном виде.

Таблица Ж.5 – Исходные данные к лабораторной работе 5. Часть 2.4

Вариант	Открытый текст Plaintext для блока зашифрования	
	в режиме 3DES EDE2 CBC	в режиме DESX PCBC
1	#92476375BYN	#58902552BYN
2	#23355814BYN	#26181620BYN
3	#27852845BYN	#50757741BYN
4	#45685038BYN	#37639281BYN
5	#79339297BYN	#34562596BYN
6	#58510047BYN	#88935074BYN
7	#95844266BYN	#90326190BYN
8	#54486555BYN	#43335771BYN
9	#59991020BYN	#49294250BYN
10	#75285287BYN	#79312296BYN
11	#28195494BYN	#51298496BYN
12	#48673619BYN	#86780618BYN
13	#39959060BYN	#29137690BYN
14	#36114053BYN	#22106620BYN
15	#24647927BYN	#26828528BYN
16	#76024257BYN	#53796706BYN
17	#27527113BYN	#90256917BYN
18	#64620829BYN	#82785963BYN
19	#19696777BYN	#73118749BYN
20	#86095098BYN	#81746220BYN
21	#43339150BYN	#86552216BYN
22	#96258145BYN	#99723025BYN
23	#99917936BYN	#65963590BYN
24	#77901599BYN	#81406567BYN
25	#40807245BYN	#17246016BYN
26	#44516855BYN	#10490628BYN
27	#17179191BYN	#84998413BYN
28	#15379425BYN	#21184573BYN
29	#71291384BYN	#55615567BYN
30	#50638673BYN	#19617601BYN

Примечание – Значения указаны в символьном виде.

Таблица Ж.6 – Исходные данные к лабораторной работе 5. Часть 3.1

Вариант	Шифртекст Ciphertext для блока расшифрования в режиме ECB
1	CAC8DFD77190BDDD00C7337A286333841A5B1CAF1EED7181
2	5781E74C8AEFBBA33BBC6BA0F0F24DA626408B75A49AFC85
3	CC7420EA2DA0A20D000A9D05400B80ADC8B7F3B912E3E0C0
4	DB4BE96C665606DDF2821122831DF02BB6AD05E6D69A3914
5	D541947C799D15A15A0964421C5D1C131D5575B15A796ECE
6	D67F8B2930826E07910B7538EEEC8748F22ECC49B1D9B725
7	3B5B28B535D0B6215E95A46ACA1F8A0F74CA669424503CCA
8	07BC5520491ADFE0060149A6EC0ABF0D1F78756DF8061CAC
9	F25F6E7C9EDB35B8C0A730F3D9752590FA116EAFE20A0D48
10	D576D5198C9EF1420DB33F765E15182BF06163CDDCA61E4E
11	72AAFA9AA8088C236B525398F673822B5527FF0470085492
12	B784E6322B3C7A8124E917448BC62FDD921ADF4DF6E28023
13	E45A47777C1166EFB400C6EA6B923DD2834D2C6B941923DE
14	E5EDD7ACDFB485A7B67E48ADFF496C1292002B5E7C46D36B
15	F0B367EBEC2CE85EFEA2A7A4424383633B82F26E61E738D8
16	8C612C57CEC5C7E20B306456C6A10980CE0900CDE30530DD
17	E1B337FD9218EBE580204FD2046BF7335F417D9BC9BBB7A0
18	F0B5C1E68D135261CFA863EABF633B01F64C419BAB31E8AD
19	123D02C9A4D5D165EF55C838EEDE5C5E9697FC17DE3482A1
20	1A370E688177310807EB0403AA48615EFBBB84F0EEBE331F
21	3FEB947A3C2A7354743E1B82763CF4C118DBE1C29A896B0F
22	8F65A497265698920C16465F96B7E08E99694BB5DD06A81E
23	DB585BD8E1D1E6C2BDF6580ACD92003DA0A27493B1962B18
24	80671D354C6C82B915724E53049C62BFB635A7E84213F414
25	5529EECCCE7F5585D24114F7B64A980301900653FE905CC1
26	ABB2E0107FEDF8B00D9F6BAFA9DA4242811CB2664254CAC3
27	9E0B686DD73CA477A304CADEF7DF5E3188A39DEA9009C486
28	C4AACCC0B8768447B61CF3E925B78D2A64AF9AA40269B2EC
29	2956E8B39020A66B6E4DD2354B1E255B0751A3875DF8851F
30	1994C2CCD796BA4CF7DFD689BEA7CDD5E348195C001EC2B4

Примечание – Значения указаны в шестнадцатеричной системе счисления.

Таблица Ж.7 – Исходные данные к лабораторной работе 5. Часть 3.2

Вариант	Шифртекст Ciphertext для блока расшифрования в режиме CBC
1	2223DED6CF3A33BA6B5B795321F39C4E5211C2DB6E75D652
2	6489BDF449D8B92D87DBD4996D3F81AF0A9ECDC43F0B1919
3	8746F31A832694A5728312F437FE658155D5C0407ABAB818
4	FDC4BA36DA9B53D8F630D4182C6B514823BF69BDFD6D09F9
5	19155F2E63D16AFB69F551D3C79AE3A5AFBC9E0513B4088D
6	94FD9DD72760D1BC378C2A28064C000900654D6260350154
7	4262F0B1F148030C0905B1B8BD5A0A67608E92D6644A1012
8	2A1A23BA81DA58428AAB7A0C7904965EEA21FA9A5F98CE80
9	2A6880E2556462E04B2DD328DA9E504B0C4F2598FA1A6C2E
10	3B20C05DE9B6678F565A00C33E902CA74C56ED8698102BD5
11	138215F85046B3B4988B0186D9E6A4A21C6DA565AC84ECAE
12	917851F875474E25E40B9A7E3F2BCE489CAD6E61A867D4CE
13	ED2EA9A8858913065967468AAF5214640FF4C65A85C64321
14	0D8F37BD0CAFE73CF34BB88161836EDCA4A8F3A869B3FD5D
15	EE70F8DC9959A0010A4656FD319DADD6977663DE155DACBD
16	455B8E2CCB2AE89569C030DDED830B13BB7E7AC4EC479A2A
17	26C0262CB9AAB16FC707EF10D31A22A2D69D2DD04C98C560
18	FE963F84836AC06FAF56F86C2592B2094CACB6CA665215D4
19	516207EA8B81E26C32DA45F62661810699357919B31966E6
20	EFEB1F854BAA1B0C4009B646A901A3AB9E6297A288A9E5CD
21	AF1F687A0BAFC3D7CD581D9B51D613002AB4F62337B20398
22	828A66F93EC6B2D6FD83B417C49834732AF71691347692A8
23	53242D7DB821317BE18A05E60D8975D3C4952F9CBF5AF25F
24	333AE99765EC20CD2A58DB8D5A6E2E2841082FE0CCEFABB2
25	56CF1B9601CED1DD230116E2C0ED63F6E9FC4E11453DF186
26	71438EF5AED75D090607C19BE4ABB901315256A4F9B508F2
27	F818049C91EF42B5336AAAA26D6F9D543C1CC9B15031F52B
28	B99316AF7523BBB972CE92727DB923285655B7A85FA47814
29	698B923A892CD8EF6A1274FFA87739B73A60D52EC2E89623
30	FB31C6949C9A54A8387C63C07A5257F52605EFE69874669A

Примечание – Значения указаны в шестнадцатеричной системе счисления.

Таблица Ж.8 – Исходные данные к лабораторной работе 5. Часть 3.3

Вариант	Шифртекст Ciphertext для блока расшифрования в режиме PCBC
1	457F49AE0138999F14CD8EF7237C025B75A45CBD1DCAF50A
2	F51ED4277F4D16720D74C4A71E3B4ADABB77DE9E27478A6A
3	4E414A183057D291538D9D74F5F5BAA9C1F777116C93CE66
4	345A02380FC1851CFA0BC133DE0C2ED93D06E34494A4D2B4
5	22B31813D261BFE5D1F6ECABCEA5E43A97A6FBC555085822
6	15C3584AC751F54EF848971BA30208B4385C679E58E4921F
7	302EA118FDD8BD4CBEA36C638533451C6448393877E3842E
8	5FBC7CA5FEFF0AB9209C439C869AD34250939BDB607817C7
9	EF30F7B121DF374734A428D9EE547586190621D29E4C14D1
10	E26A3BA678FF6F38525EE23912DF046A48BFFC0F7876DD6D
11	884C56E1A84392703EDBEFD7F18087093B3094095DC4C000
12	E17D88EA186FD841B298F8E0D1BFCFF6299DCD5A8C4236AB
13	0E4AE3B890F85487019E238309C943E9509B7F0F10AB6883
14	2EC0B23101889E12120459E132B7C9CB0D91E05ED480F5A4
15	6C581DF47228748F6E518CF98560AC58CB661A30CEF89B82
16	FBD91B78A155586E2E726DF5262E1E2A4E44678651BAD3FA
17	13DF5A1E3E07930650FF4EAC31F61DA6C855B183CDF0ABCB
18	CE59EA6E819E4A8D463E931B747E41F64F82B30C79CF95A5
19	E17BA7E244EFB4AED1F9F0D9AE673C5A88A200D47F65B977
20	DC1150BB5553194152D7C80B5BB2C1A2FE4D3D3D459B549A
21	4E2A75C426B755A14E4849093077F2DF78203A404509847C
22	9C5AB7E6A7ABFFDDE83051DEAF1B2D72E4CA161DD479816E
23	E937075DAB2E2090A393AE0CC1018EC630F416FBF7315C7F
24	3640778CA5EEC735828ADED35CD8FF15F182A1298174D60D
25	4566DAD1E88282A6888A52A253C1182E1CC836F03C5E83B6
26	88D3B845393C038268A3605B151544AD9ADBBD7B9973F0C8
27	EA44AA754EA7CAFBA8A6A381A673958DE4AC5433AAAED5AC
28	D3B32424A6ECB570FF29B3C1363B3064543A243F45153D2E
29	D5DD213758FEF2D876473D024C534BF5269FA1390ABB8CED
30	516CF5E2AD2B63DA49864927E86786E8BFEAAB34002EB9D4

Примечание – Значения указаны в шестнадцатеричной системе счисления.

Таблица Ж.9 – Исходные данные к лабораторной работе 5. Часть 3.4

Вариант	Шифртекст Ciphertext для блока расшифрования в режиме CFB
1	42BEE3CA4F36DBBD77B34EF460C5CBE82B07B3316C2E87AD
2	34275A3ADFC27036987FB20B46407407DA7E1CC0D866E410
3	25FD2353EB6D0727DE98F46FAFE5AC827AAF69EDC0AAB07D
4	FEB978C3801FB667B8BAC9A92A53E4F17E762702A2C672D2
5	62EC40D7E8EB47656B3F88BD145E99980E8C5F1646FF6635
6	D6AF7A2C123CAD997920CC9A482F58638A861EDE514AF67D
7	E3DA43947EB2C72127186C2843692E5D6A8005D31E682044
8	D8971D489712F9D23DBEC9F671613AB0B6CBF96873C048FF
9	FC6843A9C3E4DBEEDFCFCABD4CBA597CEDEAEB8CF871DA00
10	3695C2B63D7CA31770F2FB406DD6CB20266D5E16EE511DF0
11	5CFB2D91DA046545930C36B9155371C98DF60451FB3F0781
12	8FB94D1FD822980808001E1AEB808F414FB538764AE1D9D2
13	77FE7C8EEFDC44CE8BF47D0F371DCB9DCEAD7A0F72BAF3A3
14	B6562931D0836257308F7D84AF67178DE60650BD7188CC7C
15	400FCBB4904009D0AC6636A6034671AA5FE76D6009085D01
16	AFF97198AA980E3A621B08EFF12B5DC643C12B2994C7D026
17	38EE29D8976C1FC661ABD786F8B47F14B34684FE1916B166
18	5BA366E05E0DAEAA783A94F3A67DE0B69AA91112523881D4
19	E60BACF81255574F703D7455C812DCB6341A6FE01B123F4F
20	AC307E741D07660B36F827EC1CFCEDDCCF95A0433B18427D
21	C8A0483CAB917B15C44ED98FE798FCA62E7B6D5FE8ABD6D0
22	08C0A40CFD0FC7A6120DAEC48F2FE6DA4948E8F7763BE46E
23	9EFAB0CD0419EEACFA6C133AD9F6FF047D742F2A08530077
24	5366311EE3F2782C48812544B229B6BB4C85D653E3E0BFB6
25	B85AD74583297B46E41072D9BC1B01AA1FD4F3B3B3EDB95B
26	387B13145154585F2B964F981F41D34AF6699CB5DE90E6B2
27	C313A9C03E90EBBA9B5434EAB214F3E14150BC9C2B2EF80C
28	9398592CC8E20A8056CC8D99A0ADEAB83FB9BA32C99ECD9F
29	F6C72FB6F5E7A626551EBCDAEC1B4135A538E558BD613B1E
30	BA2CCD6C853E17BB57611EAFD8034EDA91A18555E7B3C847

Примечание – Значения указаны в шестнадцатеричной системе счисления.

Таблица Ж.10 – Исходные данные к лабораторной работе 5. Часть 3.5

Вариант	Шифртекст Ciphertext для блока расшифрования в режиме OFB
1	0A3A2965C6331ED7CF84F560D1A1A9C2B4DD524E6F5F2D2C
2	F5501E55AAA79E73C4525F608BF3B1C2F42AA8DA33D83F02
3	891D91A6771D1C6B83B6CF7D8B5A22B0A65229196A8626AA
4	A708AE937DE046BBC8552DDEFC300BA6393B4E9C8E3CAFE5
5	7AFC378C1533BC5C949374AF986E90D4A024AB3B8C85A6F3
6	0F032109E7DD47A31E3DB16D857CED7194A1D49E0130B2D2
7	506D0D3BD94C7524D437A5B5DF616A02BB1276A9C365B20A
8	D587E9EDA17E66BE28A1D9BDF0521FB1DF433D87C7CBD03E
9	ED9E342CA2C3B647AD3C72C08654DFEC1ACB5D6527CC3BA3
10	ECA4BB1169D290A9ECCE82BC77BC5A2A33D6EE49AD7A2801
11	01EAC556E5F3797E626484B5C0251DA92FD4538C92967C29
12	B2575CDAA45C77AE300C595223752C638D12CD45C206100F
13	CBB9771121F4FAAF58E9B8186FC53245ED6BAD7BD90F5822
14	EFA10E06F1150069B34D2CADC95F8A8F9F14671EF85F42E0
15	3BE5175893C4366F3F0940EB28879FB5D84E7C910A42E696
16	4320305F38D37F9C2CD27C8B34404A07AA8131BA4AB34DF5
17	390D92948F1468318ED43950C92DA3534DD28663BD9EB3C0
18	854BB54DB80591DC75D27938473970C477B12312658222C3
19	4F5A8884137F35F59030DA483EE5C9F6BADCB9DB2009DC8D
20	8934252406A2C388155F8CF51F9739D14D9A6EF0A94BC2BE
21	726549D6F3CBC454546B6AF29AF0B4CB7E74595D1B3E660F
22	30E603F21B38E7A40C04DE7049D7C10AE43DFC7762380103
23	FAF0DACFBC7F32EE0D4DA4A329A91B130816C9AC6EBCECDB
24	3C5F8B39EEA8D6AA084EAE5CDF142CD9551A4DB8150A9554
25	0F7C5C2E2AEEF5CA32CE1D4B52A93C19F8C2E54538BE0EF7
26	6D73C2C4754AF95937C725A4D375E645D7C2C37DB1084531
27	8A9831939917FC387BF60950E931E0049A11529A80931BA5
28	AA5194EEE0DDA44EE8CFB13DE1CC2143971B75F8812E2968
29	EA70B92074375BD2B3EBFBE55B2F527F09AFCD00FD9E1E8B
30	4465DD8A5C896A2C57D710A9EF14110E8620EDCD4E31EE91

Примечание – Значения указаны в шестнадцатеричной системе счисления.

Таблица Ж.11 – Исходные данные к лабораторной работе 5. Часть 3.6

Вариант	Шифртекст Ciphertext для блока расшифрования в режиме CTR v.1
1	C4390BFF9FED01AE0197218A784EBC4F2235CD6BCC157527
2	73CAC482596E66E11C5B20757AB25CC1637F8606A3368EEF
3	9D5352CD48DE385C6BDA37413D839DEEC92026A530D7FF74
4	11636453A2117BD17B7AD00B8F1EC2C2746166C993473231
5	BC8A2D6FCDB6EFF1041A8D7CBD577B0B6A1D3E2A6B7607BC
6	87E7E5F700FCCFE2F97BC5E215317C5997D9FAFFE53F2357
7	A3BA01EB828EB689C0405E84F386F913BB4BBE2A8ED095C8
8	8AFCC3583857F41DB19E4CB900828988FD429231EEA54B01
9	F4389C465485E72BDF3E8156B95843DE75DA2F1A5236B5AB
10	624DC9DB6E43B82E24F7B372A0806D0BB4E885ECED7B8921
11	06AAA1BFD1BABA3DBFE9B552ED284838B878FBB41EE01144
12	806FA7362BED797B75D8B9B0E24B18FEED263EDF1B037F91
13	B8DD95967A74991AE2BE921FB03AAFF6FBB921072E07071D
14	951ADB2B104562EE7DC1FE65C559C61F106097282B4E088B
15	E5D96385AB9917E48850B2571E79182A3415993AD61FC210
16	7E1362E5A88BC3CF92A33CCBA81F3F4E92B1E4E5E5C98683
17	3FF4FF90E7631BB7F5F43267F053A791525059E26AE8447B
18	159E275F026B5CEDE2553EBD4333A8C2224BD6C94ECEA3CE
19	4E87326DAD02041A733B52DB483A7723D873890F2368C1C5
20	A7619F72EF4257D0674B47350BBCAC311C44F0A74CF99290
21	886B3B281C2291CD863221544A602162E7C286AF4662DFB5
22	7AC1201FC0DCBAA7662B4AAC133E5C2788D045AA08D8FA17
23	140C13FD7405E1D9D8D7C8AA6180C3586F116A3CF1386DAD
24	BA7525DA7F9B69BE07BE5EDB6BF920114A01C8013F21145F
25	FFF79D4A0ECE403BCDD1DF1E7B9E1DF6F94399CA4D0853B8
26	737BC45985A640E49BAB501BF00E45E5C935458AFDAA7F85
27	4D53CB1ACEECA13BAD805C0188692F62AC15871D94BCA340
28	0861E06ACF0537DC9A99DAE797BEC3A4C58FA325FA06B3B0
29	A11A901561EFFE688FA8E91522515B5BD794514B6E5E5A92
30	C43E6D6FCD0EE25A4BADDD55D531D1B244879CDD632A22B9

Примечание – Значения указаны в шестнадцатеричной системе счисления.

Таблица Ж.12 – Исходные данные к лабораторной работе 5. Часть 3.7

Вариант	Шифртекст Ciphertext для блока расшифрования в режиме CTR v.2
1	AB0A6C4C465C57637C33518500F96D7FEAFD2BBFF5DA7400
2	D41407FED7EB93F8E8A617E7490CE80685F62E15A4F9E418
3	D54607F2466CB3F7A579E8A1D96407A25E56B9E5E9B77609
4	1CA6C57BEA9318DE9D50BAE721FE7373639CDC1BF7D4661E
5	83DEB3E99459C070697ED4618BA9B7ABF49AB3FD1356D6C2
6	D47B09131D3C02A425CE4B1692182E656C25A7F70A145701
7	94A794E41DDFE4A29A331ABA2AEFF211899623AAF1A59A93
8	551B5A2FCD27785A4E4C4AB23845DDDDCD7D911FEB8A9BA3
9	DCCD8DEFA3BD33ECEA0F3387073249CFED5AD6EC7193C68A
10	8AEC7E9CBD3CF09944E513D7080941CD5F45BC553C6DD7D2
11	A9EF7B3D34FE1F3D63771843E119A3EED8E08F139F19FD3D
12	85F0072365A5082462C6629A26F021A8326116B9434287EF
13	C66C2FDC27A74EFAD37D1EC33B81FA2521AB6A958C416C30
14	1793C65622FD9ECF4AB363C114CB632063D54CBEB907D59C
15	339E875BCEDB222D8F632EA8E41AE414C4D6C1F109A4F140
16	DB061E497A76497EA2549E1AE7E02BFEA8F4FACFC082CB80
17	EEBFEBFDA1FA2D5CA9DC939AAAFA0EED6A0B653FCDFC5B01
18	6029746F94AF3DEE28F5BAF040A736F2042A3A8BD886638B
19	CAA9FD0CFF5BC3A40CB59A6D6BA9103B5943D3ADDC7320FB
20	7DCD36037FCB9ECC3C2AFCE3FF7C073BC703A4B81AD580AD
21	3E3ECB7F9CF083B2AFA74D4157282103D1214F7F306EAECF
22	056A5CF5828F450AEA62876822BFC0A4FC8D8E87085356A8
23	E4AF3B8701FD70AF7E23ED344633168C3B6A85D020D0569E
24	2832AFF9C1DD4945646CEB5BF349577C01C62B957E2BBDD2
25	ADBDF2F1F5D1FB8D075BEDCE6391D471482C246EDCDAFCD7
26	89E08EEFC222F83DC34A6F263EF0074B6D3E883E4B95AC7A
27	97FC3EEEAD0B9B129DFD78A1C48EF08BAAC4A714FC484530
28	F7C1FF02D805954CDB888E56A137A2E908793A0CAC8A2ED0
29	B670C9836FCF556975DA8584A2DB4DCC8AD02B2B7681BF6D
30	C207A3171CACE796F49473DE54E7A26B4C00E40F4CE5DDBD

Примечание – Значения указаны в шестнадцатеричной системе счисления.

Таблица Ж.13 – Исходные данные к лабораторной работе 5. Часть 3.8

Вариант	Шифртекст Ciphertext для блока расшифрования в режиме CTR v.3
1	35B8C96570276C80E554893201C43E53E77FDCFB6575362A
2	FF6D7731768CF604694D746C9FABBE08B23514FB17616BF4
3	7ECCC3041B2FAA055882BDA32EB2B2DFE57AA0374B056AD5
4	F0F4F2DA01C5EFD0BBE34DE4626DCBCDC3509A12DBE1FBED
5	E3546D543D532928286423254D6E641AEE6AC72462FB1F5C
6	19787E9A894C9BE9F20EC30486B242B558A7D27BDA86E554
7	F0AC8AD473E9D74B0750A749716C65085F1DE123E512F373
8	AC84CBDBD4A10AE5FAEDA49D13DC81AD1929FECEB5443DDC
9	78029E70BF1C3E4CA2EF3F0941ED820CC9D5BFBE8755B82C
10	9559F84C6B0D60B495667CB051F73E03FB85BCA63EB1A93D
11	74D28D1EAF5A8B8F770A76CF92FFBCC5BA8F5DC3BA1CEC1E
12	4B198EA64BCBAD39AAE78770C82F366DA0985C76F17BA426
13	559C24FFA67AB7671D2C55EDAD82B3EC96C213961ACD6040
14	01CA8F9895BE762FCA15422451D28CFDD91834F62A1DEA8E
15	11D6D45459D9F1B5FC6DD697F751D40812F38F78723A3D32
16	6D2C5D4A57D7F0A9CD06D28CC99877B229F3D6EFB93725B8
17	047547C8A26617A50471905054C473E1E43ED7F3CC64A92B
18	A9B8C7C413FBAD4D98C1A671B4ED8EABCD2EB99116F514FA
19	57D01E75D43A63C04D1EF5A3A9E0140462A6987F21033A00
20	64DE750A69182A95E447EA8F2F22F34CE5082D5BE1D6BA86
21	56C94B72C45078E669DA3BAEBCCF9197781DBB9845B11A18
22	81097A44D1B4CACCACB89C5E1BD407503E79126F56BCF39C
23	78D5015D502251223CE5732A4850A24948D43388E4425330
24	60D03AA34A38A0E0A776CBB325C2BC4DC40C6B6D58F9AE73
25	D4F836AD757B1F63326E56591C88F46211135D937ECEB8EC
26	BB696C1C7D9647010FCA56D95912325FB35564F7601419C1
27	11FD1B343BA53C7E984C9F89D7E8AE932D538D98D0B39ED8
28	9807A3947E042D3E910641DA9879DAAFAC8BE4AB4503A0BE
29	6BEE33642A66AE5EAF530E4FE491C10F8DFC40C4C5CF08E0
30	3680564BCE5B34542D344B1E38327025D76DFF045FEDED45

Примечание – Значения указаны в шестнадцатеричной системе счисления.

Таблица Ж.14 – Исходные данные к лабораторной работе 5. Часть 3.9

Вариант	Шифртекст Ciphertext для блока расшифрования в режиме CTR v.4
1	025FFA8F5F755E3A9B9A07C924F8842D28941B8CEB55DA92
2	4B860BB780639695B603F3E83A6A7D8B79BDFAC3F920BE76
3	EEF8B251CF5131D6B2586D03233E4903B87BEED71709498B
4	6A75FB369DE72DA1FB5CA51CD3E3CE6546BF16046CC41EF3
5	7594F8FEB5115DAC40DE162285D1AC29BD24D015F5C30E08
6	CB032205A68E15CA82FFF1E152798A657425CD27A29C2551
7	ABD569EEA9145FBF6248428DCE48889A4035CAE2D85E23F2
8	09807FB96D9EE53B8869776D06E356C4B401CEA3078056F3
9	CD6E5220C659B942B70698F61864D7B8B1785F6DE80D3E35
10	2FF935CE233FEAFA5299FB002D1BFA7D1536EADB5FE74430
11	8DF13FDF93780ECF3535AE16E8B4116B5D8D252D6C0962DB
12	2513F56368E3C38318285344A70C9AB170104B05FA817723
13	AD4DC2A2740CDDDD515251479E7FAC83E24C94FA8B9414C7
14	D1C070B6784B0606CAC584B7AF2DD9F5F7BB939CA81609BE
15	C02077C2D625222CC92502FA5F0BB14456FA6DD434094FC1
16	38CA7C5992171ED932997919ABEF172D4863F98FE3E81451
17	2294C7868350E5391822837DEE40CB337E0637889CCA8E3F
18	945059E8B578564D93C1CE113774B98769D1E0E39541DC8D
19	91D5BF0FC610894519722A0848028123F86CF1275DB44C66
20	779210766522F02398317B18B90727D19C486D814E0B2ABE
21	94AF10C7A5C1E2BB9A8C53B1BDDC8B20878480027F3F0001
22	888253103815BCEC028E740CFE588219136EDF70A8A29292
23	1E13624DA46E7A3BC11D8DA52D255B971331300B3C56A9D9
24	EDDCFAF15D5F1C4A0FC39D74E719B2D40D81000A5D8AFE0B
25	9A4921993F8F7DBE93BCAEEBDF84B8B52CB8394876213BA0
26	09A221ECF6DC6F9585E282D9CE2B004532DC85C1ED232512
27	FC979B022FA07E236471D17226C8B07986142D89DF34CF2E
28	6D879B2B4E95C0D95C273EB46D4482778A9E2F8C6A9EA0E2
29	66D979804059DA2DA1687F7FB45D20E2D39425E6F547620B
30	80DE7D1F3E4D3D6BBA571529ACD9AC21AF5BB7BAFFDC0106

Примечание – Значения указаны в шестнадцатеричной системе счисления.

Таблица Ж.15 – Исходные данные к лабораторной работе 5. Часть 3.10

Вариант	Шифртекст Ciphertext для блока расшифрования в режиме 3DES EDE2 CBC
1	F6E1B3197AC3C9651EE7BE84C490781C6A5A1C1BB508BE05
2	FEE3EF75A9DB413BE059BAA013A7ADD972B9522A551DAA01
3	97A80D60C005CCF8955AF3D5FBE2D3389A9881A8AF6EE5C2
4	40A5C41C9F76A5003CE7F82DCEE27CFEC18F64DAA0DA44B9
5	0AFF6E80516820AEBE06B04D16C2FD7019C09163B462917D
6	470F6098A4F0B57B8DFF32BAF2CF015DD199A392A0279AF9
7	201AC6A2F758ABFB568727F4E10DB7FD9A336BA243FE884A
8	A925694B7E935F316DFCE2813608EA4680FF6617D8986CB0
9	8571E7D0696EEDF8C26B99A1B63573B7B3255493BCEE7185
10	66542FF75C6B45E59E2EC923F75B86A52C154974E887F07D
11	3BABB503EDDB883511B997720A4952BD3DF1B1FEA5049962
12	B6A23376F0F6EEB2E190A57DD8963000F8E443B169857525
13	D98E4675C9FB608112FDF9B301A18D349F67F5743DBC7306
14	3EA71E467E47582EAE0D32D3E331E22DFC9E2BB8DED03A86
15	CD861EB936C2BF9AC3DCA5E412706096A1ED54F860C62951
16	37882EF78ECF36565E00C7747F94C9142480934E4F59F526
17	246F90879D77AD1EC9572FA9D95047FCB3496851DBD23450
18	9BFA97B029CA71717DFF102783804393CABB7651796DD762
19	633620A63A96DB631F399006DBF5F1AB93CF48A5F708A02E
20	3645F08DE9E2CA1F7FD03A1200713123078DAA0276A69E2A
21	B6187F36BDC27593F12AAB2F4080D9618F182BA69D4E6C97
22	7747D9D95B9E8AA2339719390FE5ED89BCE19E1BF7771139
23	56ECE40787A9EE9A44A83AEA2910CA261BC3B0F58742B673
24	E36AC34B9C4D91E6231030FAD59A2D4647FD7C4129AD4FDC
25	8BF9E89DDBD30D464FCC3E819FDD105B3B85A20D61BBD414
26	3E8AB64E2A1EACD5B73347F638DDB8270FF0A911229F8DEA
27	87E76D4DC34C9F52FD38B9ED21C65D1670A6A25E3B0E314F
28	49374E762E7CE81303B3AE13A3FA71839DD8BD10B0AE5550
29	0784158FD1B888D3D6DFF0BB28EF14B5F0A5B83514AA2754
30	253F05A454596F849A54E33A3DFB2CFE518392F37B45D8B3

Примечание – Значения указаны в шестнадцатеричной системе счисления.

Таблица Ж.16 – Исходные данные к лабораторной работе 5. Часть 3.11

Вариант	Шифртекст Ciphertext для блока расшифрования в режиме DESX PCBC
1	4840A04DA4D793DE5D5B98E5A091D7DC370A444DB2CF172E
2	3FE6057C0DE47694C77E081C1E0159961E4EB5D519B10B8E
3	5C275C3E57BDA2BB7D9CF08A8BBA95E9A205EE859FC09BFF
4	3C2C795FECAF3E2F5B270260D014FD3B89F891E74FFD10A4
5	03A1021C7C2A647B2409B1C06E45C6C4BD6F0D685DAC7204
6	8B9C2DCD0D6AA8699D9E2D1121D0E80A79D24DC5C4B2D628
7	A2972F2762E9234FA36A181723FADFC60831D6F60DE222BF
8	DBF6D547AF9D6D4512DD511E161D91CFDED604D57389657B
9	1378D5E6315B3E5C2A9A37652D91002A65D3CC8AC085B910
10	D8EFCD0968EC9568705CE786E756ABD3E991D6D78468647D
11	23AE7B762AA6F5B945C3C2E90E6898540A7B249A2AEB84F6
12	6A9B2819BF5E5CA30555F1001A5D7A02202FE4C4DEADF1C1
13	9EA2051D8756C0C81E6FC8BE357FAA6BD2BACBA74E72DA2B
14	D64410E840EC462D9B3D3A88A3548224E965E7EDDB892956
15	8ADC7244B0471C2F660CBCF6631127F5B9CBA44D9643DBE3
16	15240EF82EF829E0504A4D3F12FB0ED4DB2867258AEC1EF3
17	958D7FBAFF9FEC71DAA9E9D7B2D70A6807076B2D5098FB4D
18	6FFC9DD1CD84B16C563296A15D2287D8FC8DEFA03B63D3CA
19	53306C2534F8238382E5B70C8ADBF34E891F694FBA125024
20	D3AFA49B31C3A5C5878B531245DE7C2099FE2D689013ED56
21	6F63A224CF330A2DCD958F3C95BC4FBA027C89D24070513B
22	7CA9CEA42F5CBBD7398D531EAA9272B3CBC1D9D93F1396CC
23	39E4C3CB6EC33C34EEC42DAE89E1EAAE08B852D898C46E57
24	DFBB214D0D425FF6873D05B779E29E10B0BDF6E035D9AC2A
25	C206D03DB3736114B8543E5BA37351CEF8675EADAB598E43
26	BC6D63DD3A13AF0EE059C9B9FE0702C0FAA54927824C75D4
27	952A60F55F23E957E915A1683F71D9B8F92CC67AFD664BCC
28	0F75288263D9CD31632DA2F8474EE74CE336DB176AA9E22C
29	E669AF4EED35DE0528FC91744EA3A9B105616EF6CBA301DF
30	C5D24904A80581446EC62BCC8035D1241D31D4093562465D

Примечание – Значения указаны в шестнадцатеричной системе счисления.

ПРИЛОЖЕНИЕ И

Примеры решений практических заданий

Таблица И.1 – Пример решения задания по лабораторной работе 1

Преобразование i	Последовательность C_iD_i	Раундовый ключ k_i
1	C3C29BD16E4BA7	59B8D51CD791
2	878537B2DC974E	994C7CBC38EC
3	1E14DEEB725D38	C46B9C60DAF7
4	78537B8DC974E2	16BF2517ACBB
5	E14DEE1725D38B	CB3C63AF1D51
6	8537B87C974E2D	E9E6EC0BE376
7	14DEE1E25D38B7	D0D78A75CD84
8	537B878974E2DC	709B73C804DF
9	A6F70F02E9C5B9	BAFA30F1B5F0
10	9BDC3C2BA716E4	8C375E29AE2B
11	6F70F0AE9C5B92	66565D7E7C16
12	BDC3C29A716E4B	4FD9602D41FE
13	F70F0A69C5B92E	8AE9FB85F8C3
14	DC3C29B716E4BA	BD670BE68675
15	70F0A6FC5B92E9	631F899B8FCE
16	E1E14DE8B725D3	3A30E945372E

Примечание – Значения указаны в шестнадцатеричной системе счисления для исходных данных, приведенных в таблице В.1 (вариант 30).

Таблица И.2 – Пример решения задания по лабораторной работе 2

Преобразование i	Последовательность C_iD_i	Раундовый ключ k_i
16	A91D1A39F7C8E5	8F2A6E81E79F
15	D48E8D1CFBE472	D9E103D7A2BE
14	7523A34B3EF91C	72CDE1F05A57
13	1D48E8D2CFBE47	4575C2BD6BA8
12	47523A3CB3EF91	01FE5DCB7736
11	D1D48E872CFBE4	C83B41BADC19
10	347523A1CB3EF9	B25F2859EFE9
9	8D1D48E472CFBE	8C62EACED6F4
8	468EA4723967DF	C1C49B7D157C
7	D1A3A91C8E59F7	79A56156FF1A
6	7468EA4F23967D	627D83EB8B6B
5	1D1A3A97C8E59F	05EF46F635F1
4	47468EADF23967	C0F85906FB8F
3	91D1A3AF7C8E59	581F68FA41EF
2	A47468E7DF2396	AA76887F3685
1	523A3473EF91CB	21879FB53FC9

Примечание – Значения указаны в шестнадцатеричной системе счисления для исходных данных, приведенных в таблице Г.1 (вариант 30).

Таблица И.3 – Пример решения задания по лабораторной работе 3

Преобразование i	Последовательность L_iR_i
1	CADA5961F493B87A
2	F493B87AB9A65E3F
3	B9A65E3F26A0DC48
4	26A0DC4850AC3B7F
5	50AC3B7FCEC500FB
6	CEC500FB4435D1E0
7	4435D1E07281A165
8	7281A165E4EF2195
9	E4EF2195893EF208
10	893EF2084415BC48
11	4415BC489CEEE5FD
12	9CEEE5FD595C34E8
13	595C34E8A8CB2809
14	A8CB28091A884C3A
15	1A884C3A1DC4800F
16	1FC56CE91DC4800F
Шифртекст Ciphertext = D342F6C7C0053539.	

Примечание – Значения указаны в шестнадцатеричной системе счисления для исходных данных, приведенных в таблице Д.1 (вариант 30).

Таблица И.4 – Пример решения задания по лабораторной работе 4

Преобразование i	Последовательность L_iR_i
16	40634235495B6FBE
15	495B6FBEF307C875
14	F307C875F850295E
13	F850295E68A71E8A
12	68A71E8A1D4901A3
11	1D4901A38C7B9E83
10	8C7B9E831E82DBC5
9	1E82DBC53B67A2D5
8	3B67A2D51D3413F6
7	1D3413F662DDF0D3
6	62DDF0D30AA1CB07
5	0AA1CB07C936C277
4	C936C277DFA78429
3	DFA78429552390CF
2	552390CFB4AC4DD3
1	B4AC4DD3FE05995B
Открытый текст Plaintext = 6AC7F4DFCA90C2CD.	

Примечание – Значения указаны в шестнадцатеричной системе счисления для исходных данных, приведенных в таблице Е.1 (вариант 30).

Таблица И.5 – Пример решения задания по лабораторной работе 5. Часть 1

Режим работы	Шифртекст Ciphertext для блока зашифрования
ECB	328F78AE4F3D82E5994960B3C4A184B2932262AE87F6558A
CBC	C29AD7BB66E6874D160C0A75B039346AF5D424CF56952DFA
PCBC	8D69B93086ED0C341F9ABD625CB87736755F98B82A5E9953
CFB	7B1ADA8AAD5AE3DF4AC5C3164FBD22499BD998007999DBD0
OFB	8D2685F1C25EED52FF5999569C63002FB539EE1A7CCEF3D9
CTR v.1	45B2E165C7CBCB7CF6424E6A982A3F7B769CEFE9AC636D47
CTR v.2	4538351FB49082A82079103835DC11F2391B9EAAAE94D3D3
CTR v.3	E0D395A9BD227438DE9C92708A2A7D3E1F2B3AFF3D9D438F
CTR v.4	57FC3BDBD24E72439FE6824C9852CC57A7E3973FF431C819
3DES	3208716A0DB51FA224B48A6748A8972340073D36C3BF1989
DESX	685FAF8A7B73D2E34522F5E5EBAD1CAC8534EF72A54C37B3

Примечание – Режимы работы 3DES и DESX рассчитаны при условии их сочетания с режимами EDE2 CBC и PCBC соответственно; значения указаны в шестнадцатеричной системе счисления для исходных данных, приведенных в таблицах Ж.1 – Ж.5 для варианта индивидуального задания 30, а также данных из таблиц И.7 – И.9.

Таблица И.6 – Пример решения задания по лабораторной работе 5. Часть 2

Режим работы	Открытый текст Plaintext для блока расшифрования
ECB	#20359760BYN
CBC	#55067101BYN
PCBC	#28198760BYN
CFB	#55598954BYN
OFB	#36800065BYN
CTR v.1	#79859832BYN
CTR v.2	#72650215BYN
CTR v.3	#93446606BYN
CTR v.4	#96170582BYN
3DES	#93194760BYN
DESX	#30512435BYN

Примечание – Режимы работы 3DES и DESX рассчитаны при условии их сочетания с режимами EDE2 CBC и PCBC соответственно; значения указаны в шестнадцатеричной системе счисления для исходных данных, приведенных в таблицах Ж.1, Ж.6 – Ж.16 для варианта индивидуального задания 30, а также данных из таблиц И.7 – И.9.

Таблица И.7 – Пример решения задания по лабораторной работе 5. Часть 3.1

Режим работы	Секретный ключ Main Key	
	для блока зашифрования	для блока расшифрования
ECB	0660B8F3F0174D33	8756968756142D7D
CBC	55C3FC6A41CC1EF5	DB6C53F68D3FD89F
PCBC	C0717865B8849FCF	E4823655939039BB
CFB	789F7BC9C9A5A5E4	DB82BD96BD30FCC0
OFB	122D428711EEDB8D	06847D2EA6AAB8E4
CTR v.1	EB829F36F9BE2BED	11B15C77AF8BCA88
CTR v.2	DEAF051E5CC048A6	A399278BEE4D4B8E
CTR v.3	A947840A7B8BB118	B14D039C9FF3C94B
CTR v.4	871BCF9A74051BA3	5339ACFCD8CF4E74
3DES	k_1 = 5C5A507DDB412BBB; k_2 = 0081F99FED05289A	k_1 = 90C577F377E47D1E; k_2 = BE78816006CF1718
DESX	k_1 = CC63A56F0AE11135; k_2 = BE3CA5561450A0FA; k = DE0312286F4B9FB8	k_1 = 6C7BEB24DEE4EE99; k_2 = 6C1D7DD1F3C3AC6C; k = 4148E73990E84835

Примечание – Режимы работы 3DES и DESX рассчитаны при условии их сочетания с режимами EDE2 CBC и PCBC соответственно; значения указаны в шестнадцатеричной системе счисления для исходных данных, приведенных в таблицах Ж.1 – Ж.16 для варианта индивидуального задания 30.

Таблица И.8 – Пример решения задания по лабораторной работе 5. Часть 3.2

Режим работы	Вектор инициализации *IV*	
	для блока зашифрования	для блока расшифрования
CBC	AC032F656FDEEC7D	B45F03D2C28A2BBD
PCBC	94901A6474AB4025	45772F4F4F21F626
CFB	4B698B3D7223E69E	6F1F3BD35C32E558
OFB	690AAF5CE6DFAE93	8197482531294C2C
CTR v.1	7E1C229CE40BEC3F	C12ECD01A6BE87A6
CTR v.2	1984BBA91B0760FF	7E462789C4C3798A
CTR v.3	C7215F47DA306FED	8EA2F036FBAE3411
CTR v.4	40F2BEE449BC4FCB	8B3F4CFF5DA3E4B3
3DES	40E124449F5D1649	6FB71D61CA1453B5
DESX	E527DCECF1DD2C3B	14AF2B2EB7E0403D

Примечание – Режимы работы 3DES и DESX рассчитаны при условии их сочетания с режимами EDE2 CBC и PCBC соответственно; значения указаны в шестнадцатеричной системе счисления для исходных данных, приведенных в таблицах Ж.1 – Ж.16 для варианта индивидуального задания 30.

Таблица И.9 – Пример решения задания по лабораторной работе 5. Часть 3.3

Режим работы	Значения приращений для 2-го и 3-го блоков $Delta_i = (Delta_2, Delta_3)$	
	для блока зашифрования	для блока расшифрования
CTR v.3	(30581, 25515)	(58659, 11665)
CTR v.4	(42890, 22780)	(27288, 25625)

Примечание – Значения указаны в десятичной системе счисления для исходных данных, приведенных в таблицах Ж.1 – Ж.16 для варианта индивидуального задания 30.

Резерв, 2023

Учебное издание

Тимофеев Александр Михайлович

СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ: СТАНДАРТ DES. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *В. М. Задоля*

Подписано в печать 26.03.2024. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Times».
Отпечатано на ризографе. Усл. печ. л. 7,32. Уч.-изд. л. 7,2. Тираж 55 экз. Заказ 245.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
Ул. П. Бровки, 6, 220013, г. Минск