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

Факультет инфокоммуникаций

Кафедра защиты информации

**А. М. Тимофеев**

# КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

*Рекомендовано УМО по образованию*
*в области информатики и радиоэлектроники*
*в качестве учебно-методического пособия для специальности*
*1-98 01 02 «Защита информации в телекоммуникациях»*

Минск БГУИР 2020

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 №10 от 05.05.2019);

доцент кафедры информационно-измерительной техники и технологии Белорусского национального технического университета кандидат технических наук, доцент А. К. Тявловский;

заведующий кафедрой инфокоммуникационных технологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» доктор технических наук, доцент В. Ю. Цветков

**Тимофеев, А. М.**

Т41 Криптографическая защита информации : учеб.-метод. пособие / А. М. Тимофеев. – Минск : БГУИР, 2020. – 112 с. : ил.

ISBN 978-985-543-555-7.

Содержит 12 лабораторных работ, направленных на изучение используемых в современных системах и сетях связи симметричных и асимметричных алгоритмов и стандартов шифрования данных, протоколов идентификации объектов и алгоритмов электронных цифровых подписей. Композиционно каждая лабораторная работа включает краткие теоретические сведения, практическое задание, содержание отчета и перечень контрольных вопросов. Для выполнения практических заданий используются специально разработанные компьютерные программы, реализующие стандарты и алгоритмы шифрования данных DES, ГОСТ 28147-89, RSA, Рабина, Эль Гамаля, протоколы идентификации объектов Фейге – Фиата – Шамира, параллельной идентификации с нулевой передачей знаний, Гиллоу – Куискуотера и стандарты электронных цифровых подписей RSA и DSA.

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

**УДК 004.056.55(076)**
**ББК 32.972.5я73**

**ISBN 978-985-543-555-7**

**СОДЕРЖАНИЕ**

# ЛАБОРАТОРНАЯ РАБОТА №1
# СТАНДАРТ ШИФРОВАНИЯ ДАННЫХ DES

**Цель:** изучение алгоритмов шифрования и расшифрования данных DES.

## 1.1 Краткие теоретические сведения

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 (остальные 8 бит – проверочные биты для контроля на четность). Дешифрование в DES является операцией, обратной шифрованию, и выполняется путем повторения операций шифрования в обратной последовательности.

Алгоритм DES поясняется структурной схемой, приведенной в программной реализации алгоритма, где также приводятся все таблицы алгоритма.

Для шифрования данных 64-битовый блок $T$ преобразуется с помощью матрицы начальной перестановки IP, что можно описать выражением

$$T_o = IP(T). \qquad (1)$$

Полученная последовательность битов $T_o$ разделяется на две части: $L_o$ – левые, или старшие, биты, $R_o$ – правые, или младшие, биты, каждая из которых содержит по 32 бита. Затем выполняется итеративный процесс шифрования, состоящий из 16 шагов (циклов).

Пусть $T_i$ – результат $i$-й итерации, тогда

$$T_i = L_i R_i, \qquad (2)$$

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 описывается следующими формулами:

$$\begin{aligned} L_i &= R_{i-1}, \ \ i = 1, \ 2, \ ..., \ 16; \\ R_i &= L_{i-1} \oplus f\left(R_{i-1}, K_i\right), \ \ i = 1, \ 2, \ ..., \ 16. \end{aligned} \tag{3}$$

Функция $f$ называется функцией шифрования. Ее аргументами являются последовательность $R_{i\text{-}1}$, получаемая на предыдущем шаге итерации, и 48-битовый ключ $K_i$, который является результатом преобразования 64-битового ключа шифра $K$.

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 обратной перестановки $IP^{-1}$. Полученные биты $R_{16}L_{16}$ переставляются в соответствии с матрицей $IP^{-1}$.

Процесс расшифрования данных является инверсным по отношению к процессу шифрования. Все действия должны быть выполнены в обратном порядке. Это означает, что расшифровываемые данные сначала переставляются в соответствии с матрицей $IP^{-1}$, а затем над последовательностью битов $R_{16}L_{16}$ выполняются те же действия, что и в процессе шифрования, но в обратном порядке.

Итеративный процесс расшифрования может быть описан следующими формулами:

$$\begin{aligned} R_{i-1} &= L_i, \ \ i = 1, \ 2, \ ..., \ 16; \\ L_{i-1} &= R_i \oplus f\left(L_i, K_i\right), \ \ i = 1, \ 2, \ ..., \ 16. \end{aligned} \tag{4}$$

Таким образом, для процесса расшифрования с переставленным входным блоком $R_{16}L_{16}$ на первой итерации используется ключ $K_{16}$, на второй итерации – $K_{15}$ и т. д. На 16-й итерации используется ключ $K_1$. На последнем шаге итерации будут получены последовательности $L_o$ и $R_o$, которые конкатенируются в 64-битовую последовательность $L_oR_o$. Затем в этой последовательности 64 бита переставляются в соответствии с матрицей IP.

Для вычисления значения функции шифрования $f$ используются функции расширения $E$, преобразования $S$ и перестановки $P$. Причем выбор элемента в матрице $S$ осуществляется следующим образом. 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.

Ключ $K$ представляет собой 64-битовый блок с 8 битами контроля по четности, расположенными в позициях 8, 16, 24, 32, 40, 48, 56, 64. Для удаления контрольных битов и подготовки ключа к работе используется функция первоначальной подготовки ключа $G$. Результат преобразования $G(K)$ разбивается на две половины $C_0$ и $D_0$ по 28 бит каждая. Первые четыре строки матрицы $G$ определяют, как выбираются биты последовательности $C_0$. Следующие четыре строки матрицы $G$ определяют, как выбираются биты последовательности $D_0$. Для генерации последовательностей $C_0$ и $D_0$ не используются биты 8, 16, 24, 32, 40, 48, 56 и 64 ключа шифра. Эти биты не влияют на шифрование и могут служить для других целей, например, для контроля по четности. Таким образом, в действительности ключ шифра является 56-битовым.

После определения $C_0$ и $D_0$ рекурсивно определяются $C_i$ и $D_i$ ($i$ = 1, 2, …, 16). Для этого применяются операции циклического сдвига влево на один или два бита в зависимости от номера шага итерации. Причем операции сдвига выполняются для последовательностей $C_i$ и $D_i$ независимо.

Ключ $K_i$, определяемый на каждом шаге итерации, есть результат выбора конкретных битов из 56-битовой последовательности $C_iD_i$ и их перестановки:

$$K_i = H(C_i D_i), \tag{5}$$

где функция $H$ определяется матрицей, завершающей обработку ключа.

Алгоритм DES используется как для шифрования, так и для аутентификации данных и позволяет непосредственно преобразовывать 64-битовый входной открытый текст в 64-битовый выходной шифрованный текст, однако данные редко ограничиваются 64 разрядами. В целях использования алгоритма DES для решения разнообразных криптографических задач разработаны четыре рабочих режима: электронной кодовой книги (Electronic Code Book, ECB), или режим прямого шифрования, сцепления блоков шифра (Cipher Block Chaining, CBC), обратной связи по шифртексту (Cipher Feed Back, CFB) и обратной связи по выходу (Output Feed Back, OFB).

В режиме обратной связи по шифртексту CFB размер блока может отличаться от 64 бит. Файл, подлежащий шифрованию (расшифрованию), считывается последовательными блоками $M_i$ длиной $k$ битов ($k$ = 1, 2, ..., 64). Входной блок (64-битовый регистр сдвига) вначале содержит вектор инициализации IV, выровненный по правому краю. Процесс зашифрования в режиме CFB может быть описан выражением

$$C_i = M_i \oplus P_{i-1}, \tag{6}$$

где $P_{i-1}$ – $k$ старших битов предыдущего зашифрованного блока.

Обновление сдвигового регистра осуществляется путем удаления его старших $k$ битов и записи $C_i$ в регистр. Восстановление зашифрованных данных выполняется аналогичным образом:

$$M_i = C_i \oplus P_{i-1}. \tag{7}$$

### 1.2 Практическое задание

1.2.1 Включите персональный компьютер.

1.2.2 Запустите файл «lr1_Data_Encryption_Standard.exe» на выполнение.

1.2.3 Выполните предлагаемые задания в соответствии с индивидуальным вариантом, который определяется преподавателем дисциплины.

Выполнение заданий заключается в последовательной реализации алгоритма DES, заполнении и анализе таблицы с полученными результатами. Условие заданий является общим для всех вариантов, а конкретные исходные данные по каждому варианту представлены в соответствующих таблицах.

1.2.4 По результатам выполнения заданий заполните таблицу 1.

Задание считается выполненным, если все предлагаемые задания завершены успешно. При неправильном варианте ответа на экран выводится сообщение об ошибке. В этом случае необходимо повторно выбрать и записать вариант ответа в соответствии с предлагаемой инструкцией.

1.2.5 Продемонстрируйте выполнение практического задания преподавателю дисциплины.

Таблица 1 – Результаты выполнения индивидуального задания

| Параметр | Значение | |
|---|---|---|
| | в десятичной форме записи | в шестнадцатеричной форме записи |
| Исследование работы алгоритма DES в режиме зашифрования | | |
| $IP_{вых}$ | | |
| $L_o$ | | |
| $R_o$ | | |
| Исследование схемы генерации ключей $K_i$ | | |
| $C_0$ | | |
| $D_0$ | | |
| $C_1$ | | |
| $D_1$ | | |
| $K_1$ | | |
| Исследование функции шифрования | | |
| $E_{вых}$ | | |
| $S_{вх}$ | | |
| $S_{вых}$ | | |
| $P_{вых}$ | | |

| Параметр | Значение | |
|---|---|---|
| | в десятичной форме записи | в шестнадцатеричной форме записи |
| Исследование работы обобщенного алгоритма DES | | |
| $L_1$ | | |
| $R_1$ | | |
| $L_{16}$ | | |
| $R_{16}$ | | |
| $IP^{-1}_{вх}$ | | |
| $C$ | | |
| Исследование DES в режиме обратной связи по шифртексту | | |
| $C_1$ | | |
| $C_2$ | | |
| $T_1$ | | |
| $T_2$ | | |
| Исследование комбинированного алгоритма DES в режиме зашифрования | | |
| $C$ | | |
| Исследование комбинированного алгоритма DES в режиме расшифрования | | |
| $C$ | | |
| $P$ | | |

### 1.3 Содержание отчета

1 Цель лабораторной работы.

2 Структурная схема криптосистемы на базе стандарта DES.

3 Матрица $H$, завершающая обработку ключа.

4 Таблицы с исходными данными, соответствующими индивидуальному варианту задания.

5 Таблица с результатами выполнения задания.

6 Выводы по результатам выполнения задания.

7 Ответы на контрольные вопросы.

### 1.4 Контрольные вопросы

1 Каким образом реализуется алгоритм шифрования данных DES?

2 Каким образом реализуется алгоритм расшифрования данных DES?

3 Какую длину имеет ключ шифрования данных DES?

4 Какие режимы работы определены для алгоритма DES?

5 Какое практическое применение находит алгоритм DES?

# ЛАБОРАТОРНАЯ РАБОТА №2
# СТАНДАРТ ШИФРОВАНИЯ ДАННЫХ
# ГОСТ 28147-89 В РЕЖИМЕ ПРОСТОЙ ЗАМЕНЫ

**Цель:** изучение алгоритмов шифрования и расшифрования данных ГОСТ 28147-89 в режиме простой замены.

## 2.1 Краткие теоретические сведения

Алгоритм криптографического преобразования данных ГОСТ 28147-89 предназначен для аппаратной и программной реализации, удовлетворяет криптографическим требованиям и не накладывает ограничений на степень секретности защищаемой информации. Этот алгоритм представляет собой 64-битовый блочный алгоритм с 256-битовым ключом, при описании которого используются следующие обозначения:

1) $L$ и $R$ – последовательности битов;

2) $LR$ – конкатенация последовательностей $L$ и $R$, в которой биты последовательности $R$ следуют за битами последовательности $L$;

3) $\oplus$ – операция побитового сложения по модулю 2;

4) $\boxplus$ – операция сложения по модулю $2^{32}$ двух 32-разрядных двоичных чисел;

5) $\boxplus'$ – операция сложения двух 32-разрядных чисел по модулю $(2^{32} – 1)$.

Стандарт шифрования и расшифрования данных ГОСТ 28147-89 предусматривает четыре режима работы: простой замены, гаммирования, гаммирования с обратной связью и выработки имитовставки.

Алгоритм криптографического преобразования данных ГОСТ 28147-89 в режиме простой замены поясняется структурной схемой, приведенной в программной реализации алгоритма, где также приводятся все таблицы алгоритма.

Открытые данные, подлежащие шифрованию, разбивают на 64-разрядные блоки $T_o$. Процедура зашифрования 64-разрядного блока $T_o$ в режиме простой замены включает 32 цикла ($j$ = 1, 2, ..., 32). В ключевое запоминающее устройство (КЗУ) вводят 256 бит ключа $K$ в виде восьми 32-разрядных подключей $K_j$: $K = K_7\, K_6\, K_5\, K_4\, K_3\, K_2\, K_1\, K_0$. Последовательность битов блока

$$T_o = \left(a_1(0),\ a_2(0),\ ..., a_{31}(0),\ a_{32}(0),\ b_1(0),\ b_2(0),\ ...,\ b_{31}(0),\ b_{32}(0)\right) \quad (8)$$

разбивают на две последовательности по 32 бита: $b(0)$ $a(0)$, где $b(0)$ – старшие биты, $a(0)$ – младшие биты. Эти последовательности вводят в накопители $N_1$ и $N_2$ перед началом первого цикла шифрования.

Первый цикл процедуры шифрования 64-разрядного блока открытых данных можно описать системой

$$\begin{cases} a(1) = f\left(a(0) \boxplus K_0\right) \oplus b(0), \\ b(1) = a(0), \end{cases} \quad (9)$$

где $a(1)$ и $b(1)$ – заполнения накопителей $N_1$ и $N_2$ соответственно после первого цикла шифрования;

$f$ – функция шифрования.

Аргументом функции $f$ является сумма по модулю $2^{32}$ числа $a(0)$ – начального заполнения накопителя $N_1$ – и числа $K_0$ – подключа, считываемого из накопителя $X_0$ КЗУ.

Функция $f$ включает две операции над полученной 32-разрядной суммой $a(0) \boxplus K_0$. Первая операция – подстановка (замена), которая выполняется блоком подстановки $S$. Этот блок состоит из восьми узлов замены $S_1$ … $S_8$. Поступающий из сумматора $СМ_1$ на блок подстановки $S$ 32-разрядный вектор разбивают на восемь последовательно идущих 4-разрядных векторов, каждый

из которых преобразуется в 4-разрядный вектор соответствующим узлом замены. Каждый узел замены можно представить в виде таблицы-перестановки шестнадцати 4-разрядных двоичных чисел в диапазоне 0000…1111. Входной вектор указывает адрес строки в таблице, а число в этой строке является выходным вектором. Затем 4-разрядные выходные векторы последовательно объединяют в 32-разрядный вектор. Узлы замены с соответствующими таблицами-перестановками представляют собой ключевые элементы, которые являются общими для сети передачи данных и редко изменяются. Вторая операция – циклический сдвиг влево на 11 разрядов 32-разрядного вектора, полученного с выхода блока подстановки *S*. Циклический сдвиг выполняется регистром сдвига *R*.

Далее результат работы функции шифрования $f$ суммируют поразрядно по модулю 2 в сумматоре $СМ_2$ с 32-разрядным начальным заполнением $b(0)$ накопителя $N_2$. Затем полученный на выходе $СМ_2$ результат – значение $a(1)$ – записывают в накопитель $N_1$, а старое значение $N_1$ – значение $a(0)$ – переписывают в накопитель $N_2$. Первый цикл на этом завершается. Последующие циклы осуществляются аналогично. При этом во втором цикле из КЗУ считывают заполнение $X_1$ – подключ $K_1$, в третьем цикле – подключ $K_2$ и т. д., в восьмом цикле – подключ $K_7$. В циклах с 9-го по 16-й, а также в циклах с 17-го по 24-й подключи из КЗУ считываются в том же порядке: $K_0$, $K_1$, …, $K_7$. В последних восьми циклах с 25-го по 32-й порядок считывания подключей из КЗУ обратный: $K_7$, $K_6$, …, $K_1$, $K_0$. Таким образом, при шифровании в 32 циклах осуществляется следующий порядок выборки из КЗУ подключей: $K_0$, $K_1$, $K_2$, $K_3$, $K_4$, $K_5$, $K_6$, $K_7$, $K_0$, $K_1$, $K_2$, $K_3$, $K_4$, $K_5$, $K_6$, $K_7$, $K_0$, $K_1$, $K_2$, $K_3$, $K_4$, $K_5$, $K_6$, $K_7$, $K_7$, $K_6$, $K_5$, $K_4$, $K_3$, $K_2$, $K_1$, $K_0$. В 32-м цикле результат из сумматора $СМ_2$ вводится в накопитель $N_2$, а в накопителе $N_1$ сохраняется прежнее заполнение. Полученные после 32-го цикла шифрования заполнения накопителей $N_1$ и $N_2$ являются блоком зашифрованных данных $T_ш$, соответствующим блоку открытых данных $T_o$.

Таким образом, процедуру шифрования 64-разрядного блока открытых данных можно описать системами:

$$\begin{cases} a(j) = f\left(a(j-1) \boxplus K_{j-1(\mathrm{mod}\,8)}\right) \oplus b(j-1) \\ b(j) = a(j-1) \end{cases} \text{при } j = 1 \ldots 24;$$

$$\begin{cases} a(j) = f\left(a(j-1) \boxplus K_{32-j}\right) \oplus b(j-1) \\ b(j) = a(j-1) \end{cases} \text{при } j = 25 \ldots 31; \qquad (10)$$

$$\begin{cases} a(32) = a(31) \\ b(32) = f\left(a(31) \boxplus K_0\right) \oplus b(31) \end{cases} \text{при } j = 32,$$

где $a(j) = (a_{32}(j), a_{31}(j), \ldots, a_1(j))$ – заполнение $N_1$ после $j$-го цикла шифрования;

$b(j) = (b_{32}(j), b_{31}(j), \ldots, b_1(j))$ – заполнение $N_2$ после $j$-го цикла шифрования, $j = 1 \ldots 32$.

Блок зашифрованных данных $T_ш$ выводится из накопителей $N_1$, $N_2$ в следующем порядке: из разрядов 1 … 32 накопителя $N_1$, затем из разрядов 1 … 32 накопителя $N_2$, т. е. начиная с младших разрядов. Остальные блоки открытых данных зашифровываются в режиме простой замены аналогично.

Криптосхема, реализующая алгоритм расшифрования в режиме простой замены, имеет тот же вид, что и при шифровании. В КЗУ вводят 256 бит ключа, на котором осуществлялось шифрование. Зашифрованные данные, подлежащие расшифрованию, разбиты на блоки $T_ш$ по 64 бита в каждом, которые вводят в накопители $N_1$ и $N_2$. Расшифрование осуществляется по тому же алгоритму, что и шифрование, с тем изменением, что заполнения накопителей $X_0$, $X_1$, …, $X_7$ считываются из КЗУ в циклах расшифрования в следующем порядке: $K_0$, $K_1$, $K_2$, $K_3$, $K_4$, $K_5$, $K_6$, $K_7$, $K_7$, $K_6$, $K_5$, $K_4$, $K_3$, $K_2$, $K_1$, $K_0$, $K_7$, $K_6$, $K_5$, $K_4$, $K_3$, $K_2$, $K_1$, $K_0$, $K_7$, $K_6$, $K_5$, $K_4$, $K_3$, $K_2$, $K_1$, $K_0$.

Таким образом, процедуру расшифрования 64-разрядного блока $T_ш$ можно описать следующими системами:

$$
\begin{cases} a(32-j) = f\left(a(32-j+1) \boxplus K_{j-1}\right) \oplus b(32-j+1) \\ b(32-j) = a(32-j+1) \end{cases} \text{при } j = 1 \ldots 8;
$$

$$
\begin{cases} a(32-j) = f\left(a(32-j+1) \boxplus K_{32-j(\bmod 8)}\right) \oplus b(32-j+1) \\ b(32-j) = a(32-j+1) \end{cases} \text{при } j = 9 \ldots 31; \quad (11)
$$

$$
\begin{cases} a(0) = a(1) \\ b(0) = f\left(a(1) \boxplus K_0\right) \oplus b(1) \end{cases} \text{при } j = 32.
$$

Полученные после 32 циклов работы заполнения накопителей $N_1$ и $N_2$ образуют блок открытых данных $T_o$, соответствующий блоку зашифрованных данных $T_ш$. Аналогично расшифровываются остальные блоки зашифрованных данных.

Если алгоритм зашифрования в режиме простой замены 64-битового блока $T_o$ обозначить через $A$, то

$$
A(T_o) = A\big(a(0),\ b(0)\big) = \big(a(32),\ b(32)\big) = T_ш. \quad (12)
$$

Следует отметить, что режим простой замены допустимо использовать для шифрования данных только в ограниченных случаях: при выработке ключа и зашифровании его с обеспечением имитозащиты для передачи по каналам связи или для хранения в памяти компьютера.

### 2.2 Практическое задание

2.2.1 Включите персональный компьютер.

2.2.2 Запустите файл «lr2_GOST_28147-89_RPZ» на выполнение.

2.2.3 В появившемся окне установите количество циклов шифрования и расшифрования, равное 4.

2.2.4 Выполните предлагаемые задания в соответствии с индивидуальным вариантом, который определяется преподавателем дисциплины.

Выполнение заданий заключается в последовательной реализации алгоритма ГОСТ 28147-89 в режиме простой замены, заполнении и анализе таблиц с полученными результатами. Условие заданий является общим для всех вариантов, а конкретные исходные данные по каждому варианту представлены в соответствующих таблицах.

2.2.5 По результатам выполнения заданий заполните таблицы 2 и 3.

Задание считается выполненным, если все предлагаемые задания завершены успешно. При неправильном варианте ответа на экран выводится сообщение об ошибке. В этом случае необходимо повторно выбрать и записать вариант ответа в соответствии с предлагаемой инструкцией.

2.2.6 Продемонстрируйте выполнение практического задания преподавателю дисциплины.

Таблица 2 – Результаты исследования работы схемы реализации режима простой замены при шифровании блока $T_o$

| Параметр | Значение | |
|---|---|---|
| | в десятичной форме записи | в шестнадцатеричной форме записи |
| Исследование работы схемы при реализации первого цикла шифрования | | |
| $СМ1_{вых}$ | | |
| $S_{вых}$ | | |
| $R_{вых}$ | | |
| $СМ2_{вых}$ | | |
| $N_2$ | | |
| $N_1$ | | |
| Исследование работы схемы при реализации второго цикла шифрования | | |
| $СМ1_{вых}$ | | |
| $S_{вых}$ | | |
| $R_{вых}$ | | |
| $СМ2_{вых}$ | | |
| $N_2$ | | |
| $N_1$ | | |

| Параметр | Значение | |
|---|---|---|
| | в десятичной форме записи | в шестнадцатеричной форме записи |
| Исследование работы схемы при реализации третьего цикла шифрования | | |
| $R_{вых}$ | | |
| $СМ2_{вых}$ | | |
| $N_2$ | | |
| $N_1$ | | |
| Исследование работы схемы при реализации четвертого цикла шифрования | | |
| $СМ1_{вых}$ | | |
| $S_{вых}$ | | |
| $R_{вых}$ | | |
| $СМ2_{вых}$ | | |
| $N_2$ | | |
| $N_1$ | | |

Таблица 3 – Результаты исследования работы схемы реализации режима простой замены при расшифровании блока $T_ш$

| Параметр | Значение | |
|---|---|---|
| | в десятичной форме записи | в шестнадцатеричной форме записи |
| Исследование работы схемы при реализации первого цикла расшифрования | | |
| $СМ1_{вых}$ | | |
| $S_{вых}$ | | |
| $R_{вых}$ | | |
| $СМ2_{вых}$ | | |
| $N_2$ | | |
| $N_1$ | | |
| Исследование работы схемы при реализации второго цикла расшифрования | | |
| $СМ1_{вых}$ | | |
| $S_{вых}$ | | |
| $R_{вых}$ | | |
| $СМ2_{вых}$ | | |
| $N_2$ | | |
| $N_1$ | | |
| Исследование работы схемы при реализации третьего цикла расшифрования | | |
| $СМ1_{вых}$ | | |
| $S_{вых}$ | | |
| $R_{вых}$ | | |
| $СМ2_{вых}$ | | |
| $N_2$ | | |
| $N_1$ | | |
| Исследование работы схемы при реализации четвертого цикла расшифрования | | |
| $СМ1_{вых}$ | | |
| $S_{вых}$ | | |
| $R_{вых}$ | | |
| $СМ2_{вых}$ | | |
| $N_2$ | | |
| $N_1$ | | |

### 2.3 Содержание отчета

1 Цель лабораторной работы.

2 Структурная схема криптосистемы на базе ГОСТ 28147-89 в режиме простой замены.

3 Уравнения шифрования и расшифрования данных алгоритма ГОСТ 28147-89 в режиме простой замены.

4 Таблицы с исходными данными, соответствующими индивидуальному варианту задания.

5 Таблицы с результатами выполнения задания.

6 Выводы по результатам выполнения задания.

7 Ответы на контрольные вопросы.

### 2.4 Контрольные вопросы

1 Каким образом реализуется алгоритм ГОСТ 28147-89 в режиме простой замены при шифровании данных?

2 Каким образом реализуется алгоритм ГОСТ 28147-89 в режиме простой замены при расшифровании шифртекста?

3 Какую длину имеет ключ шифрования данных ГОСТ 28147-89 в режиме простой замены?

4 Какие режимы работы определены для алгоритма ГОСТ 28147-89?

5 Какое практическое применение находит алгоритм ГОСТ 28147-89 в режиме простой замены?

# ЛАБОРАТОРНАЯ РАБОТА №3
# СТАНДАРТ ШИФРОВАНИЯ ДАННЫХ ГОСТ 28147-89
# В РЕЖИМЕ ГАММИРОВАНИЯ С ОБРАТНОЙ СВЯЗЬЮ

**Цель:** изучение алгоритмов шифрования и расшифрования данных ГОСТ 28147-89 в режиме гаммирования с обратной связью.

## 3.1 Краткие теоретические сведения

Алгоритм криптографического преобразования данных ГОСТ 28147-89 в режиме гаммирования с обратной связью поясняется структурной схемой, приведенной в программной реализации алгоритма, где также приводятся все таблицы алгоритма.

Открытые данные, разбитые на 64-разрядные блоки $T_o^{(1)}$, $T_o^{(2)}$, …, $T_o^{(m)}$, зашифровываются в режиме гаммирования с обратной связью путем поразрядного сложения по модулю 2 с гаммой шифра $\Gamma_ш$, которая вырабатывается блоками по 64 бита $\Gamma_ш^{(1)}$, $\Gamma_ш^{(2)}$, …, $\Gamma_ш^{(m)}$. Число двоичных разрядов в блоке $T_o^{(m)}$ может быть меньше 64; при этом неиспользованная для шифрования часть гаммы шифра из блока $\Gamma_ш^{(m)}$ отбрасывается.

Уравнения шифрования в режиме гаммирования с обратной связью имеют вид

$$\begin{aligned} T_ш^{(1)} &= T_o^{(1)} \oplus A\left(\tilde{S}\right) = T_o^{(1)} \oplus \Gamma_ш^{(1)}, \\ T_ш^{(i)} &= T_o^{(i)} \oplus A\left(T_ш^{(i-1)}\right) = T_o^{(i)} \oplus \Gamma_ш^{(i)}, \quad i = 2 \ldots m, \end{aligned} \tag{13}$$

где $T_ш^{(i)}$ – $i$-й 64-разрядный блок зашифрованного текста;

$A()$ – функция шифрования в режиме простой замены;

$m$ – количество 64-битовых блоков открытых данных.

Аргументом функции $A()$ на первом шаге итеративного алгоритма является 64-разрядная синхропосылка $\tilde{S}$, а на всех последующих шагах – предыду-

щий блок зашифрованных данных $T_ш^{(i-1)}$. Процедура шифрования данных в режиме гаммирования с обратной связью реализуется следующим образом. В КЗУ вводятся 256 бит ключа. В накопители $N_1$ и $N_2$ вводится синхропосылка $\tilde{S}$ из 64 бит. Исходное заполнение накопителей $N_1$ и $N_2$ зашифровывается в режиме простой замены (рассмотрено в рамках лабораторной работы №2). Полученное в результате шифрования заполнение накопителей $N_1$ и $N_2$ образует первый 64-разрядный блок гаммы шифра $Г_ш^{(1)}=A(\tilde{S})$, который суммируется поразрядно по модулю 2 в сумматоре $СМ_5$ с первым 64-разрядным блоком открытых данных. В результате получают первый 64-разрядный блок зашифрованных данных:

$$T_ш^{(1)} = T_o^{(1)} \oplus Г_ш^{(1)}, \qquad (14)$$

где $T_ш^{(1)} = \left(\tau_1^{(1)},\ \tau_2^{(1)},\ ...,\ \tau_{63}^{(1)},\ \tau_{64}^{(1)}\right)$.

Блок зашифрованных данных $T_ш^{(1)}$ одновременно является также исходным состоянием накопителей $N_1$ и $N_2$ для выработки второго блока гаммы шифра $Г_ш^{(2)}$, поэтому по обратной связи $T_ш^{(1)}$ записывается в указанные накопители $N_1$ и $N_2$. Заполнение накопителей $N_1$ и $N_2$ зашифровывается в режиме простой замены. Полученное в результате шифрования заполнение накопителей $N_1$ и $N_2$ образует второй 64-разрядный блок гаммы шифра $Г_ш^{(2)}$, который суммируется поразрядно по модулю 2 в сумматоре $СМ_5$ со вторым блоком открытых данных $T_o^{(2)}$:

$$T_ш^{(2)} = T_o^{(2)} \oplus Г_ш^{(2)}. \qquad (15)$$

Выработка последующих блоков гаммы шифра $Г_ш^{(i)}$ и шифрование соответствующих блоков открытых данных $T_o^{(i)}$ производится аналогично.

Как отмечалось ранее, если длина последнего $m$-го блока открытых данных $T_o^{(m)}$ меньше 64 разрядов, то из $Г_ш^{(m)}$ используется только соответствующее число разрядов гаммы шифра, а остальные разряды отбрасываются.

При расшифровании в режиме гаммирования с обратной связью криптосхема имеет тот же вид, что и при шифровании. В канал связи или память компьютера передаются синхропосылка $\tilde{S}$ и блоки зашифрованных данных $T_ш^{(1)}$, $T_ш^{(2)}$, ..., $T_ш^{(m)}$. Уравнения расшифрования имеют вид

$$\begin{aligned} T_o^{(1)} &= T_ш^{(1)} \oplus A\left(\tilde{S}\right) = T_ш^{(1)} \oplus \Gamma_ш^{(1)}, \\ T_o^{(i)} &= T_ш^{(i)} \oplus \Gamma_ш^{(i)} = T_ш^{(i)} \oplus A\left(T_ш^{(i-1)}\right), \quad i = 2 \ldots m. \end{aligned} \tag{16}$$

Реализация процедуры расшифрования зашифрованных данных в режиме гаммирования с обратной связью происходит следующим образом. В КЗУ вводят 256 бит того же ключа, на котором осуществлялось шифрование открытых блоков $T_o^{(1)}$, $T_o^{(2)}$, ..., $T_o^{(m)}$. В накопители $N_1$ и $N_2$ вводится синхропосылка $\tilde{S}$. Исходное заполнение накопителей $N_1$ и $N_2$ (синхропосылка $\tilde{S}$) зашифровывается в режиме простой замены. Полученное в результате шифрования заполнение $N_1$ и $N_2$ образует первый блок гаммы шифра:

$$\Gamma_ш^{(1)} = A\left(\tilde{S}\right), \tag{17}$$

который суммируется поразрядно по модулю 2 в сумматоре $СМ_5$ с блоком зашифрованных данных $T_ш^{(1)}$.

В результате получается первый блок открытых данных:

$$T_o^{(1)} = T_ш^{(1)} \oplus \Gamma_ш^{(1)}. \tag{18}$$

Блок зашифрованных данных $T_ш^{(1)}$ является исходным заполнением накопителей $N_1$ и $N_2$ для выработки второго блока гаммы шифра:

$$\Gamma_ш^{(2)} = A\left(T_ш^{(1)}\right). \tag{19}$$

Полученное заполнение накопителей $N_1$ и $N_2$ зашифровывается в режиме простой замены (см. лабораторную работу 2). Образованный в результате шифрования блок $Г_ш^{(2)}$ суммируется поразрядно по модулю 2 в сумматоре $СМ_5$ со вторым блоком зашифрованных данных $T_ш^{(2)}$. В результате получают второй блок открытых данных. Аналогично в $N_1$ и $N_2$ последовательно записывают блоки зашифрованных данных $T_ш^{(2)}$, $T_ш^{(3)}$, …, $T_ш^{(m)}$, из которых в режиме простой замены вырабатываются блоки гаммы шифра $Г_ш^{(3)}$, $Г_ш^{(4)}$, …, $Г_ш^{(m)}$.

Блоки гаммы шифра суммируются поразрядно по модулю 2 в сумматоре $СМ_5$ с блоками зашифрованных данных $T_ш^{(3)}$, $T_ш^{(4)}$, …, $T_ш^{(m)}$. В результате получают блоки открытых данных $T_o^{(3)}$, $T_o^{(4)}$, ..., $T_o^{(m)}$. При этом последний блок открытых данных $T_o^{(m)}$ может содержать меньше 64 разрядов, как отмечалось ранее.

### 3.2 Практическое задание

3.2.1 Включите персональный компьютер.

3.2.2 Запустите файл «lr3_GOST_28147-89_RGsOS.exe» на выполнение.

3.2.3 В появившемся окне установите количество циклов шифрования и расшифрования, равное 4.

3.2.4 Выполните предлагаемые задания в соответствии с индивидуальным вариантом, который определяется преподавателем дисциплины.

Выполнение заданий заключается в последовательной реализации алгоритма ГОСТ 28147-89 в режиме гаммирования с обратной связью, заполнении и анализе таблиц с полученными результатами. Условие заданий является общим для всех вариантов, а конкретные исходные данные по каждому варианту представлены в соответствующих таблицах.

3.2.5 По результатам выполнения заданий заполните таблицы 4 и 5.

Задание считается выполненным, если все предлагаемые задания завершены успешно. При неправильном варианте ответа на экран выводится сооб-

щение об ошибке. В этом случае необходимо повторно выбрать и записать вариант ответа в соответствии с предлагаемой инструкцией.

3.2.6 Продемонстрируйте выполнение практического задания преподавателю дисциплины.

Таблица 4 – Результаты исследования работы схемы реализации режима гаммирования с обратной связью при шифровании блоков $T_o$

| Параметр | Значение | |
|---|---|---|
| | в десятичной форме записи | в шестнадцатеричной форме записи |
| Исследование работы схемы при шифровании первого блока данных $T_o^{(1)}$ | | |
| $N_{2вх}$ | | |
| $N_{1вх}$ | | |
| $N_{2вых}$ | | |
| $N_{1вых}$ | | |
| $Г_ш^{(1)}$ | | |
| $T_ш^{(1)}$ | | |
| Исследование работы схемы при шифровании второго блока данных $T_o^{(2)}$ | | |
| $N_{2вх}$ | | |
| $N_{1вх}$ | | |
| $N_{2вых}$ | | |
| $N_{1вых}$ | | |
| $Г_ш^{(2)}$ | | |
| $T_ш^{(2)}$ | | |
| Исследование работы схемы при шифровании третьего блока данных $T_o^{(3)}$ | | |
| $N_{2вх}$ | | |
| $N_{1вх}$ | | |
| $N_{2вых}$ | | |
| $N_{1вых}$ | | |
| $Г_ш^{(3)}$ | | |
| $T_ш^{(3)}$ | | |
| Исследование работы схемы при шифровании четвертого блока данных $T_o^{(4)}$ | | |
| $N_{2вх}$ | | |
| $N_{1вх}$ | | |
| $N_{2вых}$ | | |
| $N_{1вых}$ | | |
| $Г_ш^{(4)}$ | | |
| $T_ш^{(4)}$ | | |

Таблица 5 – Результаты исследования работы схемы реализации режима гаммирования с обратной связью при расшифровании блоков $T_ш$

| Параметр | Значение | |
|---|---|---|
| | в десятичной форме записи | в шестнадцатеричной форме записи |
| Исследование работы схемы при расшифровании первого блока шифртекста $T_ш^{(1)}$ | | |
| $N_{2вх}$ | | |
| $N_{1вх}$ | | |
| $N_{2вых}$ | | |
| $N_{1вых}$ | | |
| $Г_ш^{(1)}$ | | |
| $T_o^{(1)}$ | | |
| Исследование работы схемы при расшифровании второго блока шифртекста $T_ш^{(2)}$ | | |
| $N_{2вх}$ | | |
| $N_{1вх}$ | | |
| $N_{2вых}$ | | |
| $N_{1вых}$ | | |
| $Г_ш^{(2)}$ | | |
| $T_o^{(2)}$ | | |
| Исследование работы схемы при расшифровании третьего блока шифртекста $T_ш^{(3)}$ | | |
| $N_{2вх}$ | | |
| $N_{1вх}$ | | |
| $N_{2вых}$ | | |
| $N_{1вых}$ | | |
| $Г_ш^{(3)}$ | | |
| $T_o^{(3)}$ | | |
| Исследование работы схемы при расшифровании четвертого блока шифртекста $T_ш^{(4)}$ | | |
| $N_{2вх}$ | | |
| $N_{1вх}$ | | |
| $N_{2вых}$ | | |
| $N_{1вых}$ | | |
| $Г_ш^{(4)}$ | | |
| $T_o^{(4)}$ | | |

### 3.3 Содержание отчета

1 Цель лабораторной работы.

2 Структурная схема криптосистемы на базе ГОСТ 28147-89, в режиме гаммирования с обратной связью.

3 Уравнения шифрования и расшифрования данных алгоритма криптографического преобразования данных, определяемого ГОСТ 28147-89, в режиме гаммирования с обратной связью.

4 Таблицы с исходными данными, соответствующими индивидуальному варианту задания.

5 Таблицы с результатами выполнения задания.

6 Выводы по результатам выполнения задания.

7 Ответы на контрольные вопросы.

### 3.4 Контрольные вопросы

1 Каким образом реализуется алгоритм шифрования данных ГОСТ 28147-89 в режиме гаммирования с обратной связью?

2 Каким образом реализуется алгоритм расшифрования данных ГОСТ 28147-89 в режиме гаммирования с обратной связью?

3 Какую длину имеет ключ шифрования данных ГОСТ 28147-89 в режиме гаммирования с обратной связью?

4 Какие режимы работы определены для алгоритма криптографического преобразования данных ГОСТ 28147-89?

5 Какое практическое применение находит алгоритм криптографического преобразования данных, определяемый ГОСТ 28147-89, в режиме гаммирования с обратной связью?

# ЛАБОРАТОРНАЯ РАБОТА №4
# СТАНДАРТ ШИФРОВАНИЯ ДАННЫХ
# ГОСТ 28147-89 В РЕЖИМЕ ГАММИРОВАНИЯ

**Цель:** изучение алгоритмов шифрования и расшифрования данных ГОСТ 28147-89 в режиме гаммирования.

## 4.1 Краткие теоретические сведения

Алгоритм ГОСТ 28147-89 в режиме гаммирования поясняется структурной схемой, приведенной на рисунке 1.

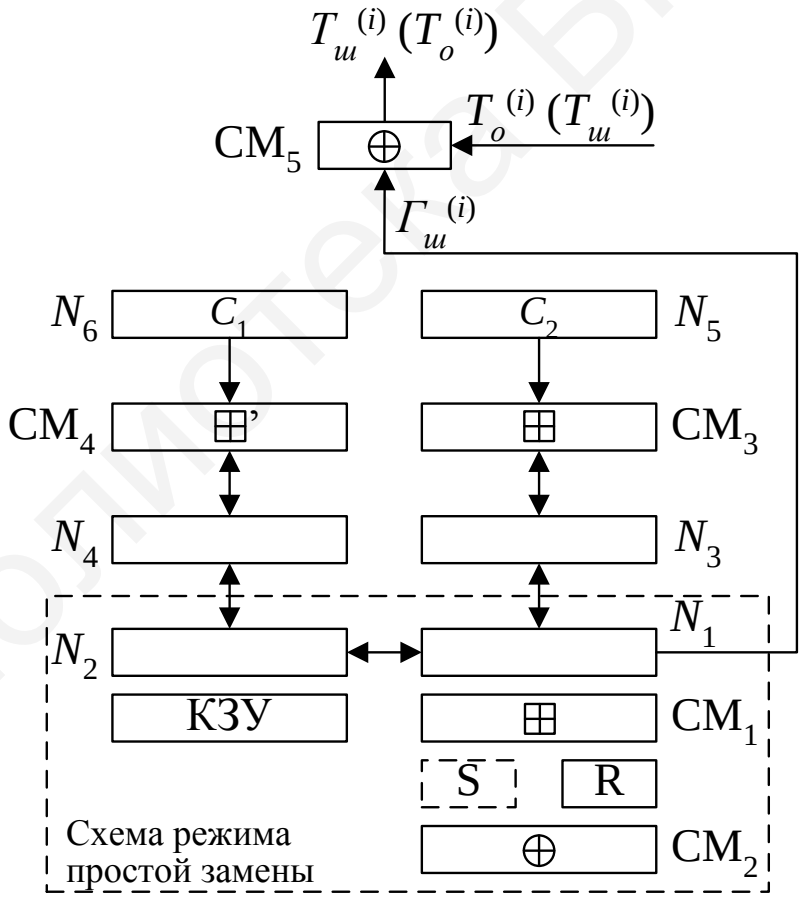



Рисунок 1 – Структурная схема реализации режима гаммирования

Открытые данные разбивают на 64-разрядные блоки $T_o^{(1)}$, $T_o^{(2)}$, …, $T_o^{(m)}$, где $T_o^{(i)}$ – $i$-й 64-разрядный блок открытых данных, $i = 1 \ldots m$ ($m$ определяется количеством информации, содержащейся в открытых данных). Эти блоки поочередно зашифровываются в режиме гаммирования путем поразрядного сложения по модулю 2 в сумматоре $СМ_5$ с гаммой шифра $Г_ш$, которая вырабатывается блоками по 64 бита $Г_ш^{(1)}$, $Г_ш^{(2)}$, …, $Г_ш^{(m)}$. Число двоичных разрядов в блоке $T_o^{(m)}$ может быть меньше 64, при этом неиспользованная для шифрования часть гаммы шифра из блока $Г_ш^{(m)}$ отбрасывается. Уравнения шифрования данных в режиме гаммирования имеют вид

$$\begin{aligned} T_ш^{(i)} &= T_o^{(i)} \oplus Г_ш^{(i)}, \\ Г_ш^{(i)} &= A\left(Y_{i-1} \boxplus C_2, Z_{i-1} \boxplus' C_1\right), \end{aligned} \tag{20}$$

где $T_ш^{(i)}$ – $i$-й 64-разрядный блок зашифрованного текста;

$A()$ – функция шифрования в режиме простой замены;

$C_1$ и $C_2$ – 32-разрядные двоичные константы;

$Y_i$ и $Z_i$ – 32-разрядные двоичные последовательности.

Величины $Y_i$ и $Z_i$ определяются итерационно по мере формирования гаммы $Г_ш$ следующим образом:

$$(Y_o, Z_o) = A(\tilde{S}), \tag{21}$$

где $\tilde{S}$ – 64-разрядная синхропосылка;

$$(Y_i, Z_i) = \left(Y_{i-1} \boxplus C_2, Z_{i-1} \boxplus' C_1\right), i = 1 \ldots m. \tag{22}$$

Рассмотрим реализацию процедуры шифрования в режиме гаммирования. В накопители $N_6$ и $N_5$ предварительно записывают 32-разрядные константы $C_1 = 01010104_{16}$ и $C_2 = 01010101_{16}$; в КЗУ вводится 256 бит ключа; в накопители $N_1$ и $N_2$ – 64-разрядная синхропосылка $\tilde{S}$. Исходное заполнение $N_1$ и $N_2$ (син-

хропосылка $\tilde{S}$) зашифровывается в режиме простой замены (рассмотрено в рамках лабораторной работы 2). Результат зашифрования (21) переписывается в 32-разрядные накопители $N_3$ и $N_4$ так, что заполнение $N_1$ переписывается в $N_3$, а заполнение $N_2$ – в $N_4$. Заполнение накопителя $N_4$ суммируют по модулю $(2^{32} – 1)$ в сумматоре $СМ_4$ с 32-разрядной константой $C_1$ из накопителя $N_6$. Результат записывается в $N_4$. Заполнение накопителя $N_3$ суммируется по модулю $2^{32}$ в сумматоре $СМ_3$ с 32-разрядной константой $C_2$ из накопителя $N_5$. Результат записывается в $N_3$. Заполнение $N_3$ переписывают в $N_1$, а заполнение $N_4$ – в $N_2$. При этом заполнения $N_3$ и $N_4$ сохраняются. Заполнение накопителей $N_1$ и $N_2$ зашифровывается в режиме простой замены. Полученное в результате зашифрования заполнение накопителей $N_1$ и $N_2$ образует первый 64-разрядный блок гаммы шифра $Г_ш^{(1)}$, который суммируют поразрядно по модулю 2 в сумматоре $СМ_5$ с первым 64-разрядным блоком открытых данных $T_o^{(1)}$. В результате суммирования по модулю 2 значений $Г_ш^{(1)}$ и $T_o^{(1)}$ получают первый 64-разрядный блок зашифрованнных данных:

$$T_ш^{(1)} = T_o^{(1)} \oplus Г_ш^{(1)} = \left(\tau_1^{(1)},\ \tau_2^{(1)},\ ...,\ \tau_{63}^{(1)},\ \tau_{64}^{(1)}\right), \qquad (23)$$

где

$$\tau_i^{(1)} = t_i^{(1)} \oplus \gamma_i^{(1)}, \quad i = 1 \ldots 64. \qquad (24)$$

Для получения следующего 64-разрядного блока гаммы шифра $Г_ш^{(2)}$ заполнение $N_4$ суммируется по модулю $(2^{32} – 1)$ в сумматоре $СМ_4$ с константой $C_1$ из $N_6$. Результат записывается в $N_4$. Заполнение $N_3$ суммируется по модулю $2^{32}$ в сумматоре $СМ_3$ с константой $C_2$ из $N_5$. Результат записывается в $N_3$. Новое заполнение $N_3$ переписывают в $N_1$, а новое заполнение $N_4$ – в $N_2$. При этом заполнения $N_3$ и $N_4$ сохраняют. Заполнение накопителей $N_1$ и $N_2$ зашифровывается в режиме простой замены. Полученное в результате шифрования заполнение накопителей $N_1$ и $N_2$ образует второй 64-разрядный блок гаммы шифра $Г_ш^{(2)}$, ко-

торый суммируется поразрядно по модулю 2 в сумматоре $СМ_5$ со вторым блоком открытых данных $T_o^{(2)}$:

$$T_ш^{(2)} = T_o^{(2)} \oplus Г_ш^{(2)}. \quad (25)$$

Аналогично вырабатываются блоки гаммы шифра $Г_ш^{(3)}$, $Г_ш^{(4)}$, …, $Г_ш^{(m)}$ и зашифровываются блоки открытых данных $T_o^{(3)}$, $T_o^{(4)}$, …, $T_o^{(m)}$.

В канал связи или память компьютера передаются синхропосылка $\tilde{S}$ и блоки зашифрованных данных $T_ш^{(1)}$, $T_ш^{(2)}$, …, $T_ш^{(m)}$. При расшифровании данных криптосхема имеет тот же вид, что и при зашифровании (см. рисунок 1). Уравнение расшифрования имеет вид

$$T_o^{(i)} = T_ш^{(i)} \oplus Г_ш^{(i)} = T_ш^{(i)} \oplus A\left(Y_{i-1} \boxplus C_2, Z_{i-1} \boxplus' C_1\right), i = 1...m. \quad (26)$$

Следует отметить, что расшифрование данных возможно только при наличии синхропосылки, которая не является секретным элементом шифра и может храниться в памяти компьютера или передаваться по каналам связи вместе с зашифрованными данными.

### 4.2 Практическое задание

4.2.1 Включите персональный компьютер.

4.2.2 Запустите файл «lr4_CryptoLab.exe» на выполнение.

4.2.3 Выполните предлагаемые задания в соответствии с индивидуальным вариантом, который определяется преподавателем дисциплины.

Выполнение заданий заключается в последовательной реализации алгоритма криптографического преобразования данных ГОСТ 28147-89 в режиме гаммирования, заполнении и анализе таблиц с полученными результатами.

Условие заданий является общим для всех вариантов, а конкретные исходные данные по каждому варианту представлены в соответствующих таблицах.

4.2.4 По результатам выполнения заданий заполните таблицы 6 и 7.

Задание считается выполненным, если все предлагаемые задания завершены успешно. При неправильном варианте ответа на экран выводится сообщение об ошибке. В этом случае необходимо повторно выбрать и записать вариант ответа в соответствии с предлагаемой инструкцией.

4.2.5 Продемонстрируйте выполнение практического задания преподавателю дисциплины.

Таблица 6 – Результаты исследования работы схемы реализации режима гаммирования при шифровании блоков $T_o$

| Параметр | Значение | |
|---|---|---|
| | в десятичной форме записи | в шестнадцатеричной форме записи |
| Исследование работы схемы при шифровании первого блока данных $T_o^{(1)}$ | | |
| $N_{3вх}$ | | |
| $N_{4вх}$ | | |
| $N_{3вых}$ | | |
| $N_{4вых}$ | | |
| $Г_ш^{(1)}$ | | |
| $T_ш^{(1)}$ | | |
| Исследование работы схемы при шифровании второго блока данных $T_o^{(2)}$ | | |
| $N_{3вх}$ | | |
| $N_{4вх}$ | | |
| $N_{3вых}$ | | |
| $N_{4вых}$ | | |
| $Г_ш^{(2)}$ | | |
| $T_ш^{(2)}$ | | |
| Исследование работы схемы при шифровании третьего блока данных $T_o^{(3)}$ | | |
| $N_{3вх}$ | | |
| $N_{4вх}$ | | |
| $N_{3вых}$ | | |
| $N_{4вых}$ | | |
| $Г_ш^{(3)}$ | | |
| $T_ш^{(3)}$ | | |
| Исследование работы схемы при шифровании четвертого блока данных $T_o^{(4)}$ | | |
| $N_{3вх}$ | | |
| $N_{4вх}$ | | |
| $N_{3вых}$ | | |
| $N_{4вых}$ | | |
| $Г_ш^{(4)}$ | | |
| $T_ш^{(4)}$ | | |

Таблица 7 – Результаты исследования работы схемы реализации режима гаммирования при расшифровании блоков $T_ш$

| Параметр | Значение | |
|---|---|---|
| | в десятичной форме записи | в шестнадцатеричной форме записи |
| Исследование работы схемы при расшифровании первого блока шифртекста $T_ш^{(1)}$ | | |
| $N_{3вх}$ | | |
| $N_{4вх}$ | | |
| $N_{3вых}$ | | |
| $N_{4вых}$ | | |
| $Г_ш^{(1)}$ | | |
| $T_o^{(1)}$ | | |
| Исследование работы схемы при расшифровании второго блока шифртекста $T_ш^{(2)}$ | | |
| $N_{3вх}$ | | |
| $N_{4вх}$ | | |
| $N_{3вых}$ | | |
| $N_{4вых}$ | | |
| $Г_ш^{(2)}$ | | |
| $T_o^{(2)}$ | | |
| Исследование работы схемы при расшифровании третьего блока шифртекста $T_ш^{(3)}$ | | |
| $N_{3вх}$ | | |
| $N_{4вх}$ | | |
| $N_{3вых}$ | | |
| $N_{4вых}$ | | |
| $Г_ш^{(3)}$ | | |
| $T_o^{(3)}$ | | |
| Исследование работы схемы при расшифровании четвертого блока шифртекста $T_ш^{(4)}$ | | |
| $N_{3вх}$ | | |
| $N_{4вх}$ | | |
| $N_{3вых}$ | | |
| $N_{4вых}$ | | |
| $Г_ш^{(4)}$ | | |
| $T_o^{(4)}$ | | |

### 4.3 Содержание отчета

1 Цель лабораторной работы.

2 Структурная схема криптосистемы на базе ГОСТ 28147-89, в режиме гаммирования.

3 Уравнения шифрования и расшифрования данных алгоритма криптографического преобразования данных, определяемого ГОСТ 28147-89, в режиме гаммирования.

4 Таблицы с исходными данными, соответствующими индивидуальному варианту задания.

5 Таблицы с результатами выполнения задания.

6 Выводы по результатам выполнения задания.

7 Ответы на контрольные вопросы.

### 4.4 Контрольные вопросы

1 Каким образом реализуется алгоритм шифрования данных ГОСТ 28147-89 в режиме гаммирования?

2 Каким образом реализуется алгоритм расшифрования данных ГОСТ 28147-89 в режиме гаммирования?

3 Какую длину имеет ключ шифрования данных ГОСТ 28147-89 в режиме гаммирования?

4 Какие режимы работы определены для алгоритма криптографического преобразования данных ГОСТ 28147-89?

5 Какое практическое применение находит алгоритм криптографического преобразования данных, определяемый ГОСТ 28147-89, в режиме гаммирования?

# ЛАБОРАТОРНАЯ РАБОТА №5
# АЛГОРИТМ ШИФРОВАНИЯ ДАННЫХ RSA

**Цель:** изучение схем шифрования данных и расшифрования шифртекстов, основанных на алгоритме RSA.

## 5.1 Краткие теоретические сведения

Для ознакомления с краткими теоретическими сведениями включите персональный компьютер и запустите файл «lr5_RSA.exe» на выполнение.

После запуска файла «lr5_RSA.exe» активизируется программное обеспечение, реализующее схемы шифрования данных и расшифрования шифртекстов на базе алгоритма RSA, и появится главное окно программы, показанное на рисунке 2.

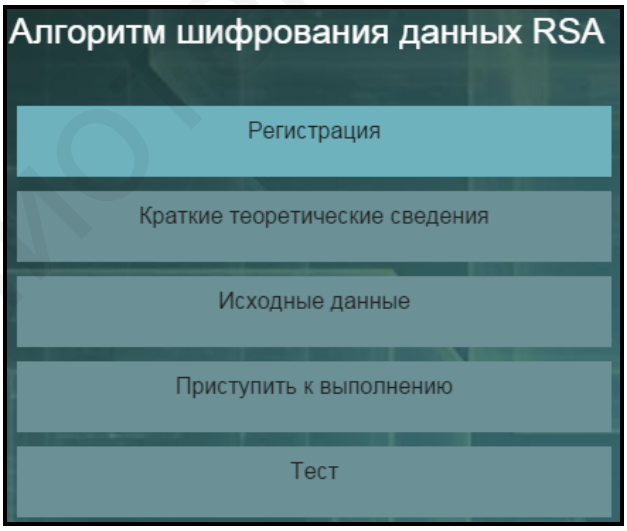



Рисунок 2 – Главное окно программы,
реализующей алгоритм шифрования данных RSA

До начала работы с программой необходимо зарегистрироваться. Для этого требуется в главном окне программы нажать кнопку «Регистрация» и в появившемся окне регистрации, приведенном на рисунке 3, ввести в поле «Фамилия и имя» свою фамилию и имя, указать номер группы в поле «Номер группы» и нажать кнопку «Регистрация».

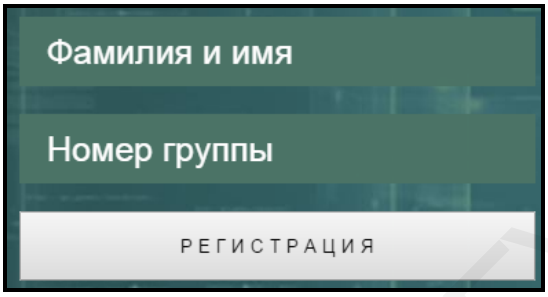



Рисунок 3 – Внешний вид окна регистрации

Затем необходимо в главном окне программы нажать кнопку «Краткие теоретические сведения», после чего на экране появится окно с краткими теоретическими сведениями, показанное на рисунке 4.

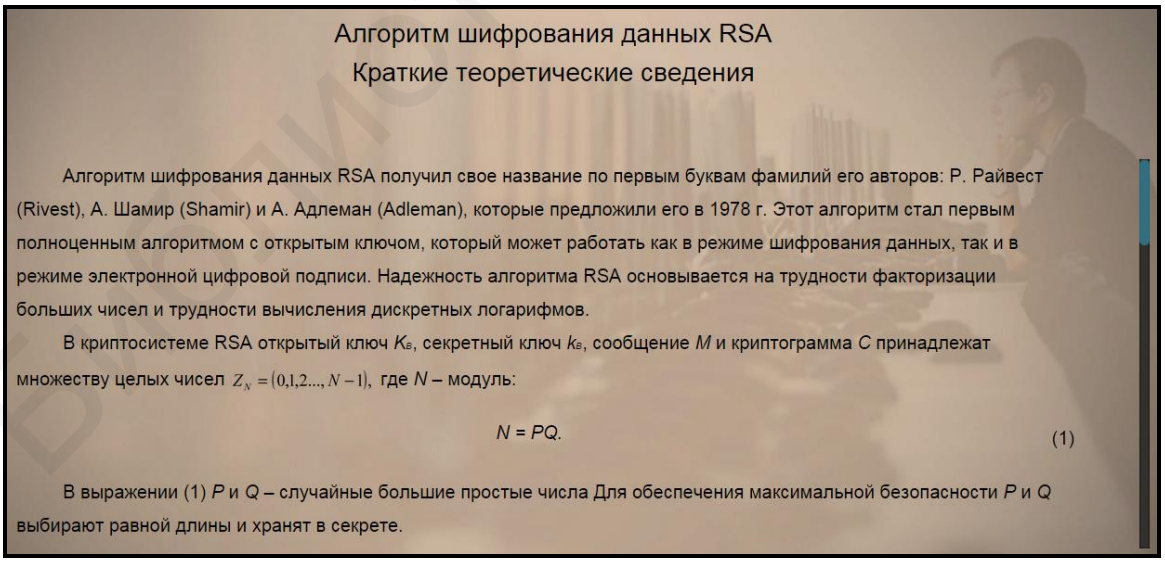



Рисунок 4 – Внешний вид окна с краткими теоретическими сведениями по алгоритму шифрования данных RSA

## 5.2 Практическое задание

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

Для загрузки исходных данных необходимо в главном окне программы (см. рисунок 2) нажать кнопку «Исходные данные» и в появившемся окне ввода и загрузки исходных данных, приведенном на рисунке 5, ввести исходные данные в соответствии с индивидуальным вариантом и нажать кнопку «Загрузить исходные данные».

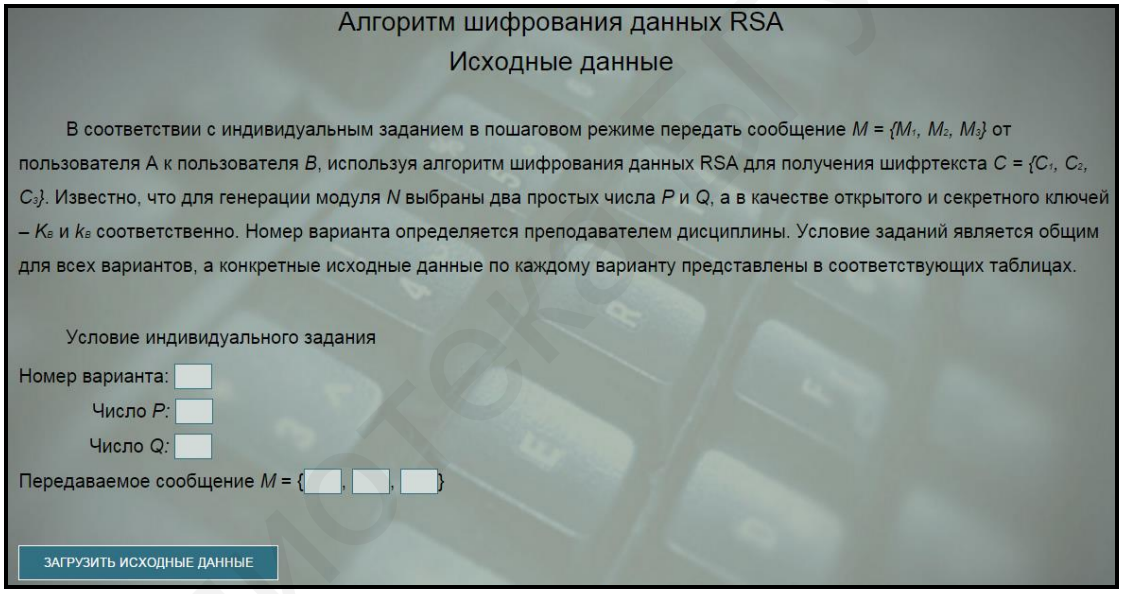



Рисунок 5 – Внешний вид окна ввода и загрузки исходных данных программы, реализующей алгоритм шифрования данных RSA

5.2.2 Выполните предлагаемые задания по передаче сообщения с использование криптосистемы, функционирующей на базе алгоритма RSA.

Выполнение заданий по передаче сообщения заключается в последовательной реализации алгоритма RSA, заполнении и анализе таблицы с полученными результатами. Условие заданий является общим для всех вариантов, а конкретные исходные данные определяются вариантом индивидуального задания.

Для выполнения заданий необходимо в главном окне программы (см. рисунок 2) нажать кнопку «Приступить к выполнению» и в появившемся окне реализации основных этапов алгоритма RSA, приведенном на рисунке 6, заполнить поля для ввода данных, располагающиеся в левой нижней его части, и нажать кнопку «Проверить».

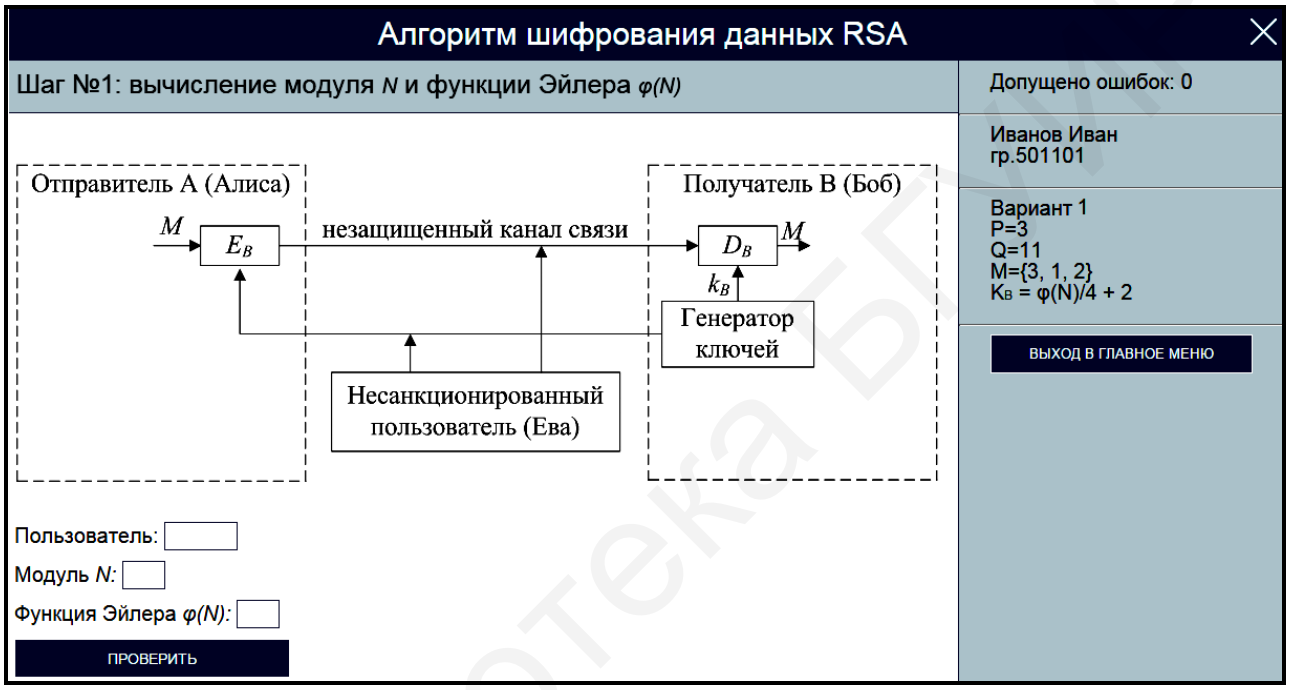



Рисунок 6 – Внешний вид окна реализации основных этапов алгоритма RSA

Если одно или несколько полей для ввода данных не соответствуют заданию, указанному в верхней области окна реализации основных этапов алгоритма RSA, на экран выводится сообщение об ошибке, показанное на рисунке 7.

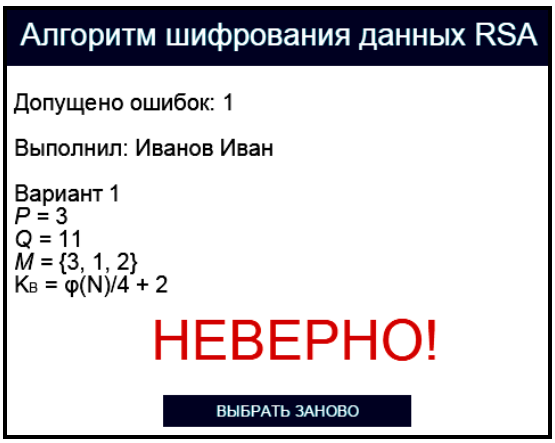



Рисунок 7 – Сообщение об ошибке
реализации основных этапов алгоритма RSA

В этом случае необходимо нажать кнопку «Выбрать заново» и повторно заполнить поля для ввода данных в окне реализации основных этапов алгоритма RSA (см. рисунок 6).

При правильном заполнении полей для ввода данных в окне реализации основных этапов алгоритма RSA на экран выводится соответствующее информационное сообщение. На рисунке 8 в качестве примера показано информационное сообщение, появляющееся после правильного выполнения задания по вычислению модуля $N$ и phi-функции Эйлера $\varphi(n)$.

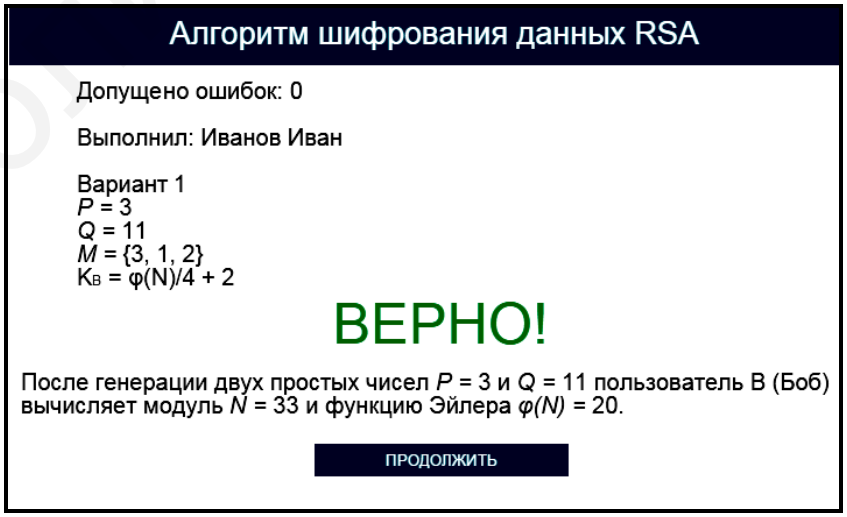



Рисунок 8 – Информационное сообщение программы,
реализующей алгоритм шифрования данных RSA

В правой верхней части окна реализации основных этапов алгоритма RSA имеются три области, в которых указано допущенное количество ошибок, зарегистрированные пользовательские данные и загруженные исходные данные. При щелчке на области, в которой указано допущенное количество ошибок, появляется окно с промежуточными результатами выполнения задания, приведенное на рисунке 9.

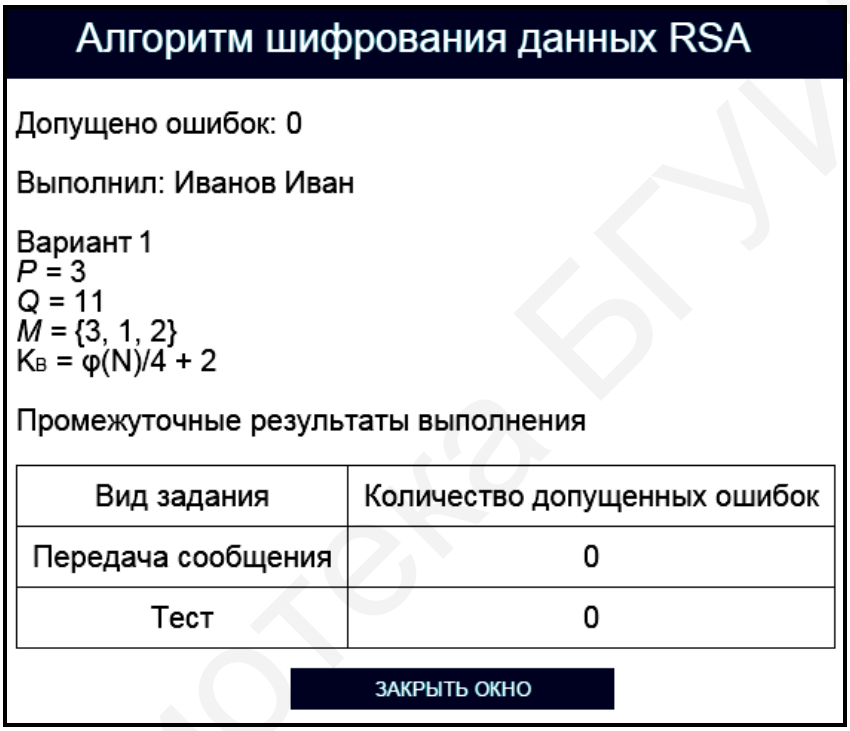



Рисунок 9 – Окно с промежуточными результатами выполнения задания программы, реализующей алгоритм шифрования данных RSA

Для возврата в окно реализации основных этапов алгоритма RSA необходимо нажать кнопку «Закрыть окно».

При нажатии на область, в которой указаны загруженные исходные данные, появляется окно подтверждения смены индивидуального задания, представленное на рисунке 10.

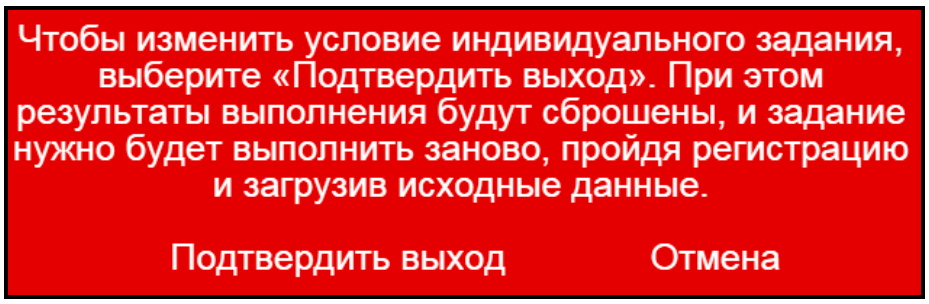



Рисунок 10 – Окно подтверждения смены индивидуального задания

Для изменения условия индивидуального задания необходимо щелкнуть на гиперссылке «Подтвердить выход», для возврата в окно реализации основных этапов алгоритма RSA – на гиперссылке «Отмена».

Выход в главное окно программы (см. рисунок 2) обеспечивается нажатием кнопки «Выход в главное меню» (см. рисунок 6). При этом появляется окно подтверждения выхода в главное окно программы, показанное на рисунке 11.

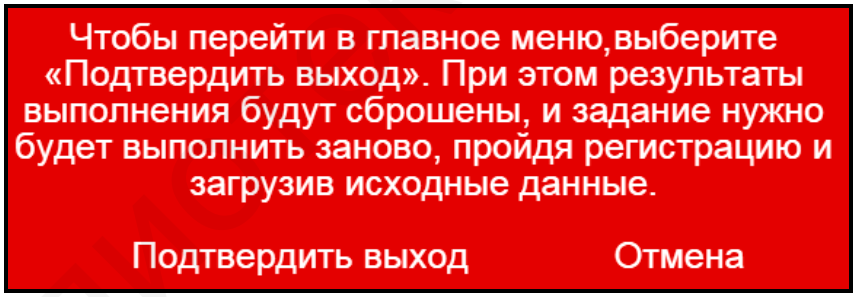



Рисунок 11 – Окно подтверждения выхода в главное окно программы

Для выхода в главное окно программы необходимо щелкнуть на гиперссылке «Подтвердить выход», для возврата в окно реализации основных этапов алгоритма RSA – на гиперссылке «Отмена».

Задание по передаче сообщения с использование криптосистемы, функционирующей на базе алгоритма RSA, считается выполненным, если все предлагаемые задания завершены успешно.

5.2.3 После выполнения заданий по передаче сообщения с использование криптосистемы, функционирующей на базе алгоритма RSA, заполните таблицу 8.

Таблица 8 – Результаты исследования работы криптосистемы, функционирующей на базе алгоритма RSA

| Номер шага (этапа) реализации | Наименование | Описание работы криптосистемы |
|---|---|---|
| | | |

*Примечание – Числа указывать в десятичной системе счисления.*

5.2.4 Выполните тестовые задания.

Для выполнения тестовых заданий необходимо в главном окне программы (см. рисунок 2) нажать кнопку «Тест» и в появившемся окне, показанном на рисунке 12, ознакомиться с инструкцией и нажать кнопку «Начать тест».

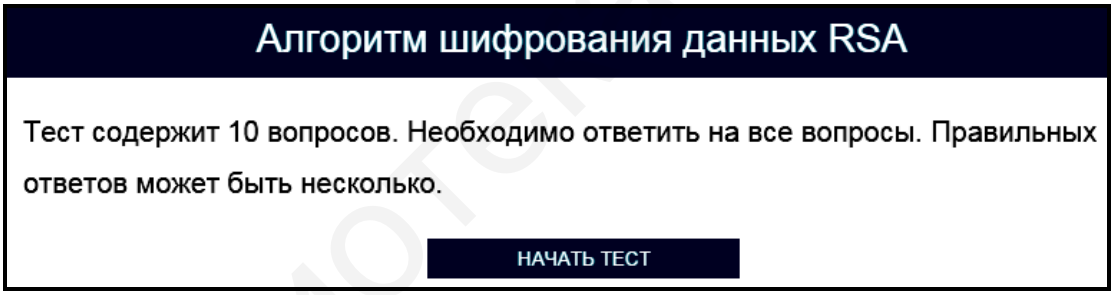



Рисунок 12 – Окно с инструкцией по выполнению тестовых заданий программы, реализующей алгоритм шифрования данных RSA

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

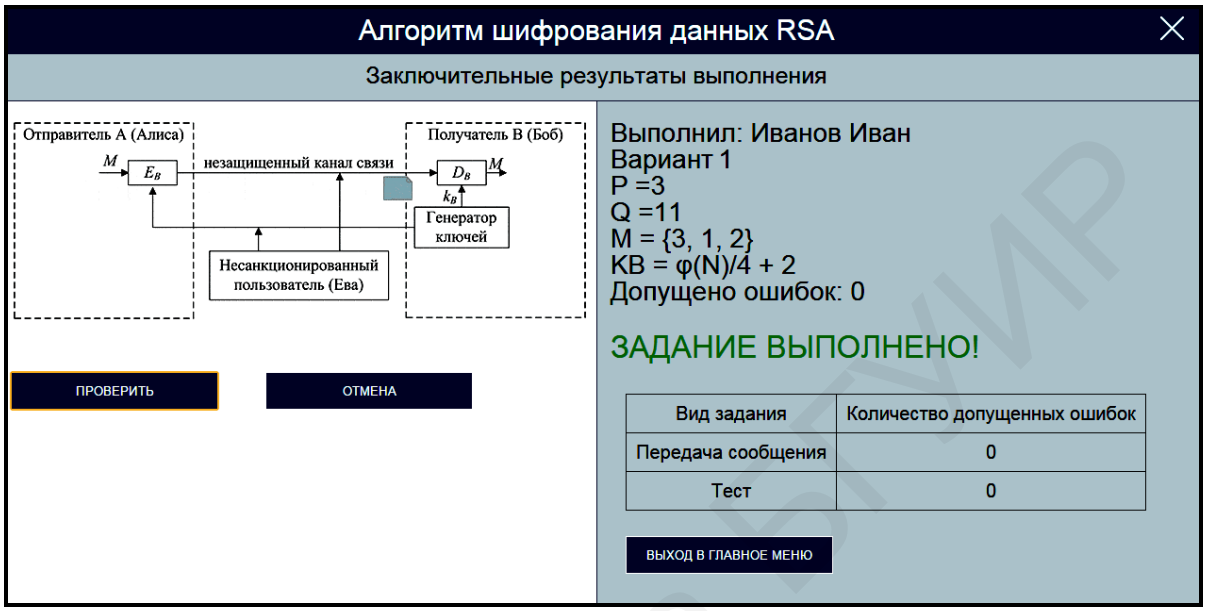
5.2.5 По результатам выполнения тестового задания заполните таблицу 9.

Таблица 9 – Результаты выполнения тестового задания 5.2.4

| Вопрос | Правильный ответ |
|---|---|
| | |

*Примечание – Числа указывать в десятичной системе счисления.*

Лабораторное задание считается выполненным, если все предлагаемые задания завершены успешно. При этом на экран выводится окно, показанное на рисунке 13, а.




а


б

а – задание выполнено; б – задание не выполнено

Рисунок 13 – Окно с заключительными результатами выполнения задания программы, реализующей алгоритм шифрования данных RSA

Лабораторное задание считается не выполненным, если на экран выводится окно, показанное на рисунке 13, б. В этом случае необходимо нажать кнопку «Выполнить еще раз» и заново выполнить пункты 5.2.1 … 5.2.5.

5.2.6 Продемонстрируйте выполнение практического задания преподавателю дисциплины.

### 5.3 Содержание отчета

1 Цель лабораторной работы.

2 Структурная схема криптосистемы RSA после выполнения шага 5 алгоритма.

3 Уравнения шифрования данных и расшифрования шифртекстов алгоритма RSA.

4 Таблица с исходными данными, соответствующими индивидуальному варианту задания.

5 Таблицы с результатами выполнения задания.

6 Выводы по результатам выполнения задания.

7 Ответы на контрольные вопросы.

### 5.4 Контрольные вопросы

1 Каким образом реализуется алгоритм шифрования данных RSA?

2 Каким образом в алгоритме RSA реализуется расшифрование шифртекста?

3 Какую длину имеет ключ шифрования данных RSA?

4 Какие криптографические операции выполняются в алгоритме RSA?

5 Какое практическое применение находит алгоритм RSA?

# ЛАБОРАТОРНАЯ РАБОТА №6
# КРИПТОГРАФИЧЕСКАЯ СИСТЕМА РАБИНА

**Цель:** изучение алгоритмов шифрования данных и расшифрования шифртекстов в криптографической системе Рабина.

## 6.1 Краткие теоретические сведения

Для ознакомления с краткими теоретическими сведениями включите персональный компьютер и запустите файл «lr6_Rabina.exe» на выполнение.

После запуска файла «lr6_Rabina.exe» активизируется программное обеспечение, реализующее схемы шифрования данных и расшифрования шифртекстов на базе алгоритма Рабина, и появится главное окно программы, показанное на рисунке 14.

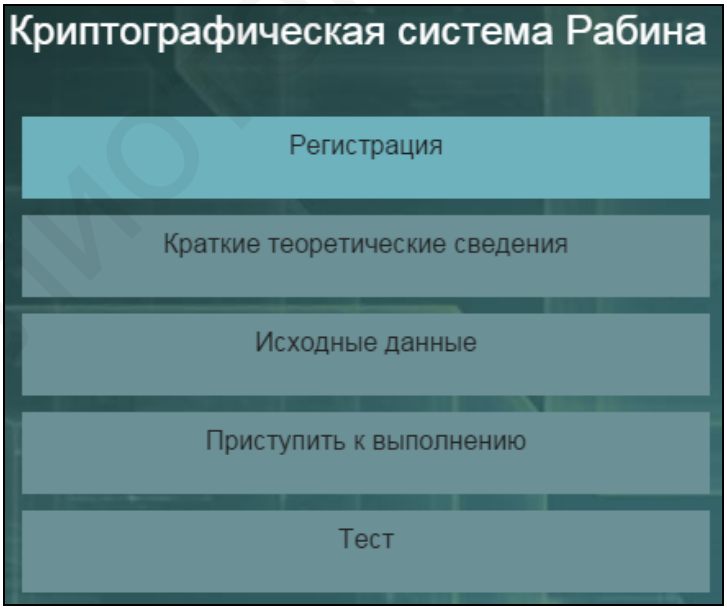



Рисунок 14 – Главное окно программы,
реализующей криптосистему Рабина

До начала работы с программой необходимо зарегистрироваться. Для этого требуется в главном окне программы нажать кнопку «Регистрация» и в появившемся окне регистрации, приведенном на рисунке 3, ввести в поле «Фамилия и имя» свою фамилию и имя, указать номер группы в поле «Номер группы» и нажать кнопку «Регистрация».

Затем необходимо в главном окне программы нажать кнопку «Краткие теоретические сведения», после чего на экран выводится окно с краткими теоретическими сведениями, показанное на рисунке 15.

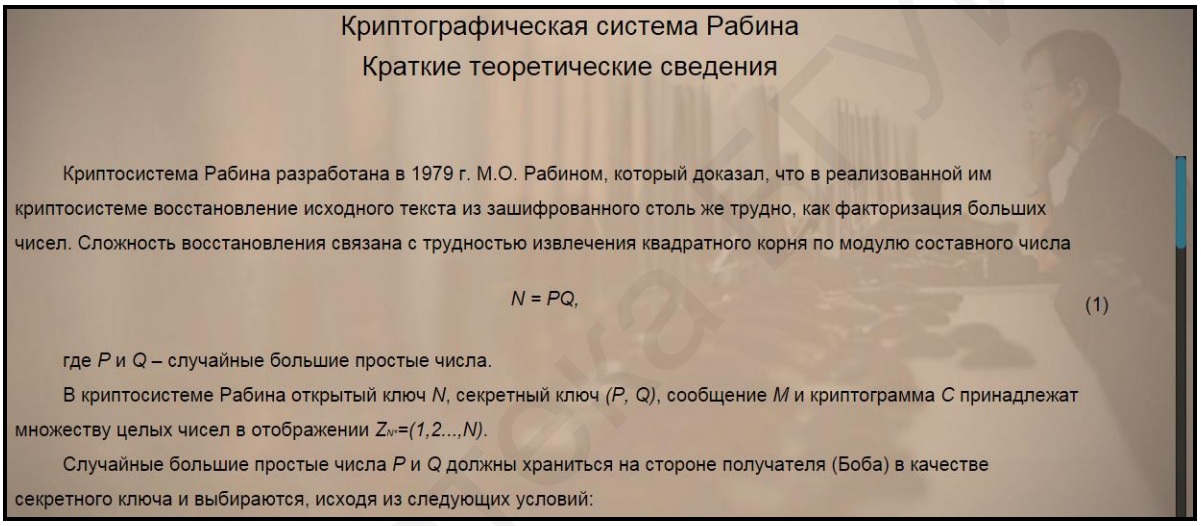



Рисунок 15 – Внешний вид окна с краткими теоретическими сведениями по криптоалгоритму Рабина

### 6.2 Практическое задание

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

Для загрузки исходных данных необходимо в главном окне программы (см. рисунок 14) нажать кнопку «Исходные данные» и в появившемся окне ввода и загрузки исходных данных, приведенном на рисунке 16, ввести исходные данные в соответствии с индивидуальным вариантом и нажать кнопку «Загрузить исходные данные».

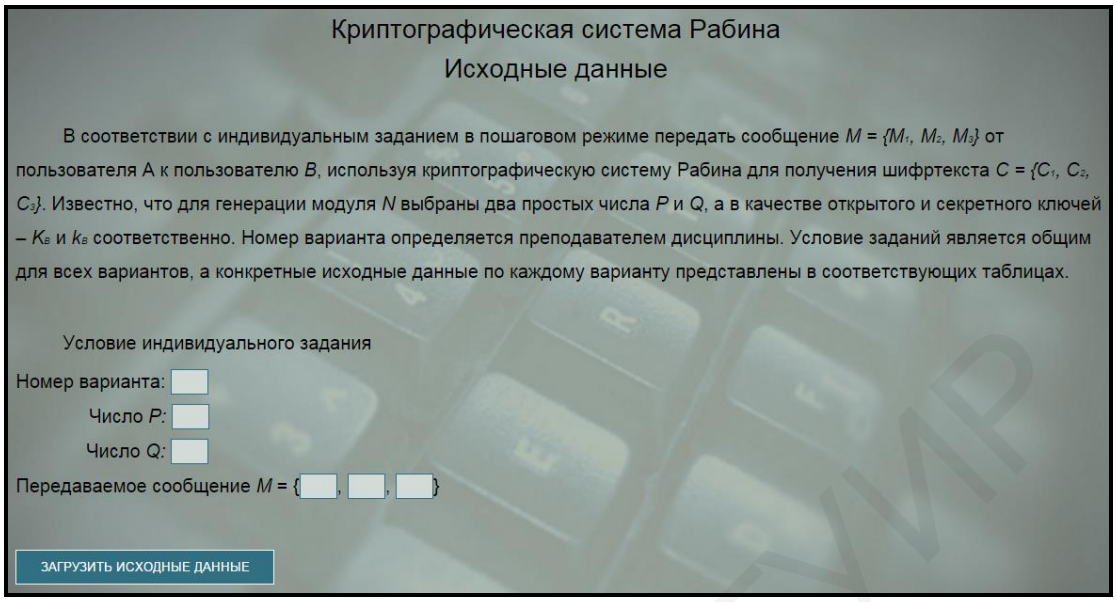



Рисунок 16 – Внешний вид окна ввода и загрузки исходных данных программы, реализующей криптосистему Рабина

6.2.2 Выполните предлагаемые задания по передаче сообщения с использование криптосистемы, функционирующей на базе алгоритма Рабина.

Выполнение заданий по передаче сообщения заключается в последовательной реализации алгоритма Рабина, заполнении и анализе таблицы с полученными результатами. Условие заданий является общим для всех вариантов, а конкретные исходные данные определяются вариантом индивидуального задания.

Для выполнения заданий необходимо в главном окне программы (см. рисунок 14) нажать кнопку «Приступить к выполнению» и в появившемся окне реализации основных этапов алгоритма Рабина, приведенном на рисунке 17, заполнить поля для ввода данных, располагающиеся в левой нижней его части, и нажать кнопку «Проверить».


Рисунок 17 – Внешний вид окна реализации основных этапов алгоритма Рабина

Если одно или несколько полей для ввода данных не соответствуют заданию, указанному в верхней области окна реализации основных этапов алгоритма Рабина, на экран выводится сообщение об ошибке, показанное на рисунке 18.

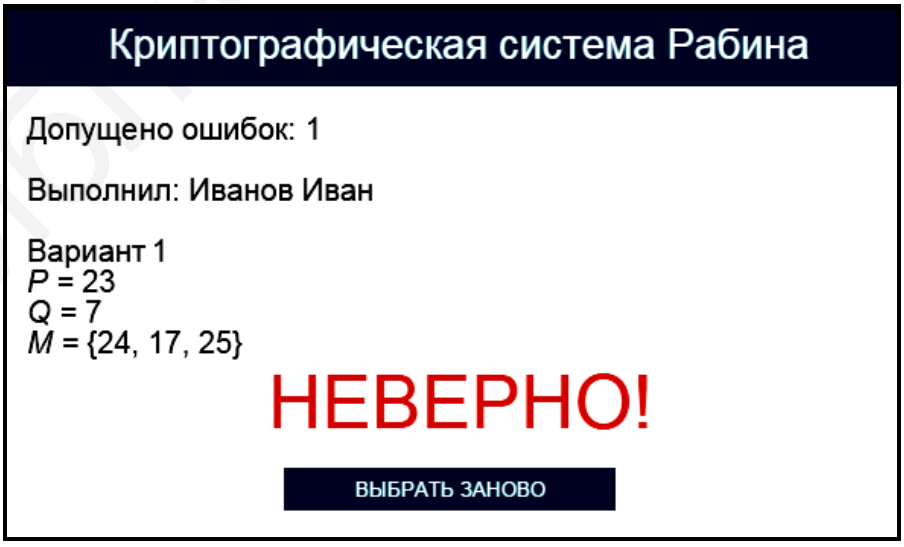



Рисунок 18 – Сообщение об ошибке реализации основных этапов алгоритма Рабина

В этом случае необходимо нажать кнопку «Выбрать заново» и повторно заполнить поля для ввода данных в окне реализации основных этапов алгоритма Рабина (см. рисунок 17).

При правильном заполнении полей для ввода данных в окне реализации основных этапов алгоритма Рабина на экран выводится соответствующее информационное сообщение. На рисунке 19 в качестве примера показано информационное сообщение, появляющееся после правильного выполнения задания по вычислению модуля $N$ и опубликованию открытых данных.

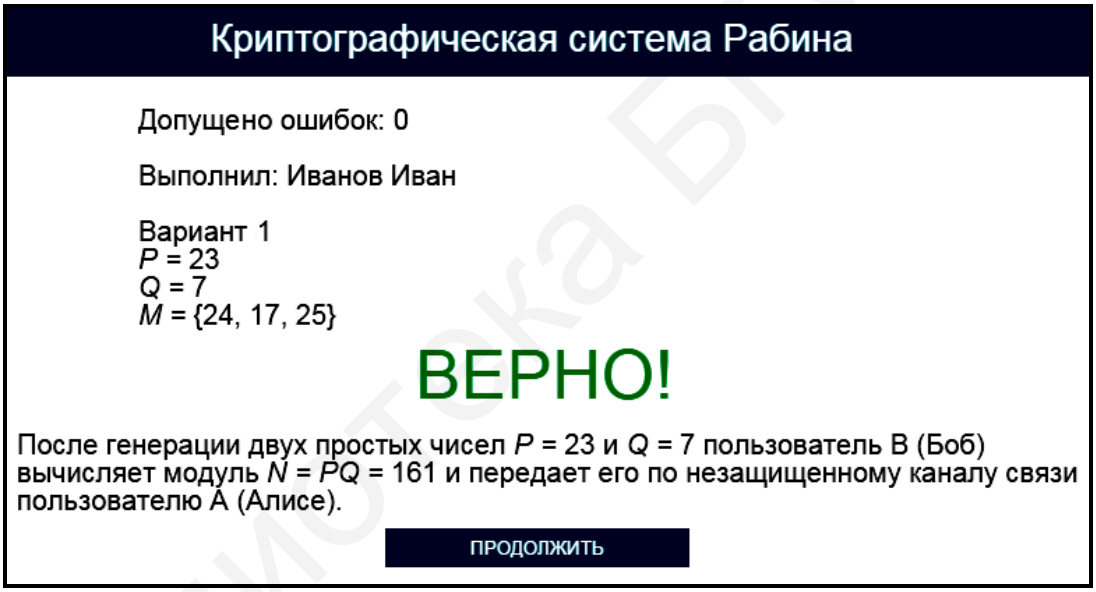



Рисунок 19 – Информационное сообщение
программы, реализующей криптосистему Рабина

В правой верхней части окна реализации основных этапов алгоритма Рабина имеются три области, в которых указано допущенное количество ошибок, зарегистрированные пользовательские данные и загруженные исходные данные. При щелчке на области, в которой указано допущенное количество ошибок, появляется окно с промежуточными результатами выполнения задания, приведенное на рисунке 20.

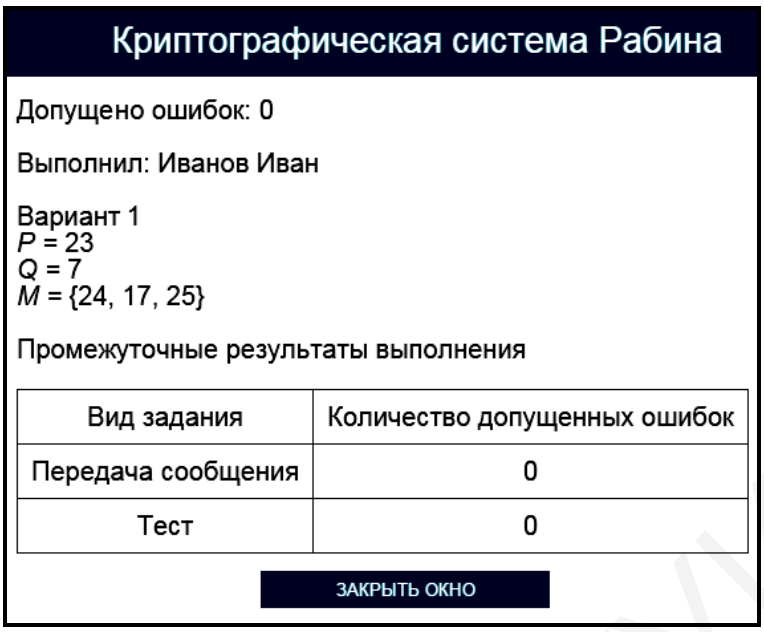



Рисунок 20 – Окно с промежуточными результатами выполнения задания программы, реализующей криптосистему Рабина

Для возврата в окно реализации основных этапов алгоритма Рабина необходимо нажать кнопку «Закрыть окно».

При щелчке на области, в которой указаны загруженные исходные данные, появляется окно подтверждения смены индивидуального задания (см. рисунок 10). Для изменения условия индивидуального задания необходимо щелкнуть на гиперссылке «Подтвердить выход», для возврата в окно реализации основных этапов алгоритма Рабина – на гиперссылке «Отмена».

Выход в главное окно программы (см. рисунок 14) обеспечивается нажатием кнопки «Выход в главное меню» (см. рисунок 17). При этом появляется окно подтверждения выхода в главное окно программы (см. рисунок 11). Для выхода в главное окно программы необходимо щелкнуть на гиперссылке «Подтвердить выход», для возврата в окно реализации основных этапов алгоритма Рабина – на гиперссылке «Отмена».

Задание по передаче сообщения с использование криптосистемы, функционирующей на базе алгоритма Рабина, считается выполненным, если все предлагаемые задания завершены успешно.

6.2.3 После выполнения заданий по передаче сообщения с использование криптосистемы, функционирующей на базе алгоритма Рабина, заполните таблицу 10.

Таблица 10 – Результаты исследования работы криптосистемы, функционирующей на базе алгоритма Рабина

| Номер шага (этапа) реализации | Наименование | Описание работы криптосистемы |
|---|---|---|
| | | |

*Примечание – Числа указывать в десятичной системе счисления.*

6.2.4 Выполните тестовые задания.

Для выполнения тестовых заданий необходимо в главном окне программы (см. рисунок 14) нажать кнопку «Тест» и в появившемся окне, показанном на рисунке 21, ознакомиться с инструкцией и нажать кнопку «Начать тест».

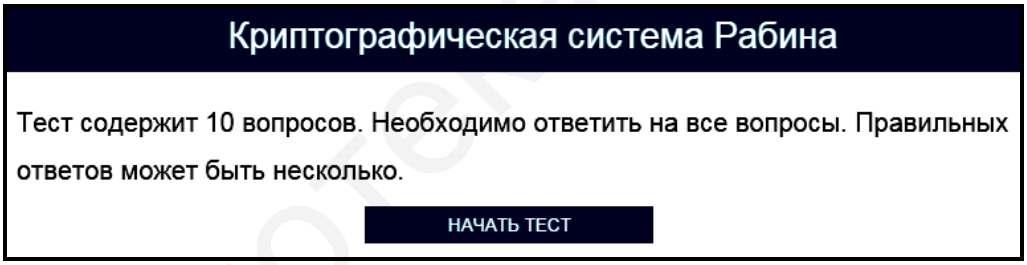



Рисунок 21 – Окно с инструкцией по выполнению тестовых заданий программы, реализующей криптосистему Рабина

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

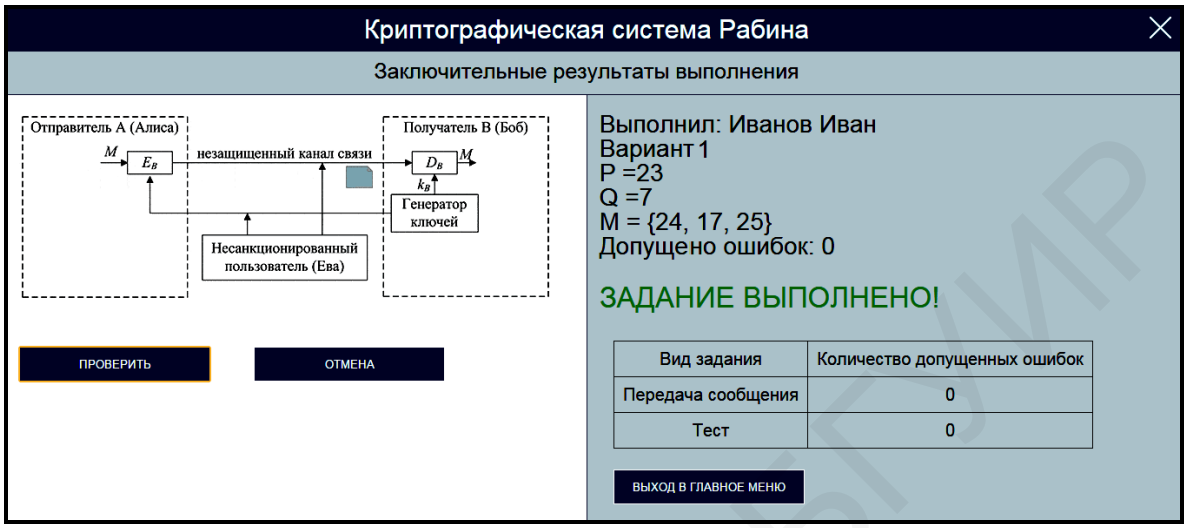
6.2.5 По результатам выполнения тестового задания заполните таблицу 11.

Таблица 11 – Результаты выполнения тестового задания 6.2.4

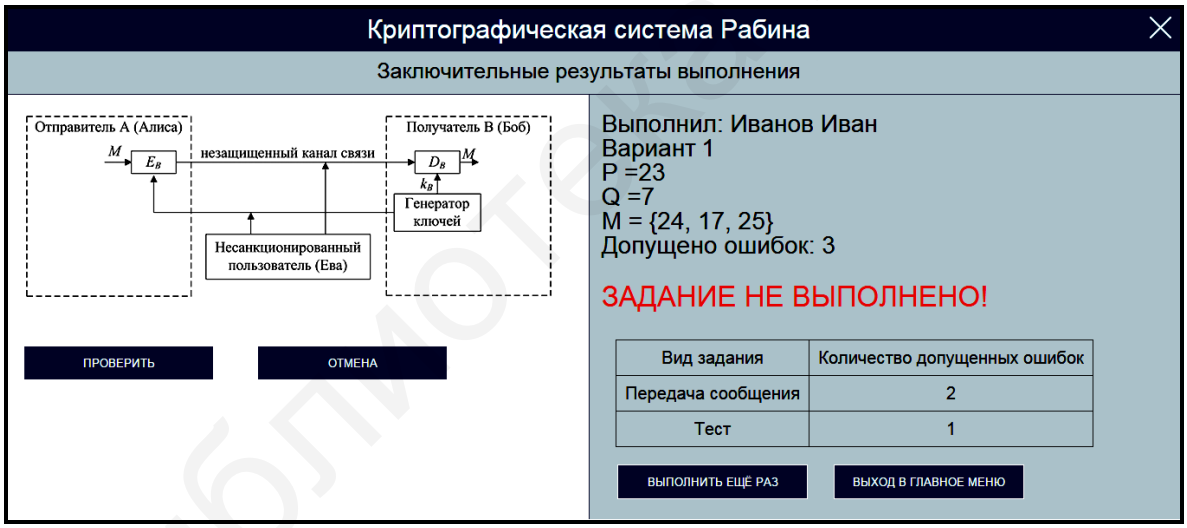
| Вопрос | Правильный ответ |
|---|---|
| | |

*Примечание – Числа указывать в десятичной системе счисления.*

Лабораторное задание считается выполненным, если все предлагаемые задания завершены успешно. При этом на экран выводится окно, показанное на рисунке 22, а.




а




б

а – задание выполнено; б – задание не выполнено

Рисунок 22 – Окно с заключительными результатами выполнения задания программы, реализующей криптосистему Рабина

Лабораторное задание считается не выполненным, если на экран выводится окно, показанное на рисунке 22, б. В этом случае необходимо нажать кнопку «Выполнить еще раз» и заново выполнить пункты 6.2.1 … 6.2.5.

6.2.6 Продемонстрируйте выполнение практического задания преподавателю дисциплины.

### 6.3 Содержание отчета

1 Цель лабораторной работы.

2 Структурная схема криптосистемы Рабина после выполнения шага 5 алгоритма.

3 Уравнения шифрования данных и расшифрования шифртекстов алгоритма Рабина.

4 Таблица с исходными данными, соответствующими индивидуальному варианту задания.

5 Таблицы с результатами выполнения задания.

6 Выводы по результатам выполнения задания.

7 Ответы на контрольные вопросы.

### 6.4 Контрольные вопросы

1 Каким образом реализуется алгоритм шифрования данных в криптографической системе Рабина?

2 Каким образом в алгоритме Рабина реализуется расшифрование шифртекста?

3 Что определяет информационную безопасность криптографической системы Рабина?

4 Какие преимущества имеет криптографическая система Рабина в сравнении с симметричными криптосистемами?

5 Какие преимущества имеет криптографическая система Рабина в сравнении с криптосистемой на базе алгоритма RSA?

# ЛАБОРАТОРНАЯ РАБОТА №7
# КРИПТОГРАФИЧЕСКАЯ СИСТЕМА ЭЛЬ ГАМАЛЯ

**Цель:** изучение схем шифрования данных и расшифрования шифртекстов, основанных на алгоритме Эль Гамаля.

## 7.1 Краткие теоретические сведения

Для ознакомления с краткими теоретическими сведениями включите персональный компьютер и запустите файл «lr7_El_Gamal.exe» на выполнение.

После запуска файла «lr7_El_Gamal.exe» активизируется программное обеспечение, реализующее схемы шифрования данных и расшифрования шифртекстов на базе алгоритма Эль Гамаля, и появится главное окно программы, показанное на рисунке 23.

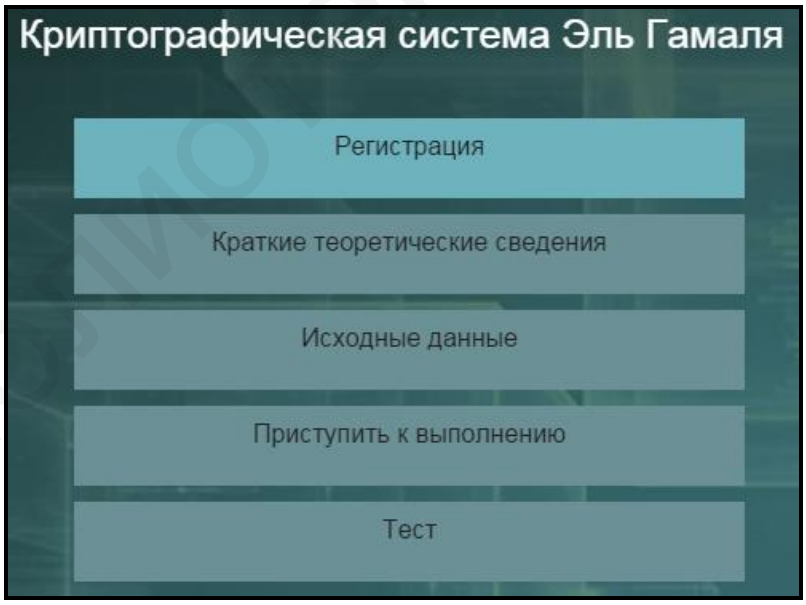



Рисунок 23 – Главное окно программы,
реализующей криптосистему Эль Гамаля

До начала работы с программой необходимо зарегистрироваться. Для этого требуется в главном окне программы нажать кнопку «Регистрация» и в появившемся окне регистрации, приведенном на рисунке 3, ввести в поле «Фамилия и имя» свою фамилию и имя, указать номер группы в поле «Номер группы» и нажать кнопку «Регистрация».

Затем необходимо в главном окне программы нажать кнопку «Краткие теоретические сведения», после чего на экран выводится окно с краткими теоретическими сведениями, показанное на рисунке 24.

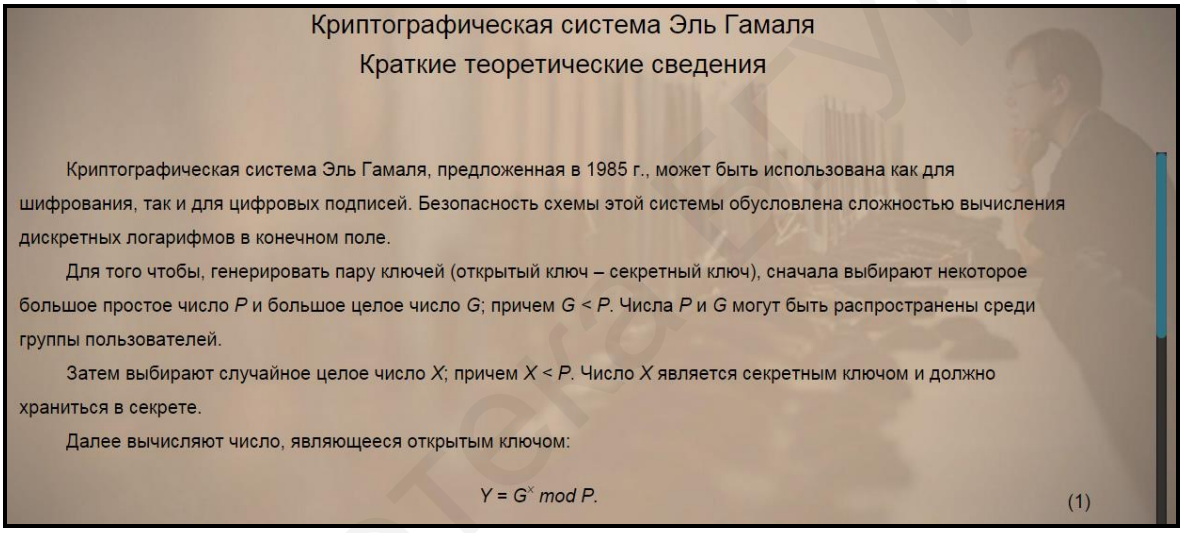



Рисунок 24 – Внешний вид окна регистрации программы, реализующей криптосистему Эль Гамаля

### 7.2 Практическое задание

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

Для загрузки исходных данных необходимо в главном окне программы (см. рисунок 23) нажать кнопку «Исходные данные» и в появившемся окне ввода и загрузки исходных данных, приведенном на рисунке 25, ввести исходные данные в соответствии с индивидуальным вариантом и нажать кнопку «Загрузить исходные данные».

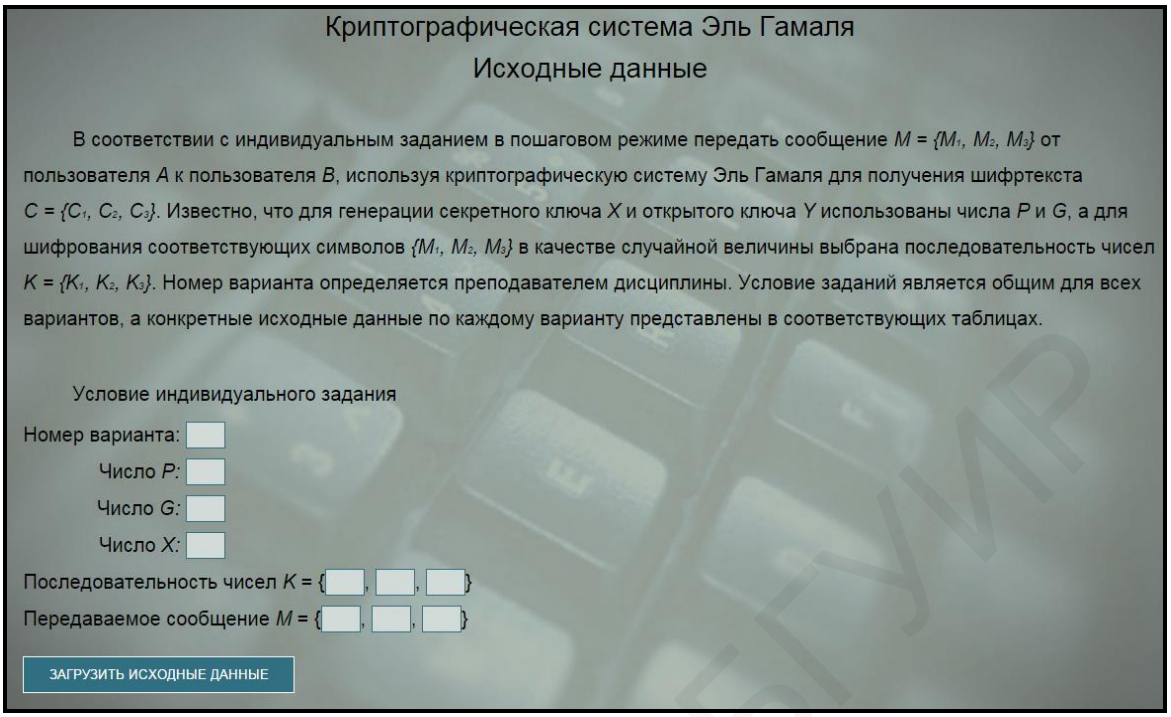



Рисунок 25 – Внешний вид окна ввода и загрузки исходных данных программы, реализующей криптосистему Эль Гамаля

7.2.2 Выполните предлагаемые задания по передаче сообщения с использование криптосистемы, функционирующей на базе алгоритма Эль Гамаля.

Выполнение заданий по передаче сообщения заключается в последовательной реализации алгоритма Эль Гамаля, заполнении и анализе таблицы с полученными результатами. Условие заданий является общим для всех вариантов, а конкретные исходные данные определяются вариантом индивидуального задания.

Для выполнения заданий необходимо в главном окне программы (см. рисунок 23) нажать кнопку «Приступить к выполнению» и в появившемся окне реализации основных этапов алгоритма Эль Гамаля, приведенном на рисунке 26, заполнить поля для ввода данных, располагающиеся в левой нижней его части, и нажать кнопку «Проверить».


Рисунок 26 – Внешний вид окна реализации основных этапов криптоалгоритма Эль Гамаля

Если одно или несколько полей для ввода данных не соответствуют заданию, указанному в верхней области окна реализации основных этапов алгоритма Эль Гамаля, на экран выводится сообщение об ошибке, показанное на рисунке 27.

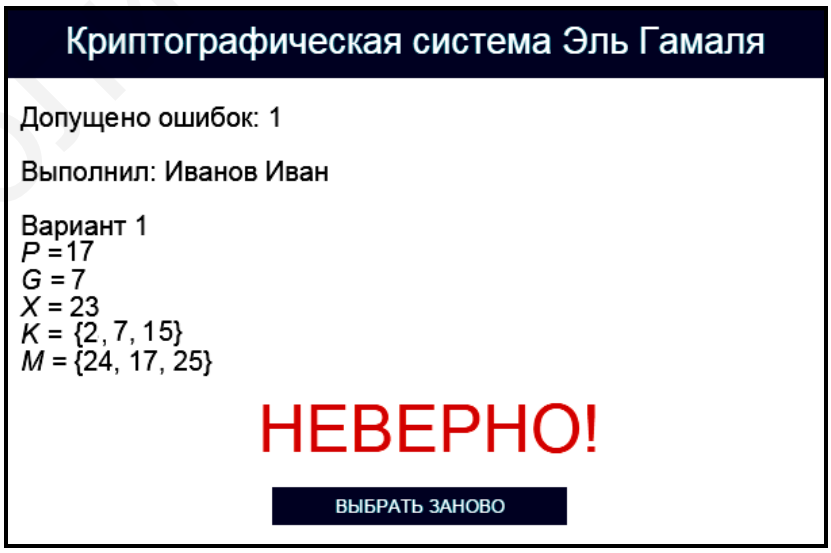



Рисунок 27 – Сообщение об ошибке реализации основных этапов криптоалгоритма Эль Гамаля

В этом случае необходимо нажать кнопку «Выбрать заново» и повторно заполнить поля для ввода данных в окне реализации основных этапов алгоритма Эль Гамаля (см. рисунок 26).

При правильном заполнении полей для ввода данных в окне реализации основных этапов алгоритма Эль Гамаля на экран выводится соответствующее информационное сообщение. На рисунке 28 в качестве примера показано информационное сообщение, появляющееся после правильного выполнения задания по вычислению открытого ключа *Y*.

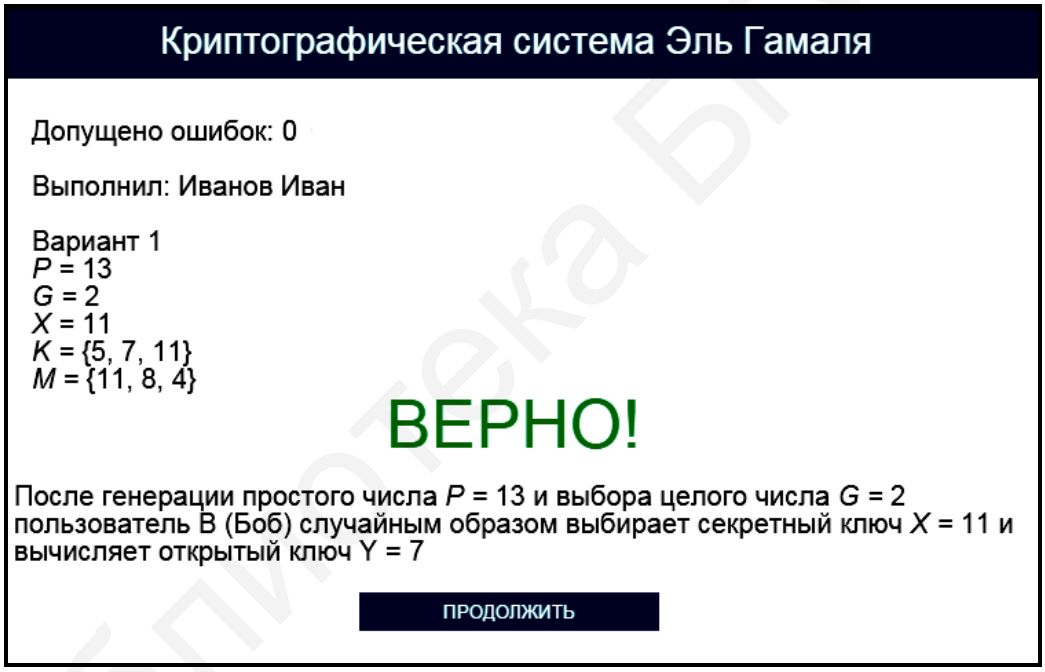



Рисунок 28 – Информационное сообщение программы, реализующей криптосистему Эль Гамаля

В правой верхней части окна реализации основных этапов алгоритма Эль Гамаля имеются три области, в которых указано допущенное количество ошибок, зарегистрированные пользовательские данные и загруженные исходные данные. При щелчке на области, в которой указано допущенное количество ошибок, появляется окно с промежуточными результатами выполнения задания, приведенное на рисунке 29.

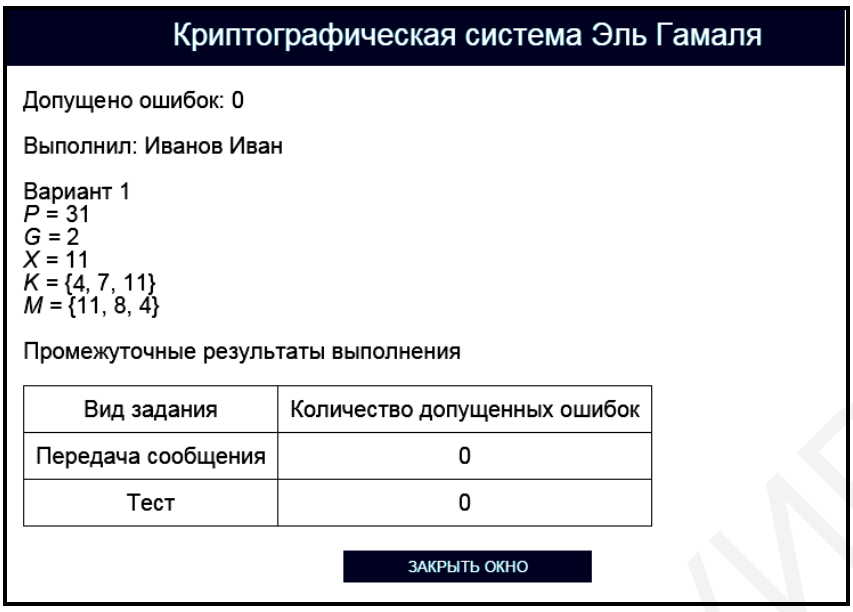



Рисунок 29 – Окно с промежуточными результатами выполнения задания программы, реализующей криптосистему Эль Гамаля

Для возврата в окно реализации основных этапов алгоритма Эль Гамаля необходимо нажать кнопку «Закрыть окно».

При щелчке на области, в которой указаны загруженные исходные данные, появляется окно подтверждения смены индивидуального задания (см. рисунок 10). Для изменения условия индивидуального задания необходимо щелкнуть на гиперссылке «Подтвердить выход», для возврата в окно реализации основных этапов алгоритма Эль Гамаля – на гиперссылке «Отмена».

Выход в главное окно программы (см. рисунок 23) обеспечивается нажатием кнопки «Выход в главное меню» (см. рисунок 26). При этом появляется окно подтверждения выхода в главное окно программы (см. рисунок 11). Для выхода в главное окно программы необходимо щелкнуть на гиперссылке «Подтвердить выход», для возврата в окно реализации основных этапов алгоритма Эль Гамаля – на гиперссылке «Отмена».

Задание по передаче сообщения с использование криптосистемы, функционирующей на базе алгоритма Эль Гамаля, считается выполненным, если все предлагаемые задания завершены успешно.

7.2.3 После выполнения заданий по передаче сообщения с использование криптосистемы, функционирующей на базе алгоритма Эль Гамаля, заполните таблицу 12.

Таблица 12 – Результаты исследования работы криптосистемы, функционирующей на базе алгоритма Эль Гамаля

| Номер шага (этапа) реализации | Наименование | Описание работы криптосистемы |
|---|---|---|
| | | |

*Примечание – Числа указывать в десятичной системе счисления.*

7.2.4 Выполните тестовые задания.

Для выполнения тестовых заданий необходимо в главном окне программы (см. рисунок 23) нажать кнопку «Тест» и в появившемся окне, показанном на рисунке 30, ознакомиться с инструкцией и нажать кнопку «Начать тест».

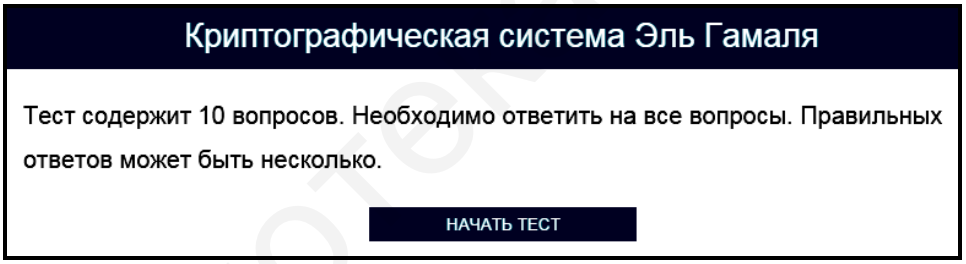



Рисунок 30 – Окно с инструкцией по выполнению тестовых заданий программы, реализующей криптосистему Эль Гамаля

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

7.2.5 По результатам выполнения тестового задания заполните таблицу 13.

Таблица 13 – Результаты выполнения тестового задания 7.2.4

| Вопрос | Правильный ответ |
|---|---|
| | |

*Примечание – Числа указывать в десятичной системе счисления.*

Лабораторное задание считается выполненным, если все предлагаемые 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 – Окно с заключительными результатами выполнения задания программы, реализующей криптосистему Эль Гамаля

Лабораторное задание считается не выполненным, если на экран выводится окно, показанное на рисунке 31, б. В этом случае необходимо нажать кнопку «Выполнить еще раз» и заново выполнить пункты 7.2.1 … 7.2.5.

7.2.6 Продемонстрируйте выполнение практического задания преподавателю дисциплины.

### 7.3 Содержание отчета

1 Цель лабораторной работы.

2 Структурная схема криптосистемы Эль Гамаля после выполнения шага 6 алгоритма.

3 Уравнения шифрования данных и расшифрования шифртекстов алгоритма Эль Гамаля.

4 Таблица с исходными данными, соответствующими индивидуальному варианту задания.

5 Таблицы с результатами выполнения задания.

6 Выводы по результатам выполнения задания.

7 Ответы на контрольные вопросы.

### 7.4 Контрольные вопросы

1 Каким образом реализуется алгоритм шифрования данных Эль Гамаля?

2 Каким образом в алгоритме Эль Гамаля реализуется расшифрование шифртекста?

3 Каким образом в криптосистеме Эль Гамаля выбирается открытый ключ?

4 Что определяет информационную безопасность криптографической системы Эль Гамаля?

5 Какие преимущества имеет криптографическая система Эль Гамаля в сравнении с другими криптосистемами?

# ЛАБОРАТОРНАЯ РАБОТА №8
# ПРОТОКОЛ ФЕЙГЕ – ФИАТА – ШАМИРА

**Цель:** изучение протокола Фейге – Фиата – Шамира, позволяющего выполнять идентификацию объектов на основе криптографических операций.

## 8.1 Краткие теоретические сведения

Для ознакомления с краткими теоретическими сведениями включите персональный компьютер и запустите файл «lr8_Feige-Fiat-Shamir.exe» на выполнение.

После запуска файла «lr8_Feige-Fiat-Shamir.exe» активизируется программное обеспечение, реализующее протокол Фейге – Фиата – Шамира, и появится главное окно программы, показанное на рисунке 32.

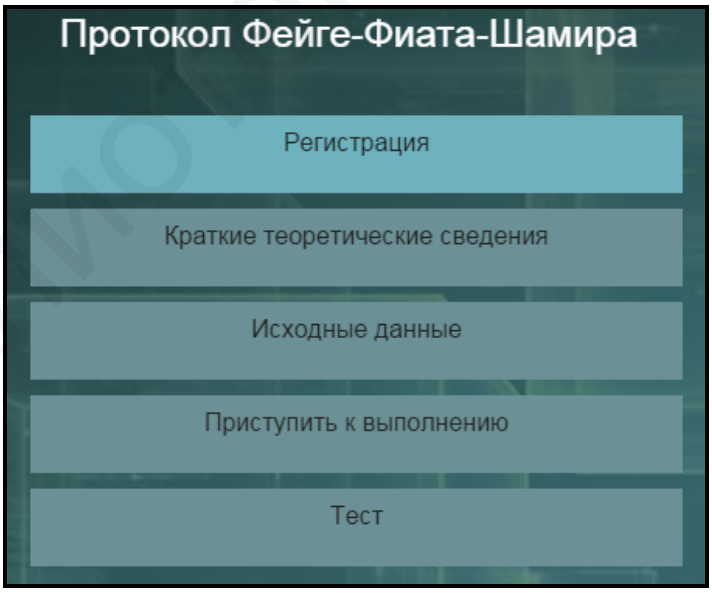



Рисунок 32 – Главное окно программы,
реализующей протокол Фейге – Фиата – Шамира

До начала работы с программой необходимо зарегистрироваться. Для этого требуется в главном окне программы нажать кнопку «Регистрация» и в появившемся окне регистрации, приведенном на рисунке 3, ввести в поле «Фамилия и имя» свою фамилию и имя, указать номер группы в поле «Номер группы» и нажать кнопку «Регистрация».

Затем необходимо в главном окне программы нажать кнопку «Краткие теоретические сведения», после чего на экран выводится окно с краткими теоретическими сведениями, показанное на рисунке 33.

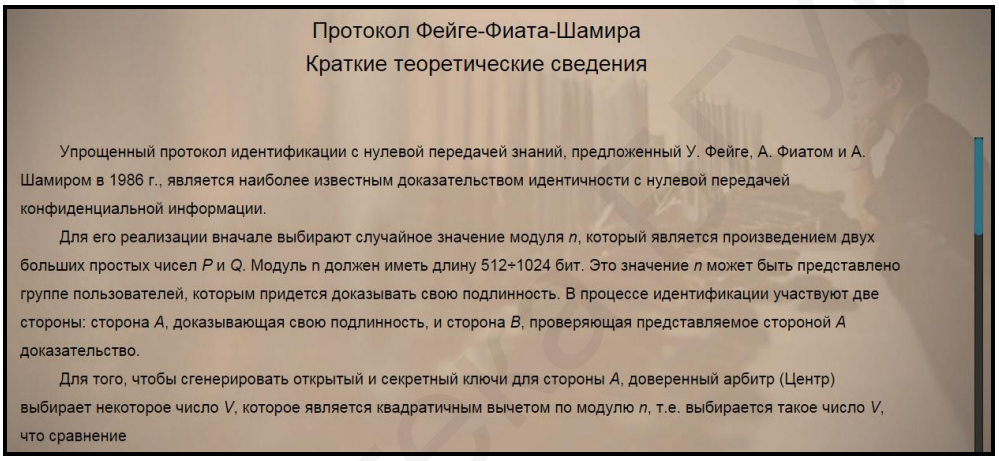



Рисунок 33 – Внешний вид окна с краткими теоретическими сведениями по алгоритму идентификации объектов на основе протокола Фейге – Фиата – Шамира

## 8.2 Практическое задание

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

Для загрузки исходных данных необходимо в главном окне программы (см. рисунок 32) нажать кнопку «Исходные данные» и в появившемся окне ввода и загрузки исходных данных, приведенном на рисунке 34, ввести исходные данные в соответствии с индивидуальным вариантом и нажать кнопку «Загрузить исходные данные».

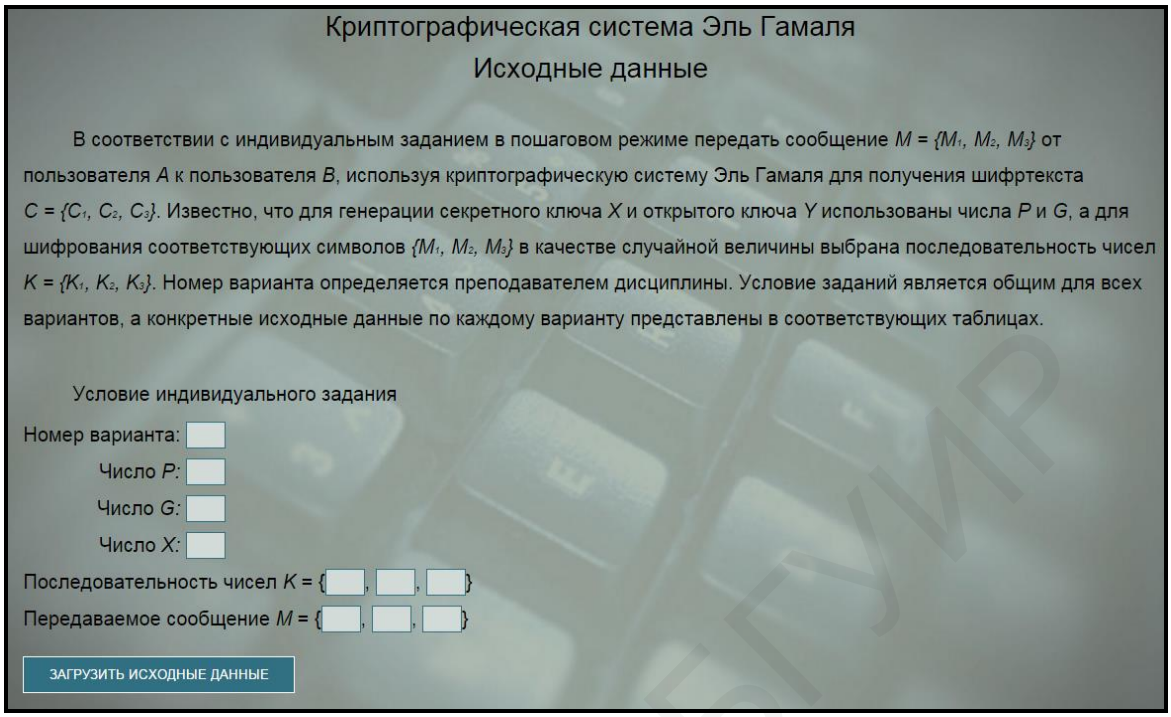



Рисунок 34 – Внешний вид окна ввода и загрузки исходных данных программы, реализующей протокол Фейге – Фиата – Шамира

8.2.2 Выполните предлагаемые задания по передаче конфиденциальной информации с использованием протокола Фейге – Фиата – Шамира.

Выполнение заданий по передаче конфиденциальной информации заключается в последовательной реализации протокола Фейге – Фиата – Шамира, заполнении и анализе таблицы с полученными результатами. Условие заданий является общим для всех вариантов, а конкретные исходные данные определяются вариантом индивидуального задания.

Для выполнения заданий необходимо в главном окне программы (см. рисунок 32) нажать кнопку «Приступить к выполнению» и в появившемся окне реализации основных этапов протокола Фейге – Фиата – Шамира, приведенном на рисунке 35, заполнить поля для ввода данных, располагающиеся в центральной его части, и нажать кнопку «Проверить».

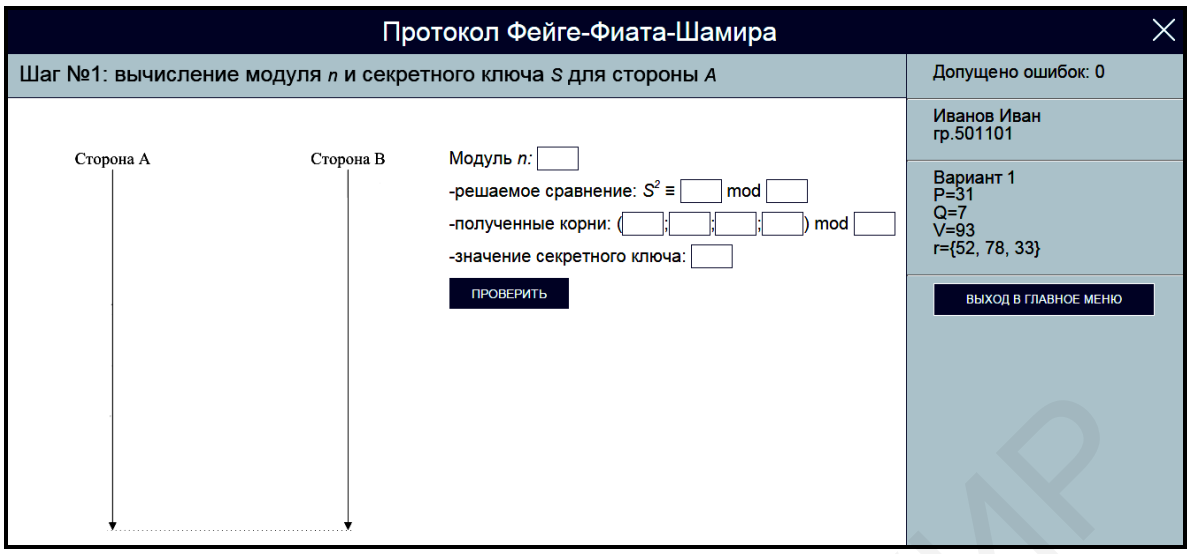



Рисунок 35 – Внешний вид окна реализации
основных этапов протокола Фейге – Фиата – Шамира

Если одно или несколько полей для ввода данных не соответствуют заданию, указанному в верхней области окна реализации основных этапов протокола Фейге – Фиата – Шамира, на экран выводится сообщение об ошибке, показанное на рисунке 36.

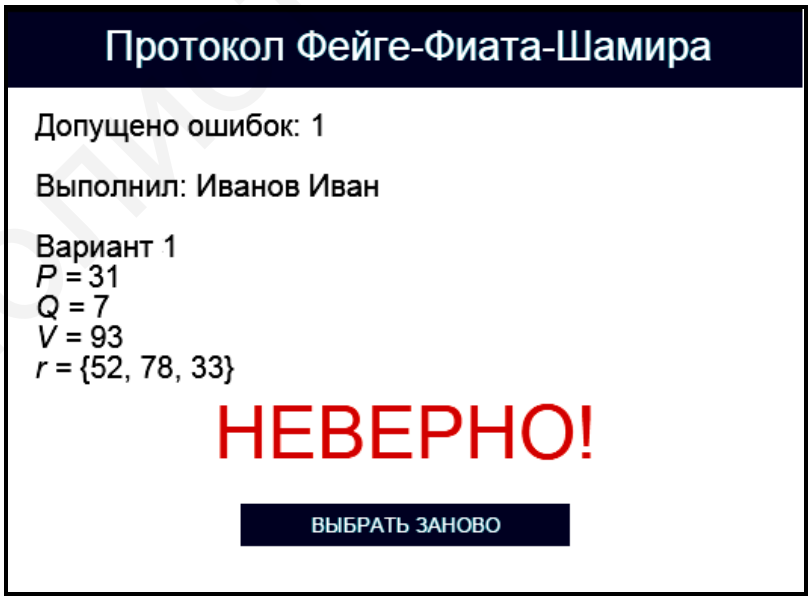



Рисунок 36 – Сообщение об ошибке реализации
основных этапов протокола Фейге – Фиата – Шамира

В этом случае необходимо нажать кнопку «Выбрать заново» и повторно заполнить поля для ввода данных в окне реализации основных этапов протокола Фейге – Фиата – Шамира (см. рисунок 35).

При правильном заполнении полей для ввода данных в окне реализации основных этапов протокола Фейге – Фиата – Шамира на экран выводится соответствующее информационное сообщение. На рисунке 37 в качестве примера показано информационное сообщение, появляющееся после правильного выполнения задания по вычислению модуля $n$ и секретного ключа $S$ для стороны А.

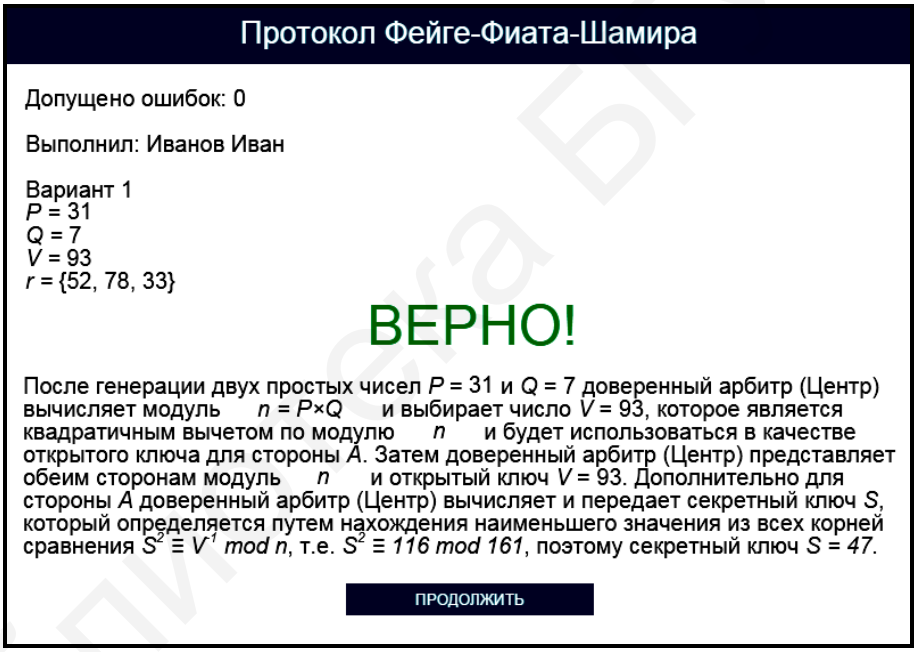



Рисунок 37 – Информационное сообщение программы, реализующей протокол Фейге – Фиата – Шамира

В правой верхней части окна реализации основных этапов протокола Фейге – Фиата – Шамира имеются три области, в которых указано допущенное количество ошибок, зарегистрированные пользовательские данные и загруженные исходные данные. При щелчке на области, в которой указано допущенное количество ошибок, появляется окно с промежуточными результатами выполнения задания, приведенное на рисунке 38.

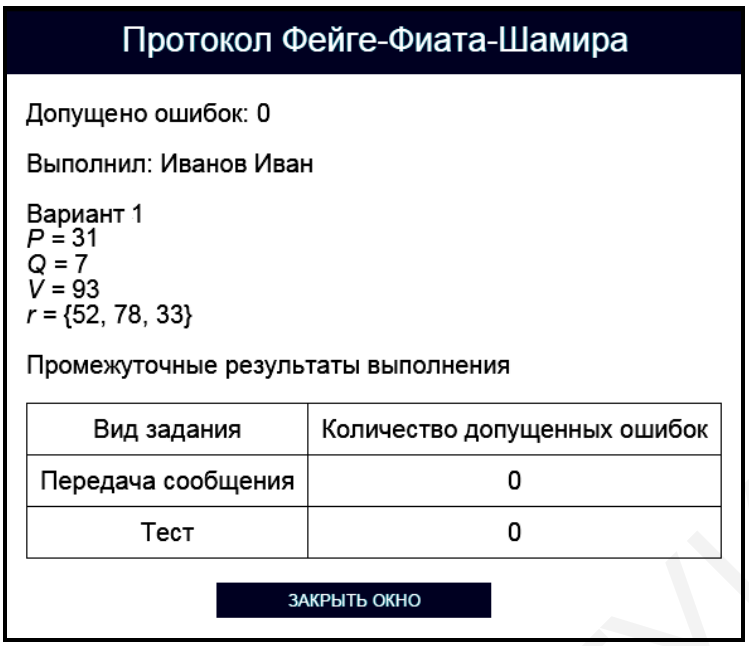



Рисунок 38 – Окно с промежуточными результатами выполнения задания программы, реализующей протокол Фейге – Фиата – Шамира

Для возврата в окно реализации основных этапов протокола Фейге – Фиата – Шамира необходимо нажать кнопку «Закрыть окно».

При щелчке на области, в которой указаны загруженные исходные данные, появляется окно подтверждения смены индивидуального задания (см. рисунок 10). Для изменения условия индивидуального задания необходимо щелкнуть на гиперссылке «Подтвердить выход», для возврата в окно реализации основных этапов протокола Фейге – Фиата – Шамира – на гиперссылке «Отмена».

Выход в главное окно программы (см. рисунок 32) обеспечивается нажатием кнопки «Выход в главное меню» (см. рисунок 35). При этом появляется окно подтверждения выхода в главное окно программы (см. рисунок 11). Для выхода в главное окно программы необходимо щелкнуть на гиперссылке «Подтвердить выход», для возврата в окно реализации основных этапов протокола Фейге – Фиата – Шамира – на гиперссылке «Отмена».

Задание по передаче конфиденциальной информации с использованием протокола Фейге – Фиата – Шамира считается выполненным, если все предлагаемые задания завершены успешно.

8.2.3 После выполнения заданий по передаче конфиденциальной информации с использованием протокола Фейге – Фиата – Шамира заполните таблицу 14.

Таблица 14 – Результаты исследования работы криптосистемы, функционирующей на базе протокола Фейге – Фиата – Шамира

| Номер шага (этапа) реализации | Наименование | Описание работы криптосистемы |
|---|---|---|
| | | |

*Примечание – Числа указывать в десятичной системе счисления.*

8.2.4 Выполните тестовые задания.

Для выполнения тестовых заданий необходимо в главном окне программы (см. рисунок 32) нажать кнопку «Тест» и в появившемся окне, показанном на рисунке 39, ознакомиться с инструкцией и нажать кнопку «Начать тест».

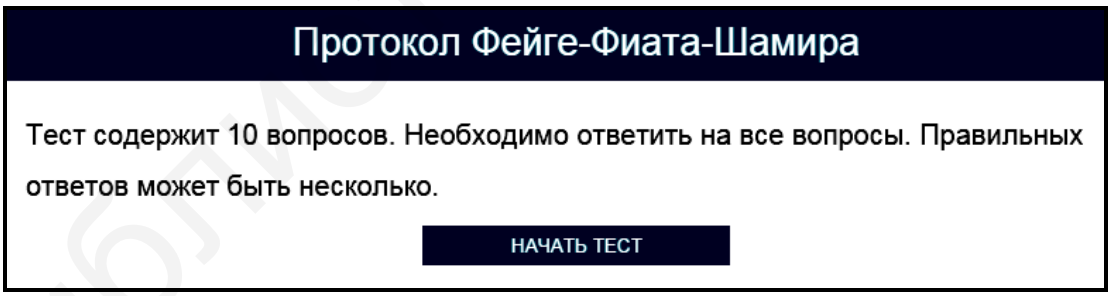



Рисунок 39 – Окно с инструкцией по выполнению тестовых заданий программы, реализующей протокол Фейге – Фиата – Шамира

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

8.2.5 По результатам выполнения тестового задания заполните таблицу 15.

Таблица 15 – Результаты выполнения тестового задания 8.2.4

| Вопрос | Правильный ответ |
|---|---|
| | |

*Примечание – Числа указывать в десятичной системе счисления.*

Лабораторное задание считается выполненным, если все предлагаемые задания завершены успешно. При этом на экран выводится окно, показанное на рисунке 40, а.

Лабораторное задание считается не выполненным, если на экран выводится окно, показанное на рисунке 40, б. В этом случае необходимо нажать кнопку «Выполнить еще раз» и заново выполнить пункты 8.2.1 … 8.2.5.

8.2.6 Продемонстрируйте выполнение практического задания преподавателю дисциплины.

### 8.3 Содержание отчета

1 Цель лабораторной работы.

2 Временные диаграммы, поясняющие выполнение 10 шагов протокола Фейге – Фиата – Шамира при реализации трех аккредитаций.

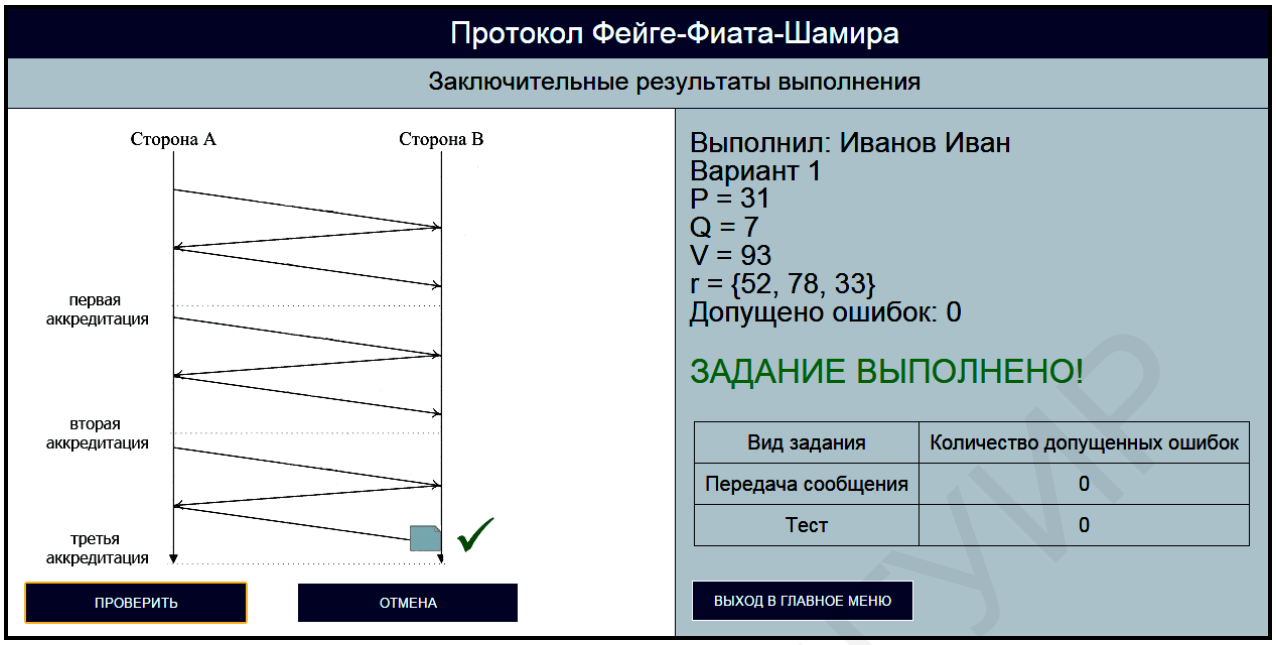
3 Условия выбора открытого и секретного ключей, используемых в протоколе Фейге – Фиата – Шамира.

4 Таблица с исходными данными, соответствующими индивидуальному варианту задания.

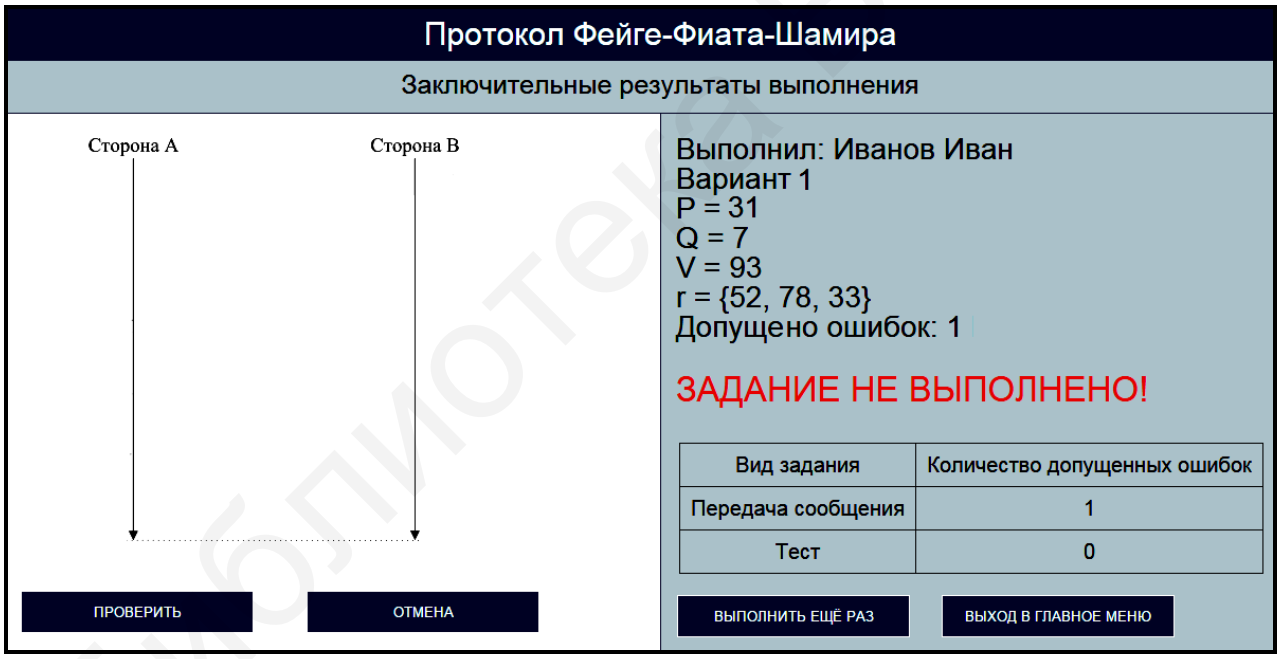
5 Таблицы с результатами выполнения задания.

6 Выводы по результатам выполнения задания.

7 Ответы на контрольные вопросы.




а




б

а – задание выполнено; б – задание не выполнено

Рисунок 40 – Окно с заключительными результатами выполнения задания программы, реализующей протокол Фейге – Фиата – Шамира

### 8.4 Контрольные вопросы

1 Каким образом реализуется идентификация объектов на основе протокола Фейге – Фиата – Шамира?

2 Какие требования необходимо выполнить для обеспечения высокого уровня информационной безопасности при реализации протокола Фейге – Фиата – Шамира?

3 Какую длину должен иметь модуль при реализации протокола Фейге – Фиата – Шамира?

4 Что называется аккредитацией?

5 Какое практическое применение находит протокол Фейге – Фиата – Шамира?

# ЛАБОРАТОРНАЯ РАБОТА №9
# ПРОТОКОЛ ПАРАЛЛЕЛЬНОЙ ИДЕНТИФИКАЦИИ С НУЛЕВОЙ ПЕРЕДАЧЕЙ ЗНАНИЙ

**Цель:** изучение протокола параллельной идентификации с нулевой передачей знаний, позволяющего выполнять идентификацию объектов на основе криптографических операций.

## 9.1 Краткие теоретические сведения

Для ознакомления с краткими теоретическими сведениями включите персональный компьютер и запустите файл «lr9_Parallel_identification_protocol.exe» на выполнение.

После запуска файла «lr9_Parallel_identification_protocol.exe» активизируется программное обеспечение, реализующее протокол параллельной идентификации с нулевой передачей знаний, и появится главное окно программы, показанное на рисунке 41.

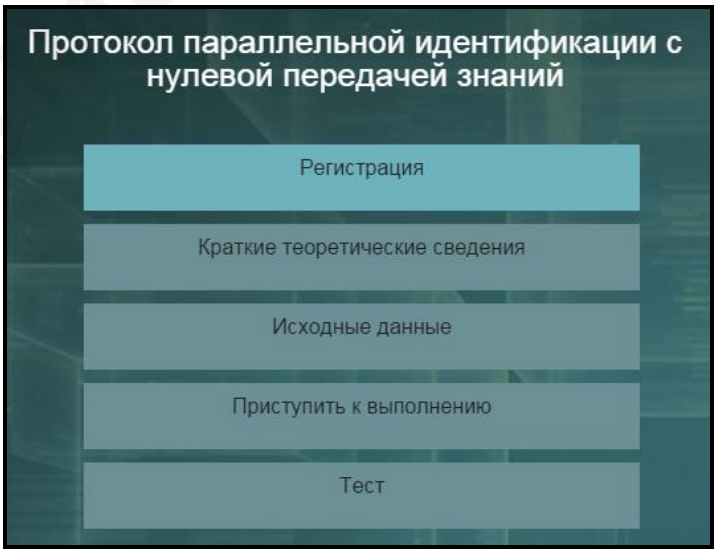



Рисунок 41 – Главное окно программы, реализующей протокол параллельной идентификации с нулевой передачей знаний

До начала работы с программой необходимо зарегистрироваться. Для этого требуется в главном окне программы нажать кнопку «Регистрация» и в появившемся окне регистрации, приведенном на рисунке 3, ввести в поле «Фамилия и имя» свою фамилию и имя, указать номер группы в поле «Номер группы» и нажать кнопку «Регистрация».

Затем необходимо в главном окне программы нажать кнопку «Краткие теоретические сведения», после чего на экран выводится окно с краткими теоретическими сведениями, показанное на рисунке 42.

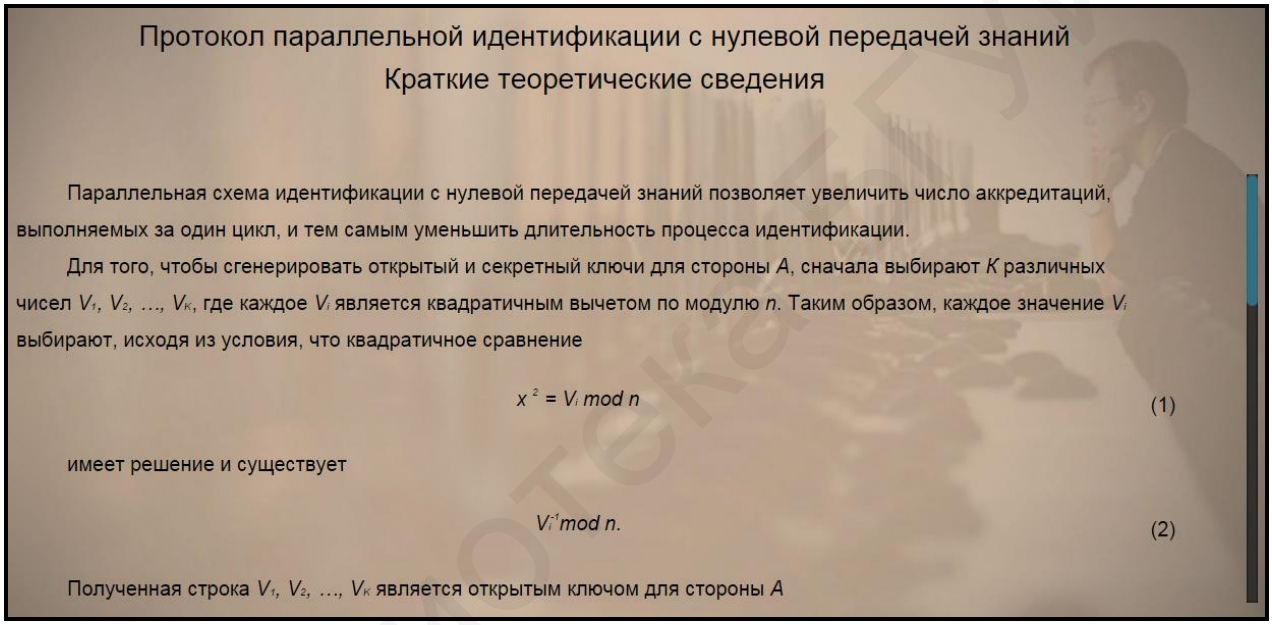



Рисунок 42 – Внешний вид окна с краткими теоретическими сведениями по алгоритму идентификации объектов на основе протокола параллельной идентификации с нулевой передачей знаний

## 9.2 Практическое задание

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

Для загрузки исходных данных необходимо в главном окне программы (см. рисунок 41) нажать кнопку «Исходные данные» и в появившемся окне вво-

да и загрузки исходных данных, приведенном на рисунке 43, ввести исходные данные в соответствии с индивидуальным вариантом и нажать кнопку «Загрузить исходные данные».

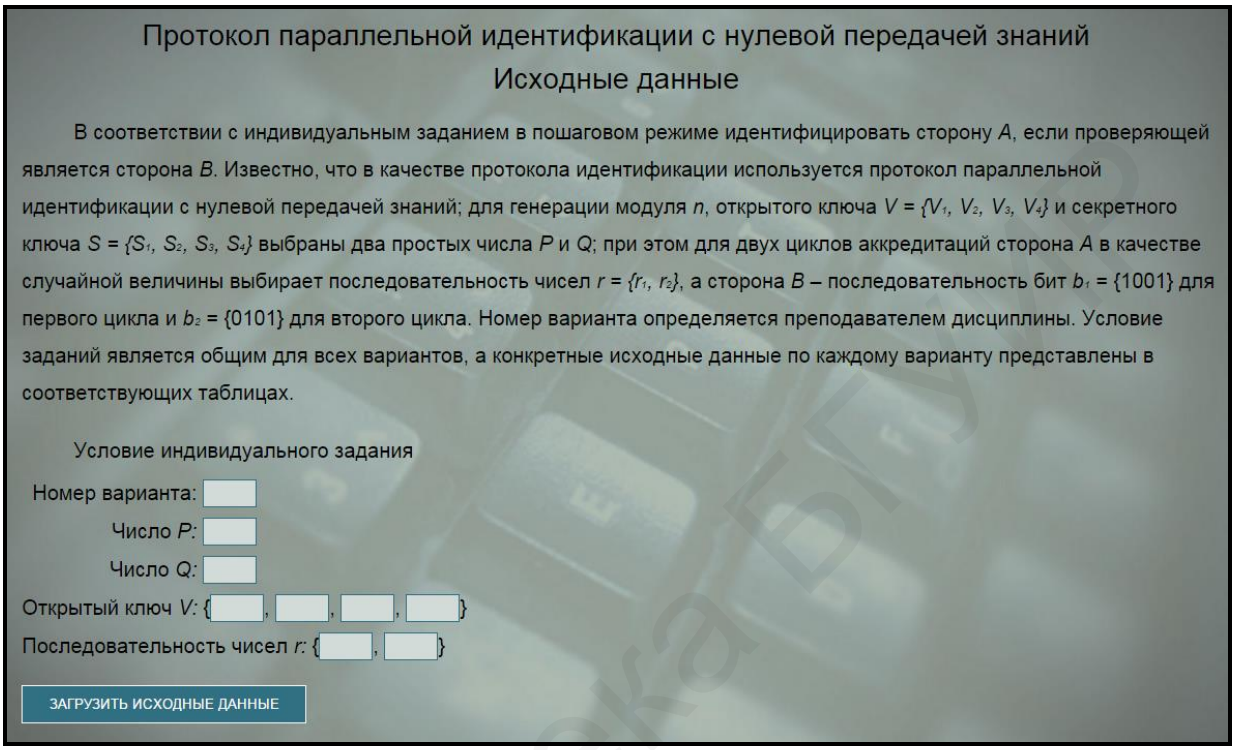



Рисунок 43 – Внешний вид окна ввода и загрузки исходных данных программы, реализующей протокол параллельной идентификации с нулевой передачей знаний

9.2.2 Выполните предлагаемые задания по передаче конфиденциальной информации с использованием протокола параллельной идентификации с нулевой передачей знаний.

Выполнение заданий по передаче конфиденциальной информации заключается в последовательной реализации протокола параллельной идентификации с нулевой передачей знаний, заполнении и анализе таблицы с полученными результатами. Условие заданий является общим для всех вариантов, а конкретные исходные данные определяются вариантом индивидуального задания.

Для выполнения заданий необходимо в главном окне программы (см. рисунок 41) нажать кнопку «Приступить к выполнению» и в появившемся окне реализации основных этапов протокола параллельной идентификации с нулевой передачей знаний, приведенном на рисунке 44, заполнить поля для ввода данных, располагающиеся в левой нижней его части, и нажать кнопку «Проверить».


Рисунок 44 – Внешний вид окна реализации основных этапов протокола параллельной идентификации с нулевой передачей знаний

Если одно или несколько полей для ввода данных не соответствуют заданию, указанному в верхней области окна реализации основных этапов протокола параллельной идентификации с нулевой передачей знаний, на экран выводится сообщение об ошибке, показанное на рисунке 45.

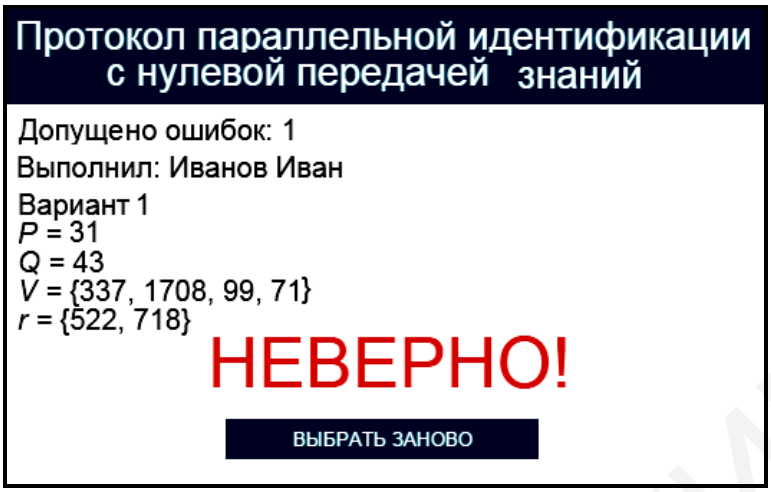



Рисунок 45 – Сообщение об ошибке реализации основных этапов протокола параллельной идентификации с нулевой передачей знаний

В этом случае необходимо нажать кнопку «Выбрать заново» и повторно заполнить поля для ввода данных в окне реализации основных этапов протокола параллельной идентификации с нулевой передачей знаний (см. рисунок 44).

При правильном заполнении полей для ввода данных в окне реализации основных этапов протокола параллельной идентификации с нулевой передачей знаний на экран выводится соответствующее информационное сообщение. На рисунке 46 в качестве примера показано информационное сообщение, появляющееся после правильного выполнения задания по вычислению модуля $n$ и символа $S_1$ секретного ключа для стороны А.

В правой верхней части окна реализации основных этапов протокола параллельной идентификации с нулевой передачей знаний имеются три области, в которых указано допущенное количество ошибок, зарегистрированные пользовательские данные и загруженные исходные данные. При щелчке на области, в которой указано допущенное количество ошибок, появляется окно с промежуточными результатами выполнения задания, приведенное на рисунке 47.

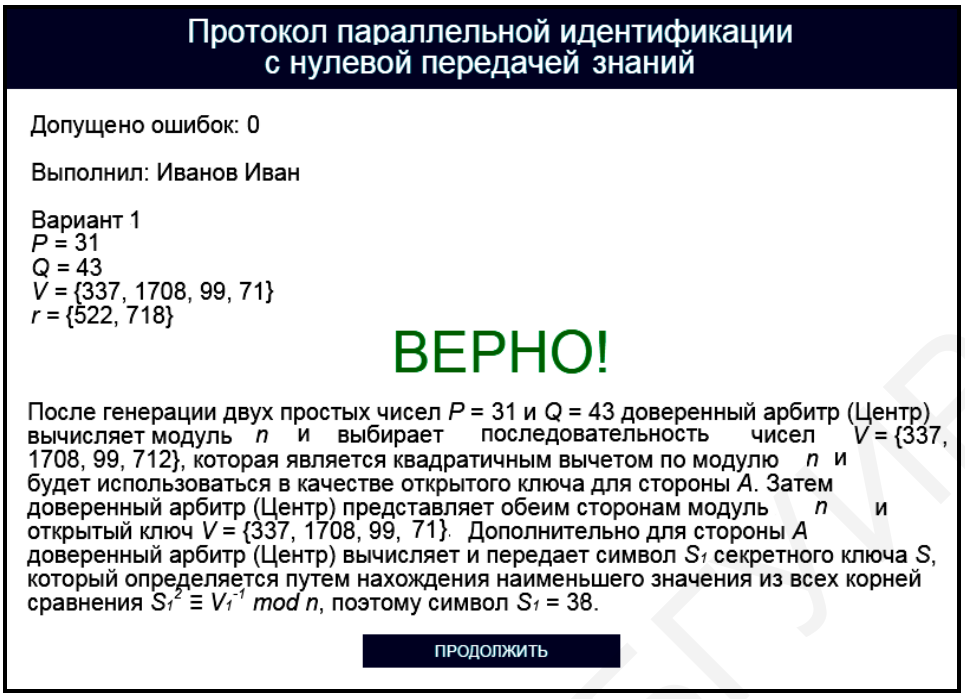



Рисунок 46 – Информационное сообщение программы, реализующей протокол параллельной идентификации с нулевой передачей знаний

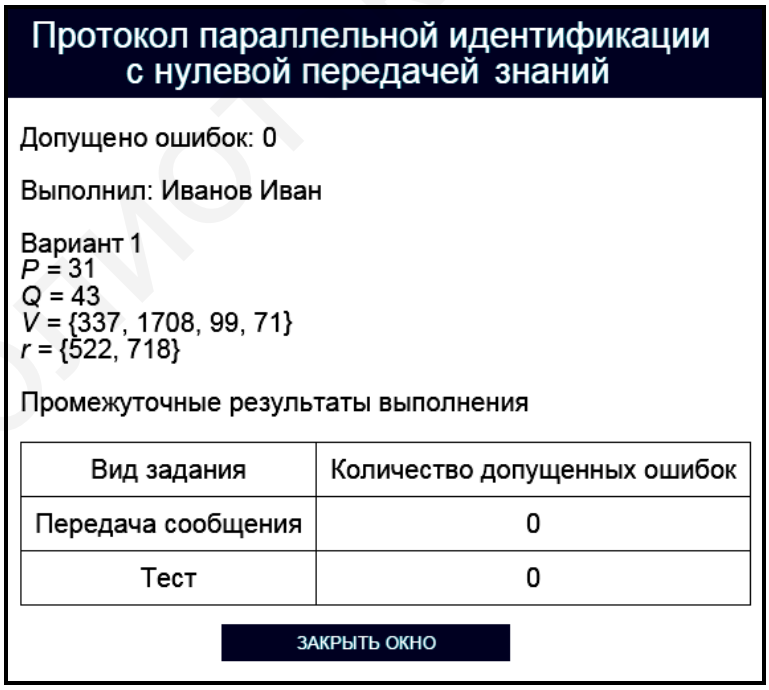



Рисунок 47 – Окно с промежуточными результатами выполнения задания программы, реализующей протокол параллельной идентификации с нулевой передачей знаний

Для возврата в окно реализации основных этапов протокола параллельной идентификации с нулевой передачей знаний необходимо нажать кнопку «Закрыть окно».

При щелчке на области, в которой указаны загруженные исходные данные, появляется окно подтверждения смены индивидуального задания (см. рисунок 10). Для изменения условия индивидуального задания необходимо щелкнуть на гиперссылке «Подтвердить выход», для возврата в окно реализации основных этапов протокола параллельной идентификации с нулевой передачей знаний – на гиперссылке «Отмена».

Выход в главное окно программы (см. рисунок 41) обеспечивается нажатием кнопки «Выход в главное меню» (см. рисунок 44). При этом появляется окно подтверждения выхода в главное окно программы (см. рисунок 11). Для выхода в главное окно программы необходимо щелкнуть на гиперссылке «Подтвердить выход», для возврата в окно реализации основных этапов протокола параллельной идентификации с нулевой передачей знаний – на гиперссылке «Отмена».

Задание по передаче конфиденциальной информации с использованием протокола параллельной идентификации с нулевой передачей знаний считается выполненным, если все предлагаемые задания завершены успешно.

9.2.3 После выполнения заданий по передаче конфиденциальной информации с использованием протокола параллельной идентификации с нулевой передачей знаний заполните таблицу 16.

Таблица 16 – Результаты исследования работы криптосистемы, функционирующей на базе протокола параллельной идентификации с нулевой передачей знаний

| Номер шага (этапа) реализации | Наименование | Описание работы криптосистемы |
|---|---|---|
| | | |

*Примечание – Числа указывать в десятичной системе счисления.*

9.2.4 Выполните тестовые задания.

Для выполнения тестовых заданий необходимо в главном окне программы (см. рисунок 41) нажать кнопку «Тест» и в появившемся окне, показанном на рисунке 48, ознакомиться с инструкцией и нажать кнопку «Начать тест».


Рисунок 48 – Окно с инструкцией по выполнению тестовых заданий программы, реализующей протокол параллельной идентификации с нулевой передачей знаний

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

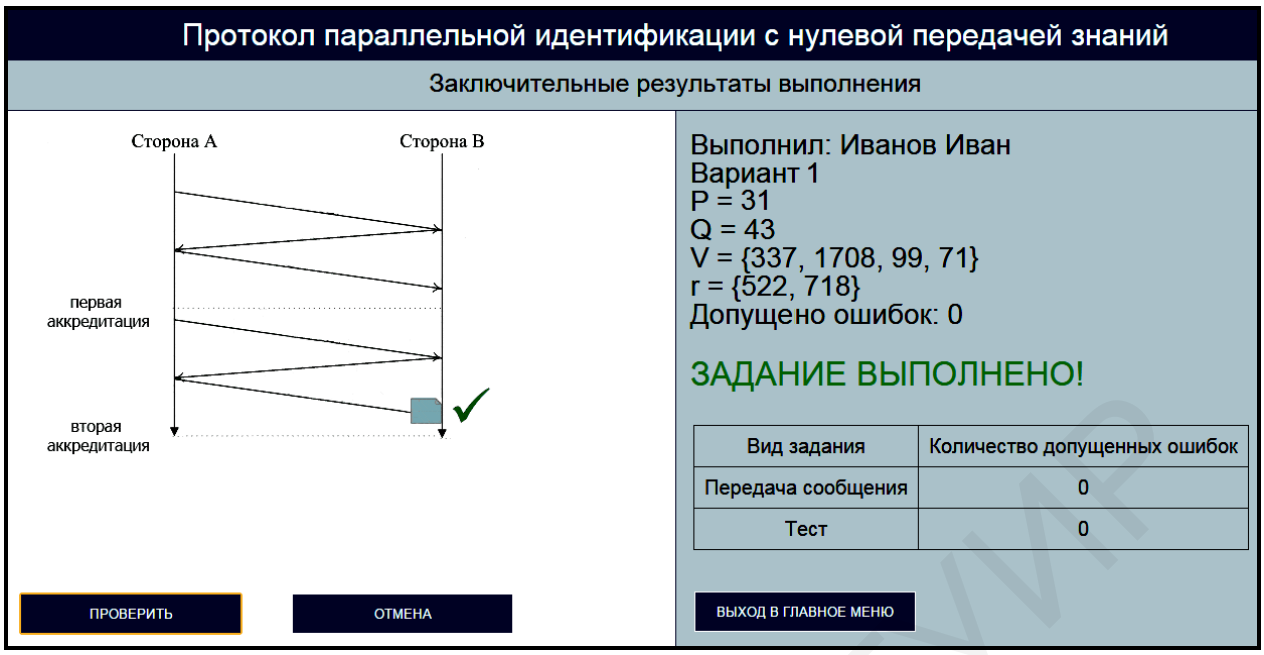
9.2.5 По результатам выполнения тестового задания заполните таблицу 17.

Таблица 17 – Результаты выполнения тестового задания 9.2.4

| Вопрос | Правильный ответ |
|---|---|
| | |

*Примечание – Числа указывать в десятичной системе счисления.*

Лабораторное задание считается выполненным, если все предлагаемые задания завершены успешно. При этом на экран выводится окно, показанное на рисунке 49, а.




а


б

а – задание выполнено; б – задание не выполнено

Рисунок 49 – Окно с заключительными результатами выполнения задания программы, реализующей протокол параллельной идентификации с нулевой передачей знаний

Лабораторное задание считается не выполненным, если на экран выводится окно, показанное на рисунке 49, б. В этом случае необходимо нажать кнопку «Выполнить еще раз» и заново выполнить пункты 9.2.1 … 9.2.5.

9.2.6 Продемонстрируйте выполнение практического задания преподавателю дисциплины.

### 9.3 Содержание отчета

1 Цель лабораторной работы.

2 Временные диаграммы, поясняющие выполнение шага 9 протокола параллельной идентификации с нулевой передачей знаний при реализации двух аккредитаций.

3 Условия выбора открытого и секретного ключей, используемых в протоколе параллельной идентификации с нулевой передачей знаний.

4 Таблица с исходными данными, соответствующими индивидуальному варианту задания.

5 Таблицы с результатами выполнения задания.

6 Выводы по результатам выполнения задания.

7 Ответы на контрольные вопросы.

### 9.4 Контрольные вопросы

1 Каким образом реализуется идентификация объектов на основе протокола параллельной идентификации с нулевой передачей знаний?

2 Какие требования необходимо выполнить для обеспечения высокого уровня информационной безопасности при реализации протокола параллельной идентификации с нулевой передачей знаний?

3 Какую длину должен иметь модуль при реализации протокола параллельной идентификации с нулевой передачей знаний?

4 Какие преимущества имеет криптографическая система на базе протокола параллельной идентификации с нулевой передачей знаний в сравнении с криптосистемами, в которых применяется протокол Фейге – Фиата – Шамира?

5 Какое практическое применение находит протокол параллельной идентификации с нулевой передачей знаний?

# ЛАБОРАТОРНАЯ РАБОТА №10
# ПРОТОКОЛ ИДЕНТИФИКАЦИИ ГИЛЛОУ – КУИСКУОТЕРА

**Цель:** изучение протокола идентификации Гиллоу – Куискуотера, позволяющего выполнять идентификацию объектов на основе криптографических операций.

## 10.1 Краткие теоретические сведения

Для ознакомления с краткими теоретическими сведениями включите персональный компьютер и запустите файл «lr10_Protocol_Gillow-Cookswater_exe» на выполнение.

После запуска файла «lr10_Protocol_Gillow-Cookswater_exe» активизируется программное обеспечение, реализующее протокол идентификации Гиллоу – Куискуотера, и появится главное окно программы, показанное на рисунке 50.

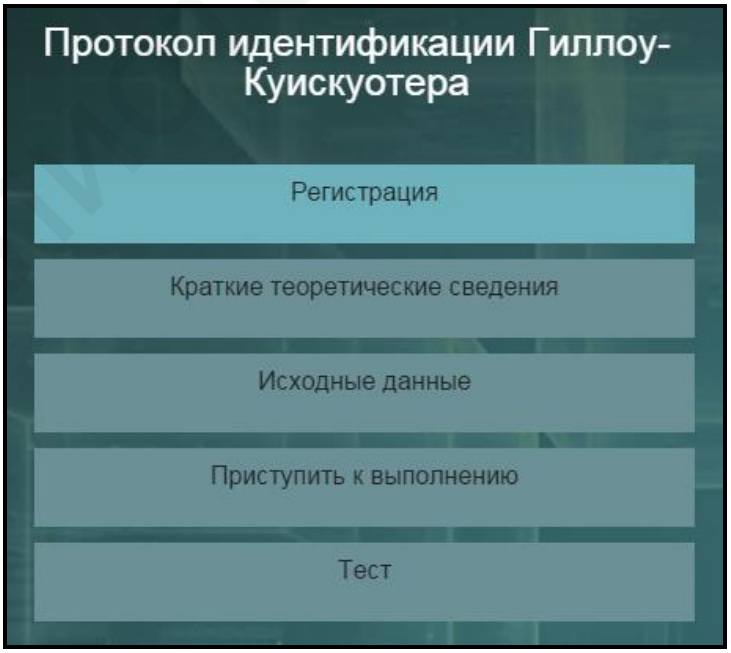



Рисунок 50 – Главное окно программы, реализующей протокол идентификации Гиллоу – Куискуотера

До начала работы с программой необходимо зарегистрироваться. Для этого требуется в главном окне программы нажать кнопку «Регистрация» и в появившемся окне регистрации, приведенном на рисунке 3, ввести в поле «Фамилия и имя» свою фамилию и имя, указать номер группы в поле «Номер группы» и нажать кнопку «Регистрация».

Затем необходимо в главном окне программы нажать кнопку «Краткие теоретические сведения», после чего на экран выводится окно с краткими теоретическими сведениями, показанное на рисунке 51.

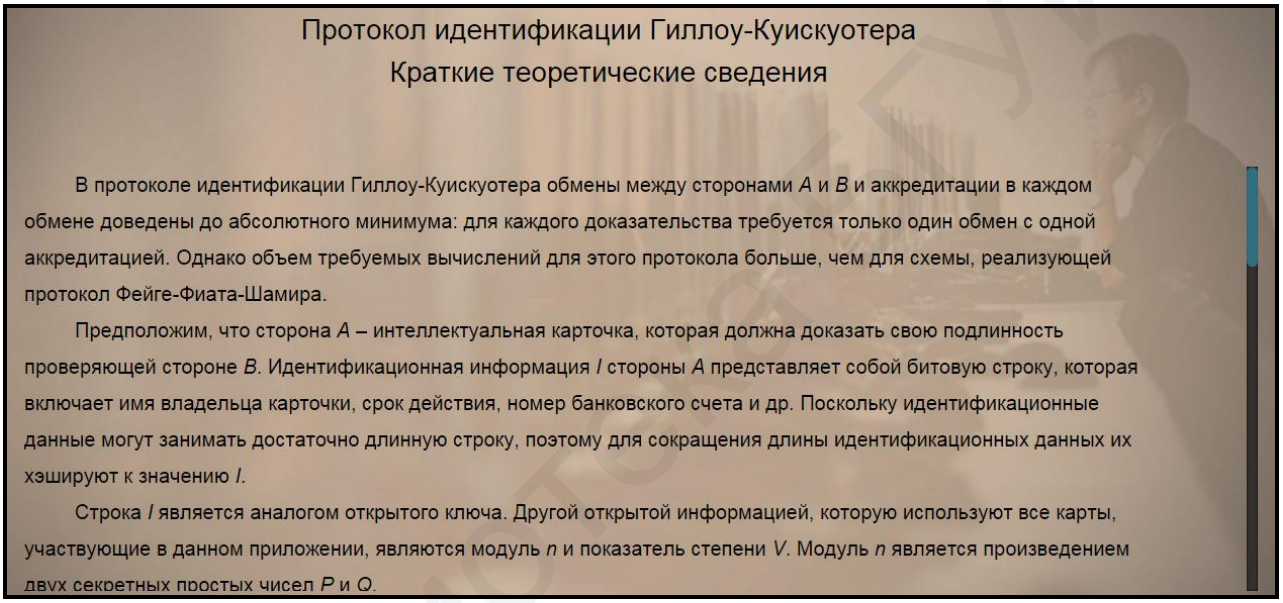



Рисунок 51 – Внешний вид окна с краткими теоретическими сведениями по реализации протокола Гиллоу – Куискуотера

### 10.2 Практическое задание

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

Для загрузки исходных данных необходимо в главном окне программы (см. рисунок 50) нажать кнопку «Исходные данные» и в появившемся окне ввода и загрузки исходных данных, приведенном на рисунке 52, ввести исходные

данные в соответствии с индивидуальным вариантом и нажать кнопку «Загрузить исходные данные».

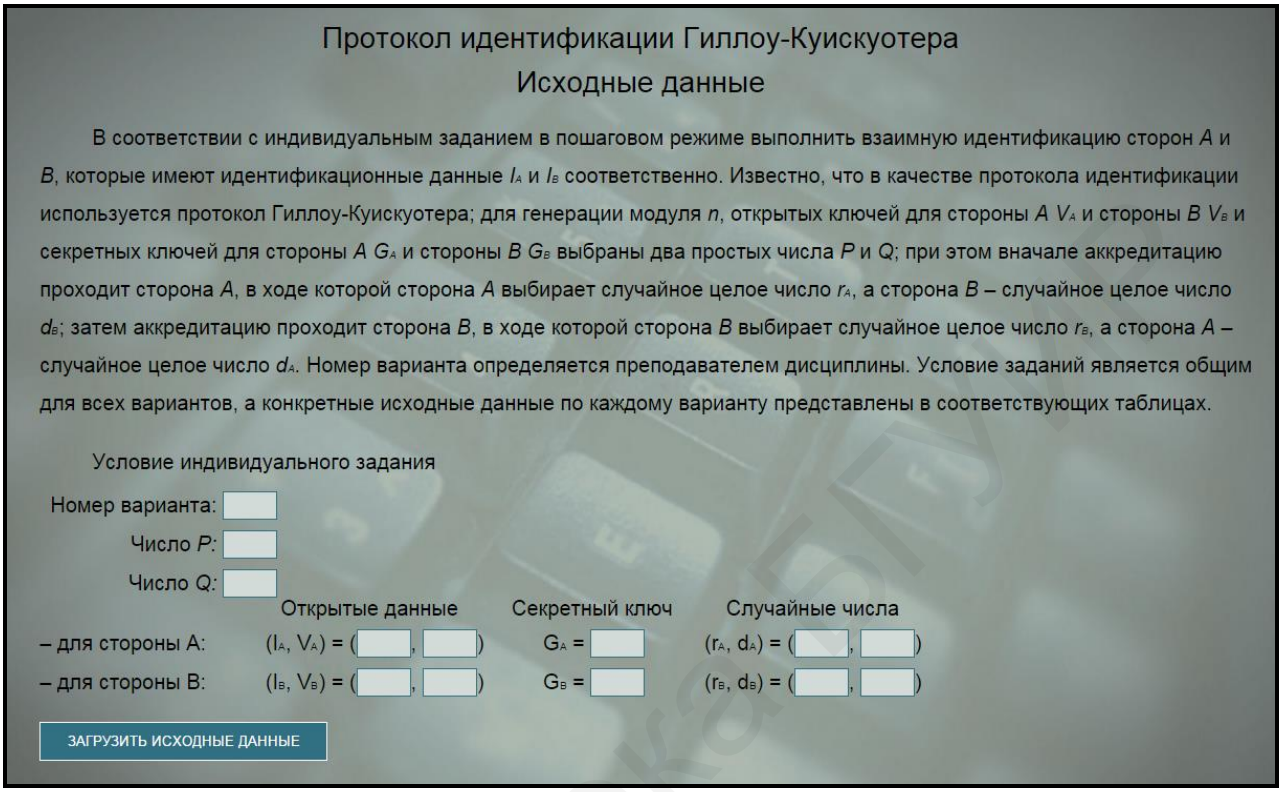



Рисунок 52 – Внешний вид окна ввода и загрузки исходных данных программы, реализующей протокол Гиллоу – Куискуотера

10.2.2 Выполните предлагаемые задания по передаче конфиденциальной информации с использованием протокола идентификации Гиллоу – Куискуотера.

Выполнение заданий по передаче конфиденциальной информации заключается в последовательной реализации протокола идентификации Гиллоу – Куискуотера, заполнении и анализе таблицы с полученными результатами. Условие заданий является общим для всех вариантов, а конкретные исходные данные определяются вариантом индивидуального задания.

Для выполнения заданий необходимо в главном окне программы (см. рисунок 50) нажать кнопку «Приступить к выполнению» и в появившемся окне реализации основных этапов протокола идентификации Гиллоу – Куиску-

отера, приведенном на рисунке 53, заполнить поля для ввода данных, располагающиеся в левой нижней его части, и нажать кнопку «Проверить».

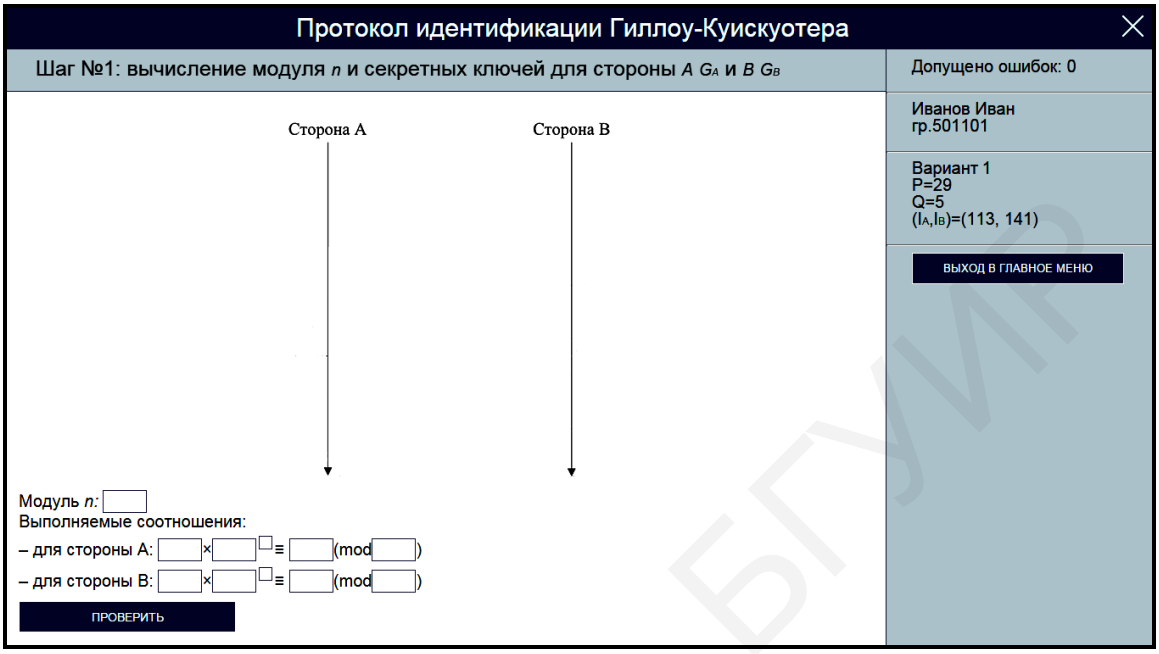



Рисунок 53 – Внешний вид окна реализации основных этапов протокола идентификации Гиллоу – Куискуотера

Если одно или несколько полей для ввода данных не соответствуют заданию, указанному в верхней области окна реализации основных этапов протокола идентификации Гиллоу – Куискуотера, на экран выводится сообщение об ошибке, показанное на рисунке 54.

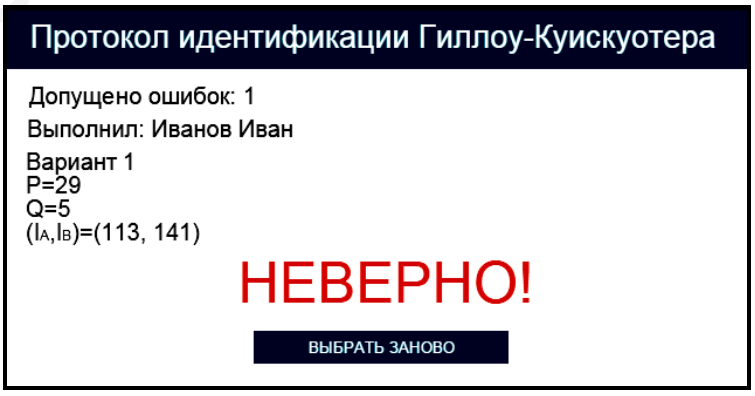



Рисунок 54 – Сообщение об ошибке реализации основных этапов протокола идентификации объектов Гиллоу – Куискуотера

В этом случае необходимо нажать кнопку «Выбрать заново» и повторно заполнить поля для ввода данных в окне реализации основных этапов протокола идентификации Гиллоу – Куискуотера (см. рисунок 50).

При правильном заполнении полей для ввода данных в окне реализации основных этапов протокола идентификации Гиллоу – Куискуотера на экран выводится соответствующее информационное сообщение. На рисунке 55 в качестве примера показано информационное сообщение, появляющееся после правильного выполнения задания по вычислению модуля $n$ и секретных ключей: $G_A$ – для стороны A и $G_B$ – для стороны B.

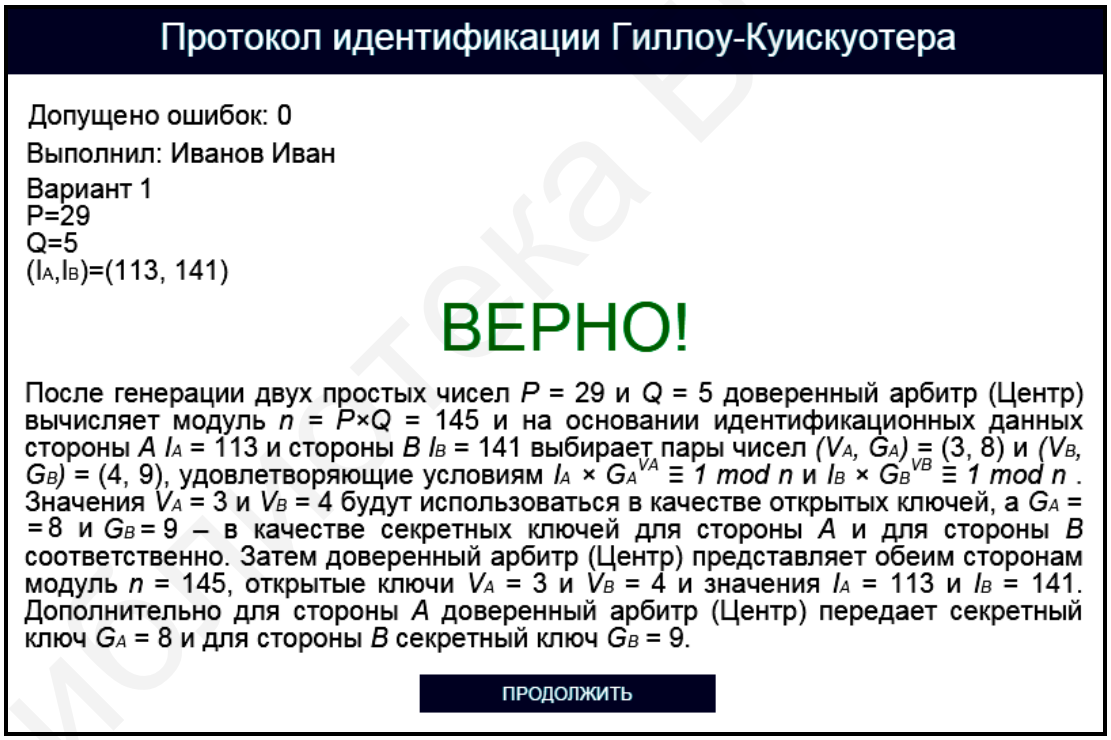



Рисунок 55 – Информационное сообщение программы, реализующей протокол идентификации объектов Гиллоу – Куискуотера

В правой верхней части окна реализации основных этапов протокола идентификации Гиллоу – Куискуотера имеются три области, в которых указано допущенное количество ошибок, зарегистрированные пользовательские данные

и загруженные исходные данные. При щелчке на области, в которой указано допущенное количество ошибок, появляется окно с промежуточными результатами выполнения задания, приведенное на рисунке 56.

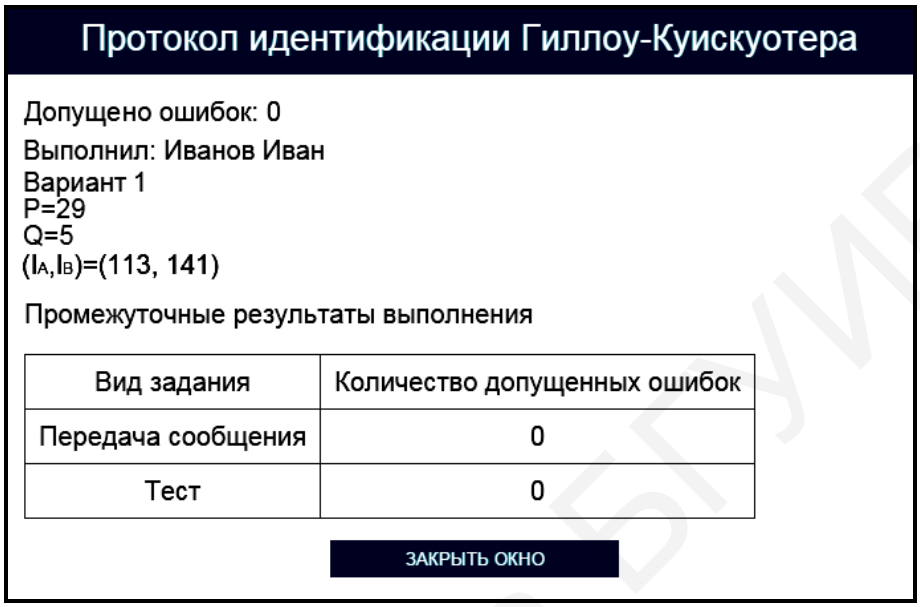



Рисунок 56 – Окно с промежуточными результатами выполнения задания программы, реализующей протокол идентификации объектов Гиллоу – Куискуотера

Для возврата в окно реализации основных этапов протокола идентификации Гиллоу – Куискуотера необходимо нажать кнопку «Закрыть окно».

При щелчке на области, в которой указаны загруженные исходные данные, появляется окно подтверждения смены индивидуального задания (см. рисунок 10). Для изменения условия индивидуального задания необходимо щелкнуть на гиперссылке «Подтвердить выход», для возврата в окно реализации основных этапов протокола идентификации Гиллоу – Куискуотера – на гиперссылке «Отмена».

Выход в главное окно программы (см. рисунок 50) обеспечивается нажатием кнопки «Выход в главное меню» (см. рисунок 53). При этом появляется окно подтверждения выхода в главное окно программы (см. рисунок 11). Для выхода в главное окно программы необходимо щелкнуть на гиперссылке

«Подтвердить выход», для возврата в окно реализации основных этапов протокола идентификации Гиллоу – Куискуотера – на гиперссылке «Отмена».

Задание по передаче конфиденциальной информации с использованием протокола идентификации Гиллоу – Куискуотера считается выполненным, если все предлагаемые задания завершены успешно.

10.2.3 После выполнения заданий по передаче конфиденциальной информации с использованием протокола идентификации Гиллоу – Куискуотера заполните таблицу 18.

Таблица 18 – Результаты исследования работы криптосистемы, функционирующей на базе протокола Гиллоу – Куискуотера

| Номер шага (этапа) реализации | Наименование | Описание работы криптосистемы |
|---|---|---|
| | | |

*Примечание – Числа указывать в десятичной системе счисления.*

10.2.4 Выполните тестовые задания.

Для выполнения тестовых заданий необходимо в главном окне программы (см. рисунок 50) нажать кнопку «Тест» и в появившемся окне, показанном на рисунке 57, ознакомиться с инструкцией и нажать кнопку «Начать тест».

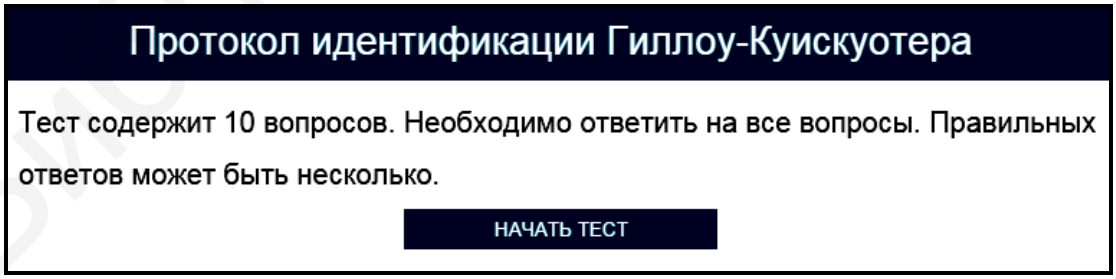



Рисунок 57 – Окно с инструкцией по выполнению тестовых заданий программы, реализующей протокол идентификации объектов Гиллоу – Куискуотера

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

10.2.5 По результатам выполнения тестового задания заполните таблицу 19.

Таблица 19 – Результаты выполнения тестового задания 10.2.4

| Вопрос | Правильный ответ |
|---|---|
| | |

*Примечание – Числа указывать в десятичной системе счисления.*

Лабораторное задание считается выполненным, если все предлагаемые задания завершены успешно. При этом на экран выводится окно, показанное на рисунке 58, а.

Лабораторное задание считается не выполненным, если на экран выводится окно, показанное на рисунке 58, б. В этом случае необходимо нажать кнопку «Выполнить еще раз» и заново выполнить пункты 10.2.1 … 10.2.5.

10.2.6 Продемонстрируйте выполнение практического задания преподавателю дисциплины.

### 10.3 Содержание отчета

1 Цель лабораторной работы.

2 Временные диаграммы, поясняющие выполнение семи шагов протокола идентификации Гиллоу – Куискуотера.

3 Условия выбора открытого и секретного ключей, используемых в протоколе идентификации Гиллоу – Куискуотера.

4 Таблица с исходными данными, соответствующими индивидуальному варианту задания.

5 Таблицы с результатами выполнения задания.

6 Выводы по результатам выполнения задания.

7 Ответы на контрольные вопросы.


а


б

а – задание выполнено; б – задание не выполнено

Рисунок 58 – Окно с заключительными результатами выполнения задания программы, реализующей протокол идентификации объектов Гиллоу – Куискуотера

### 10.4 Контрольные вопросы

1 Каким образом реализуется идентификация объектов на основе протокола идентификации Гиллоу – Куискуотера?

2 Какие требования необходимо выполнить для обеспечения высокого уровня информационной безопасности при реализации протокола идентификации Гиллоу – Куискуотера?

3 Какую длину должен иметь модуль при реализации протокола идентификации Гиллоу – Куискуотера?

4 Какие преимущества имеет криптографическая система на базе протокола идентификации Гиллоу – Куискуотера в сравнении с криптосистемами, в которых применяется протокол Фейге – Фиата – Шамира или протокол параллельной идентификации с нулевой передачей знаний?

5 Какое практическое применение находит протокол идентификации Гиллоу – Куискуотера?

# ЛАБОРАТОРНАЯ РАБОТА №11
# АЛГОРИТМ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ RSA

**Цель:** изучение алгоритма электронной цифровой подписи RSA, позволяющего выполнять аутентификацию электронных документов и их авторов.

## 11.1 Краткие теоретические сведения

Для ознакомления с краткими теоретическими сведениями включите персональный компьютер и запустите файл «lr11_EDS_RSA_exe» на выполнение.

После запуска файла «lr11_EDS_RSA_exe» активизируется программное обеспечение, реализующее алгоритм электронной цифровой подписи RSA, и появится главное окно программы, показанное на рисунке 59.

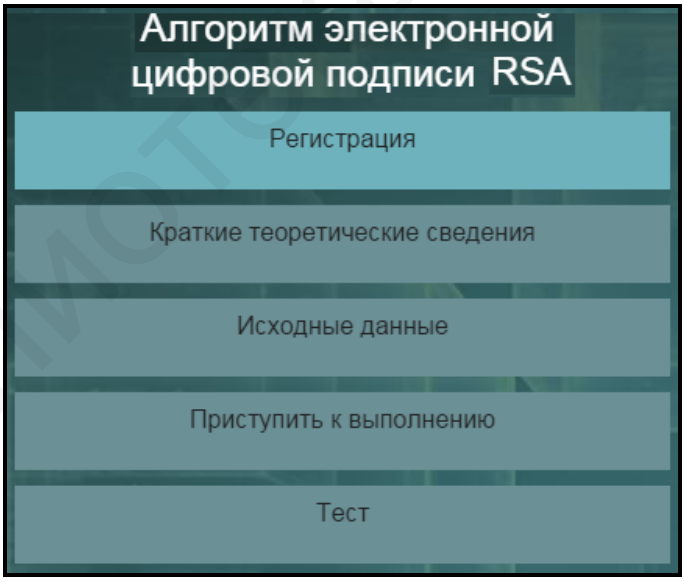



Рисунок 59 – Главное окно программы, реализующей алгоритм электронной цифровой подписи RSA

До начала работы с программой необходимо зарегистрироваться. Для этого требуется в главном окне программы нажать кнопку «Регистрация» и в появившемся окне регистрации, приведенном на рисунке 3, ввести в поле «Фамилия и имя» свою фамилию и имя, указать номер группы в поле «Номер группы» и нажать кнопку «Регистрация».

Затем необходимо в главном окне программы нажать кнопку «Краткие теоретические сведения», после чего на экран выводится окно с краткими теоретическими сведениями, показанное на рисунке 60.

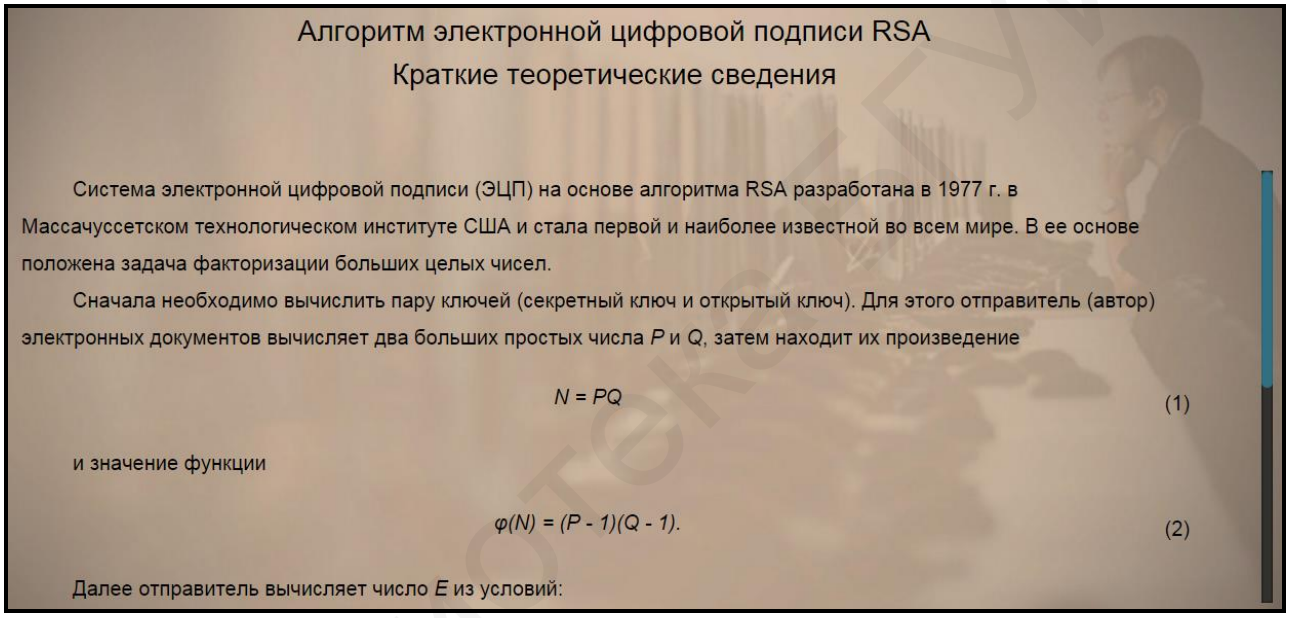



Рисунок 60 – Внешний вид окна с краткими теоретическими сведениями по алгоритму электронной цифровой подписи RSA

### 11.2 Практическое задание

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

Для загрузки исходных данных необходимо в главном окне программы (см. рисунок 59) нажать кнопку «Исходные данные» и в появившемся окне ввода и загрузки исходных данных, приведенном на рисунке 61, ввести исходные

данные в соответствии с индивидуальным вариантом и нажать кнопку «Загрузить исходные данные».

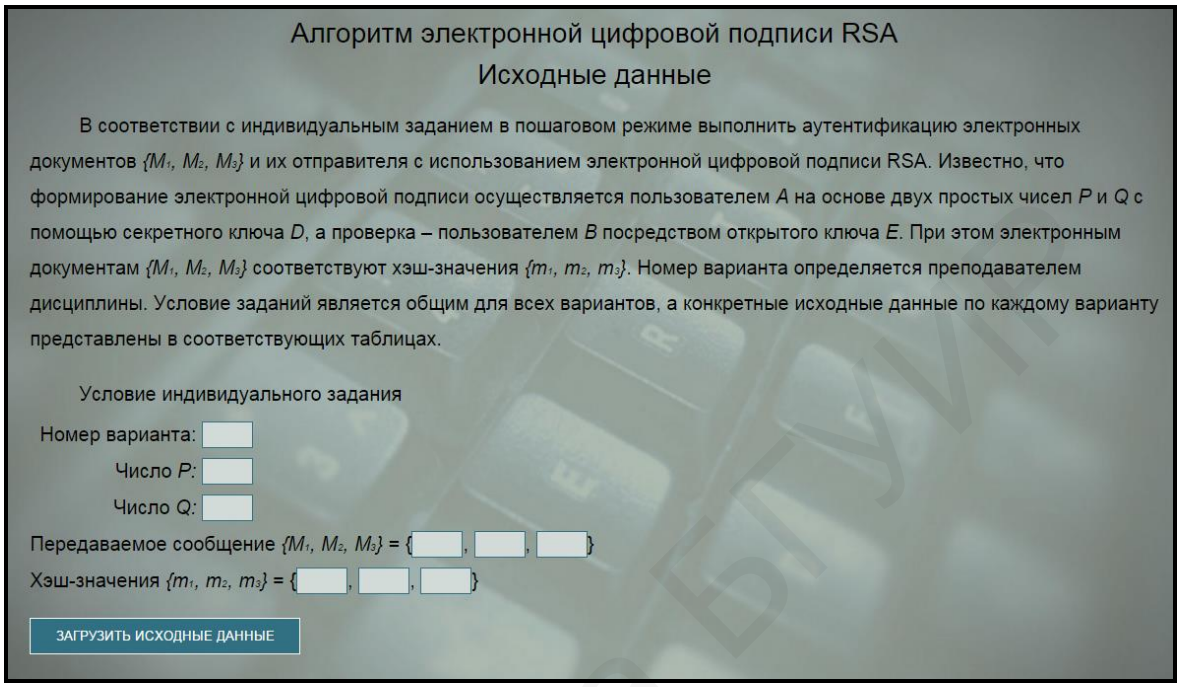



Рисунок 61 – Внешний вид окна ввода и загрузки исходных данных программы, реализующей алгоритм электронной цифровой подписи RSA

11.2.2 Выполните предлагаемые задания по передаче сообщения с использованием алгоритма электронной цифровой подписи RSA.

Выполнение заданий по передаче сообщения заключается в последовательной реализации алгоритма электронной цифровой подписи RSA, заполнении и анализе таблицы с полученными результатами. Условие заданий является общим для всех вариантов, а конкретные исходные данные определяются вариантом индивидуального задания.

Для выполнения заданий необходимо в главном окне программы (см. рисунок 59) нажать кнопку «Приступить к выполнению» и в появившемся окне реализации основных этапов алгоритма электронной цифровой подписи RSA, приведенном на рисунке 62, заполнить поля для ввода данных, располагающиеся в левой нижней его части, и нажать кнопку «Проверить».


Рисунок 62 – Внешний вид окна реализации основных этапов алгоритма электронной цифровой подписи RSA

Если одно или несколько полей для ввода данных не соответствуют заданию, указанному в верхней области окна реализации основных этапов алгоритма электронной цифровой подписи RSA, на экран выводится сообщение об ошибке, показанное на рисунке 63.

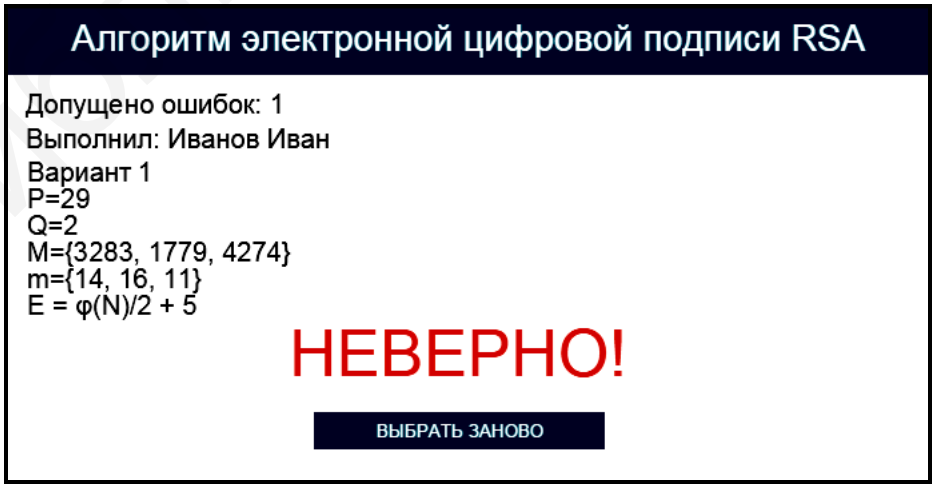



Рисунок 63 – Сообщение об ошибке реализации основных этапов алгоритма электронной цифровой подписи RSA

В этом случае необходимо нажать кнопку «Выбрать заново» и повторно заполнить поля для ввода данных в окне реализации основных этапов алгоритма электронной цифровой подписи RSA (см. рисунок 62).

При правильном заполнении полей для ввода данных в окне реализации основных этапов алгоритма электронной цифровой подписи RSA на экран выводится соответствующее информационное сообщение. На рисунке 64 в качестве примера показано информационное сообщение, появляющееся после правильного выполнения задания по вычислению модуля *N* и phi-функции Эйлера *φ(n)*.

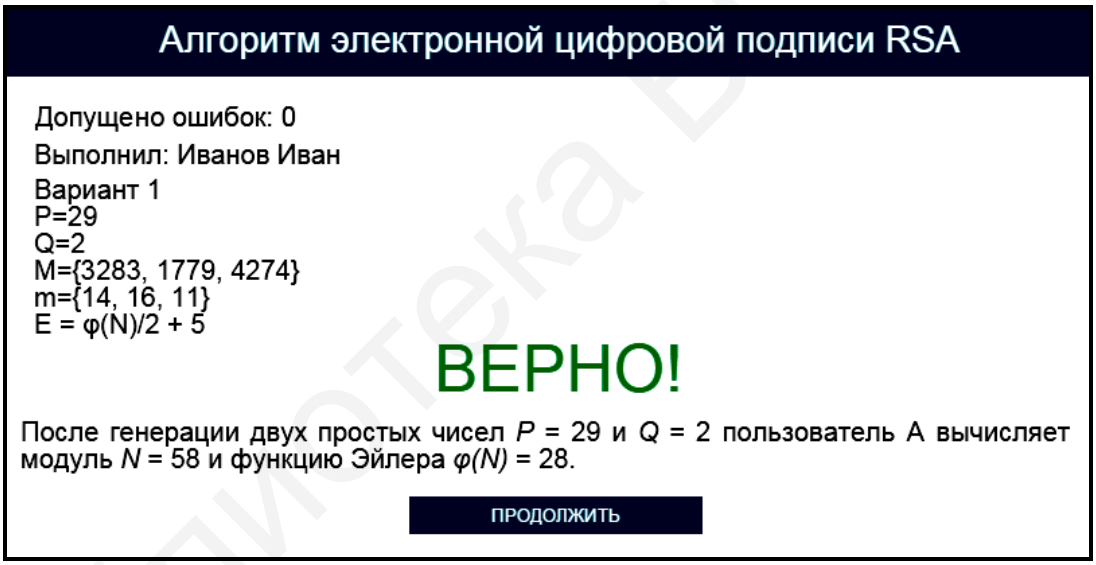



Рисунок 64 – Информационное сообщение программы, реализующей алгоритм электронной цифровой подписи RSA

В правой верхней части окна реализации основных этапов алгоритма электронной цифровой подписи RSA имеются три области, в которых указано допущенное количество ошибок, зарегистрированные пользовательские данные и загруженные исходные данные. При щелчке на области, в которой указано допущенное количество ошибок, появляется окно с промежуточными результатами выполнения задания, приведенное на рисунке 65.

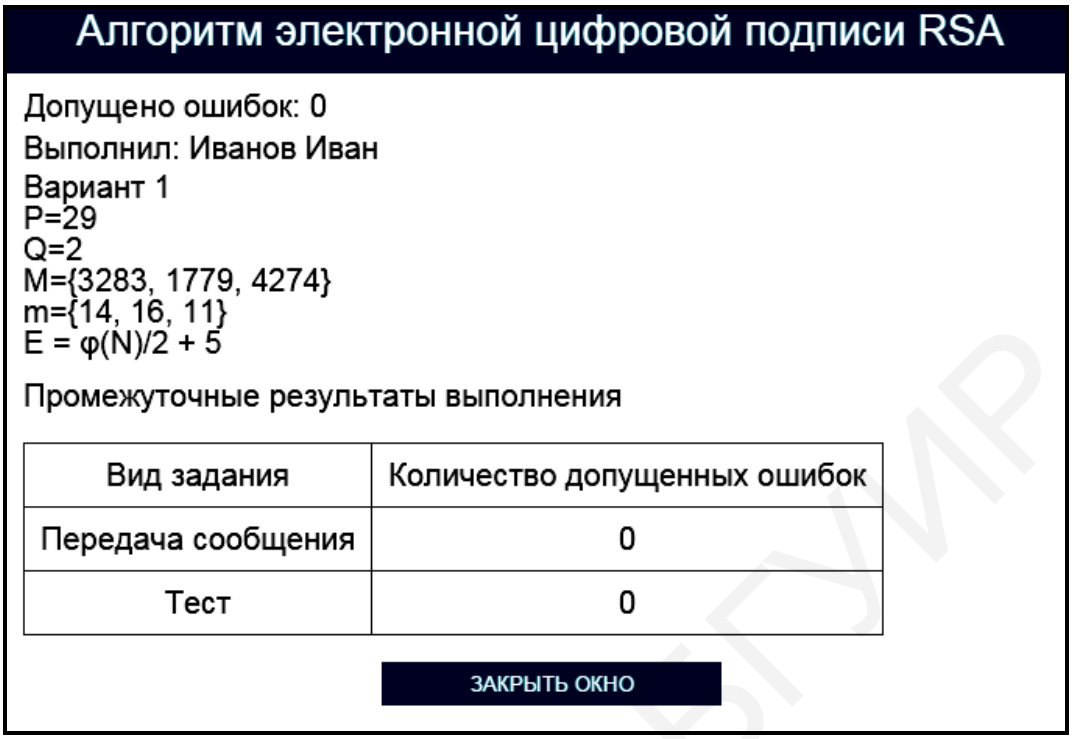



Рисунок 65 – Окно с промежуточными результатами выполнения задания программы, реализующей алгоритм электронной цифровой подписи RSA

Для возврата в окно реализации основных этапов алгоритма электронной цифровой подписи RSA необходимо нажать кнопку «Закрыть окно».

При щелчке на области, в которой указаны загруженные исходные данные, появляется окно подтверждения смены индивидуального задания (см. рисунок 10). Для изменения условия индивидуального задания необходимо щелкнуть на гиперссылке «Подтвердить выход», для возврата в окно реализации основных этапов алгоритма электронной цифровой подписи RSA – на гиперссылке «Отмена».

Выход в главное окно программы (см. рисунок 59) обеспечивается нажатием кнопки «Выход в главное меню» (см. рисунок 62). При этом появляется окно подтверждения выхода в главное окно программы (см. рисунок 11). Для выхода в главное окно программы необходимо щелкнуть на гиперссылке «Подтвердить выход», для возврата в окно реализации основных

этапов алгоритма электронной цифровой подписи RSA – на гиперссылке «Отмена».

Задание по передаче сообщения с использованием алгоритма электронной цифровой подписи RSA считается выполненным, если все предлагаемые задания завершены успешно.

11.2.3 После выполнения заданий по передаче сообщения с использованием алгоритма электронной цифровой подписи RSA заполните таблицу 20.

Таблица 20 – Результаты исследования работы криптосистемы, реализующей алгоритм электронной цифровой подписи RSA

| Номер шага (этапа) реализации | Наименование | Описание работы криптосистемы |
|---|---|---|
| | | |

*Примечание – Числа указывать в десятичной системе счисления.*

11.2.4 Выполните тестовые задания.

Для выполнения тестовых заданий необходимо в главном окне программы (см. рисунок 59) нажать кнопку «Тест» и в появившемся окне, показанном на рисунке 66, ознакомиться с инструкцией и нажать кнопку «Начать тест».

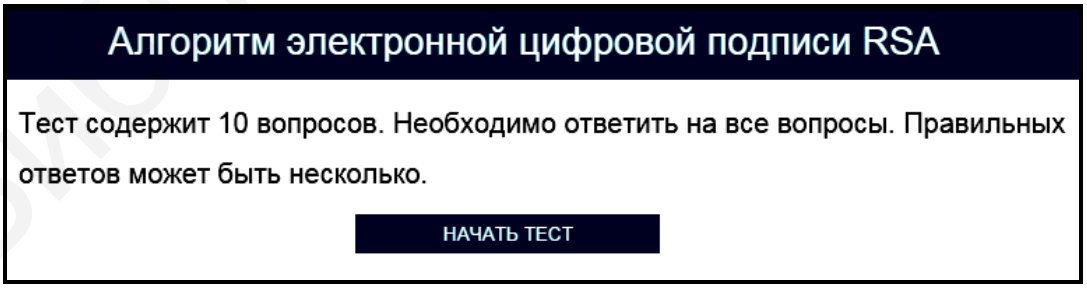



Рисунок 66 – Окно с инструкцией по выполнению тестовых заданий программы, реализующей алгоритм электронной цифровой подписи RSA

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

11.2.5 По результатам выполнения тестового задания заполните таблицу 21.

Таблица 21 – Результаты выполнения тестового задания 11.2.4

| Вопрос | Правильный ответ |
|---|---|
| | |

*Примечание – Числа указывать в десятичной системе счисления.*

Лабораторное задание считается выполненным, если все предлагаемые задания завершены успешно. При этом на экран выводится окно, показанное на рисунке 67, а.

Лабораторное задание считается не выполненным, если на экран выводится окно, показанное на рисунке 67, б. В этом случае необходимо нажать кнопку «Выполнить еще раз» и заново выполнить пункты 11.2.1 … 11.2.5.

11.2.6 Продемонстрируйте выполнение практического задания преподавателю дисциплины.

### 11.3 Содержание отчета

1 Цель лабораторной работы.

2 Структурная схема криптосистемы после выполнения девяти шагов алгоритма электронной цифровой подписи RSA.

3 Условия выбора открытого и секретного ключей, используемых в алгоритме электронной цифровой подписи RSA.

4 Таблица с исходными данными, соответствующими индивидуальному варианту задания.

5 Таблицы с результатами выполнения задания.

6 Выводы по результатам выполнения задания.

7 Ответы на контрольные вопросы.


а


б

а – задание выполнено; б – задание не выполнено

Рисунок 67 – Окно с заключительными результатами выполнения задания программы, реализующей алгоритм электронной цифровой подписи RSA

### 11.4 Контрольные вопросы

1 Каким образом осуществляется аутентификация электронных документов и их авторов с помощью алгоритма электронной цифровой подписи RSA?

2 Какие требования необходимо выполнить для обеспечения высокого уровня информационной безопасности при реализации алгоритма электронной цифровой подписи RSA?

3 Какую длину должен иметь модуль в алгоритме электронной цифровой подписи RSA?

4 Можно ли обеспечить конфиденциальность электронного документа при использовании алгоритма электронной цифровой подписи RSA?

5 Какое практическое применение находит алгоритм электронной цифровой подписи RSA?

# ЛАБОРАТОРНАЯ РАБОТА №12
# АЛГОРИТМ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ DSA

**Цель:** изучение алгоритма электронной цифровой подписи DSA, позволяющего выполнять аутентификацию электронных документов и их авторов.

## 12.1 Краткие теоретические сведения

Для ознакомления с краткими теоретическими сведениями включите персональный компьютер и запустите файл «lr12_EDS_DSA_exe» на выполнение.

После запуска файла «lr12_EDS_DSA_exe» активизируется программное обеспечение, реализующее алгоритм электронной цифровой подписи DSA, и появится главное окно программы, показанное на рисунке 68.

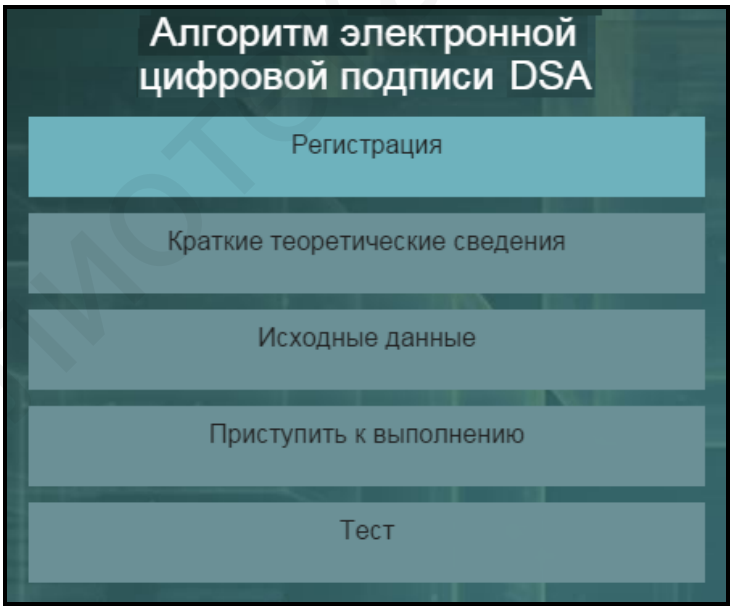



Рисунок 68 – Главное окно программы, реализующей алгоритм электронной цифровой подписи DSA

До начала работы с программой необходимо зарегистрироваться. Для этого требуется в главном окне программы нажать кнопку «Регистрация» и в появившемся окне регистрации, приведенном на рисунке 3, ввести в поле «Фамилия и имя» свою фамилию и имя, указать номер группы в поле «Номер группы» и нажать кнопку «Регистрация».

Затем необходимо в главном окне программы нажать кнопку «Краткие теоретические сведения», после чего на экран выводится окно с краткими теоретическими сведениями, показанное на рисунке 69.

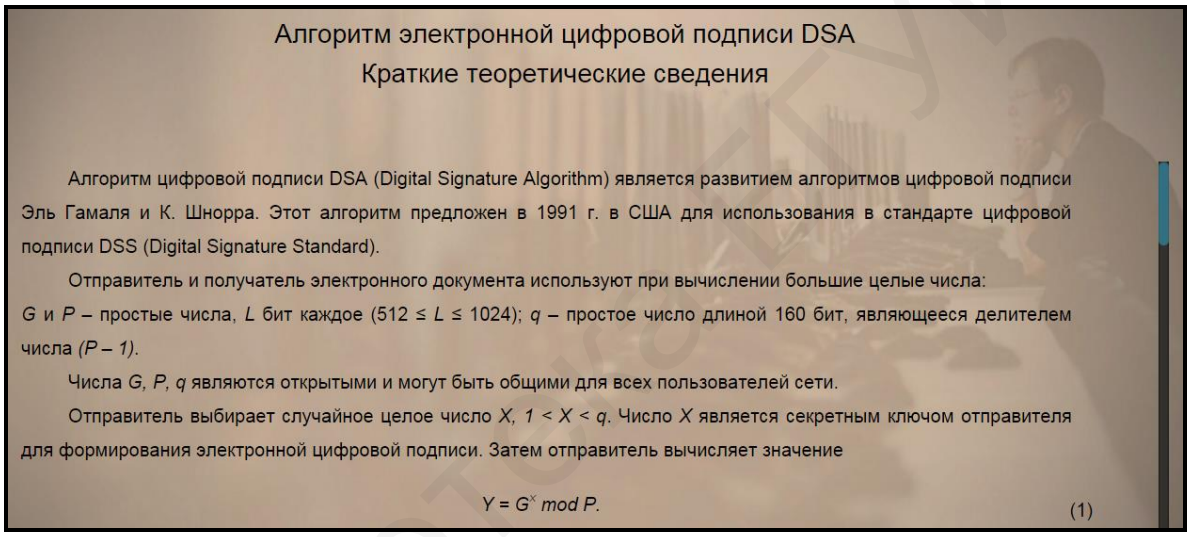



Рисунок 69 – Внешний вид окна с краткими теоретическими сведениями по алгоритму электронной цифровой подписи DSA

## 12.2 Практическое задание

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

Для загрузки исходных данных необходимо в главном окне программы (см. рисунок 68) нажать кнопку «Исходные данные» и в появившемся окне ввода и загрузки исходных данных, приведенном на рисунке 70, ввести исходные данные в соответствии с индивидуальным вариантом и нажать кнопку «Загрузить исходные данные».

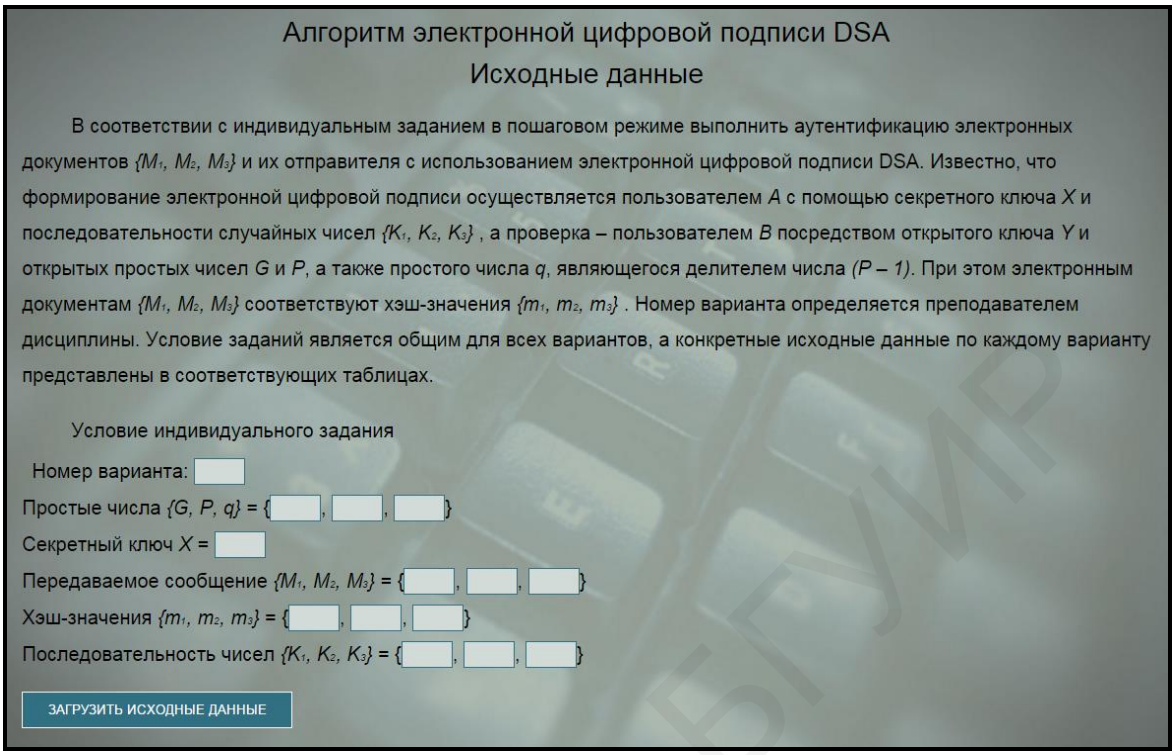



Рисунок 70 – Внешний вид окна ввода и загрузки исходных данных программы, реализующей алгоритм электронной цифровой подписи DSA

12.2.2 Выполните предлагаемые задания по передаче сообщения с использованием алгоритма электронной цифровой подписи DSA.

Выполнение заданий по передаче сообщения заключается в последовательной реализации алгоритма электронной цифровой подписи DSA, заполнении и анализе таблицы с полученными результатами. Условие заданий является общим для всех вариантов, а конкретные исходные данные определяются вариантом индивидуального задания.

Для выполнения заданий необходимо в главном окне программы (см. рисунок 68) нажать кнопку «Приступить к выполнению» и в появившемся окне реализации основных этапов алгоритма электронной цифровой подписи DSA, приведенном на рисунке 71, заполнить поля для ввода данных, располагающиеся в левой нижней его части, и нажать кнопку «Проверить».


Рисунок 71 – Внешний вид окна реализации основных этапов алгоритма электронной цифровой подписи DSA

Если одно или несколько полей для ввода данных не соответствуют заданию, указанному в верхней области окна реализации основных этапов алгоритма электронной цифровой подписи DSA, на экран выводится сообщение об ошибке, показанное на рисунке 72.

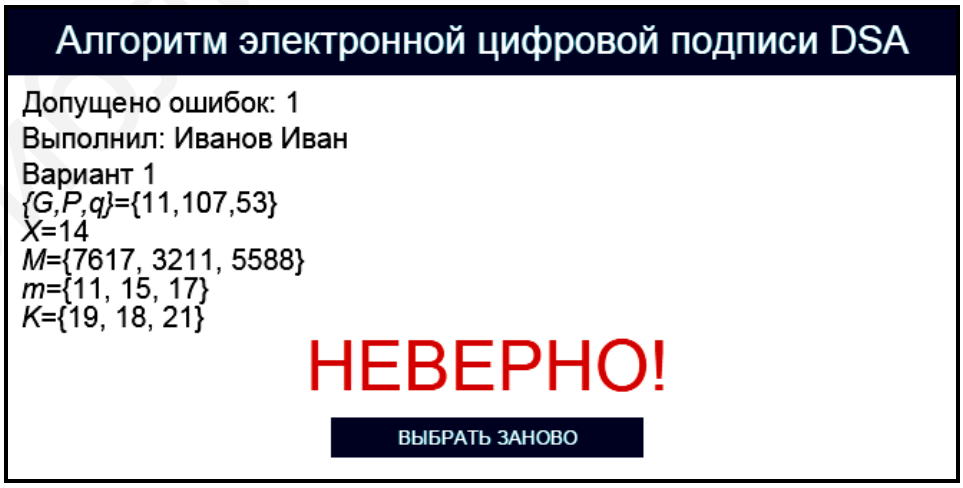



Рисунок 72 – Сообщение об ошибке реализации основных этапов алгоритма электронной цифровой подписи DSA

В этом случае необходимо нажать кнопку «Выбрать заново» и повторно заполнить поля для ввода данных в окне реализации основных этапов алгоритма электронной цифровой подписи DSA (см. рисунок 71).

При правильном заполнении полей для ввода данных в окне реализации основных этапов алгоритма электронной цифровой подписи DSA на экран выводится соответствующее информационное сообщение. На рисунке 73 в качестве примера показано информационное сообщение, появляющееся после правильного выполнения задания по вычислению открытого ключа *Y*.

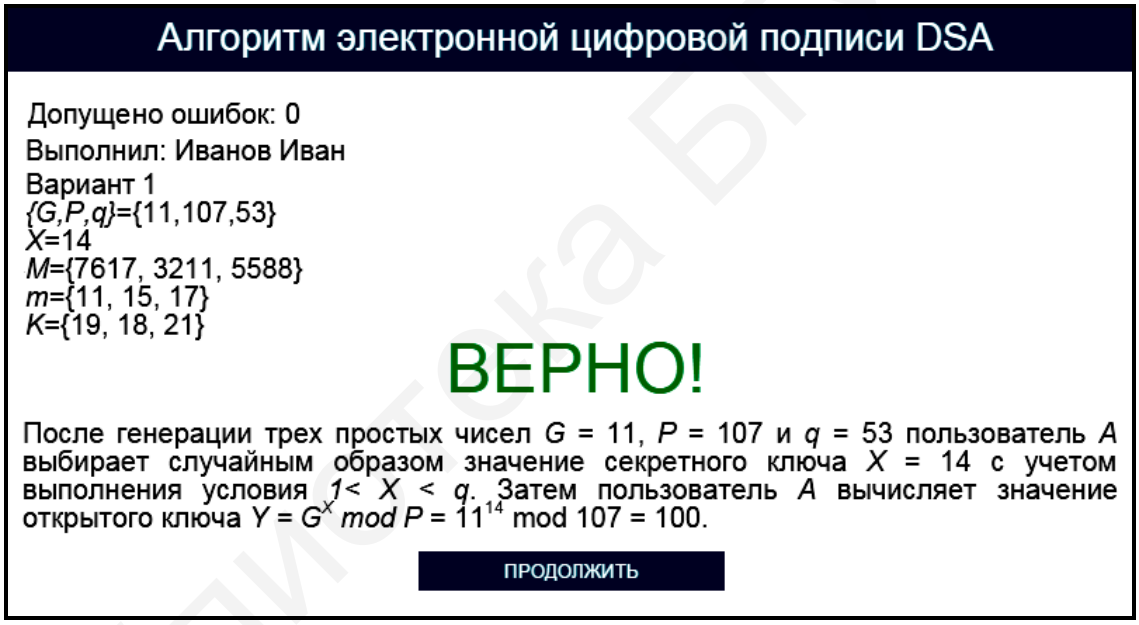



Рисунок 73 – Информационное сообщение программы, реализующей алгоритм электронной цифровой подписи DSA

В правой верхней части окна реализации основных этапов алгоритма электронной цифровой подписи DSA имеются три области, в которых указано допущенное количество ошибок, зарегистрированные пользовательские данные и загруженные исходные данные. При щелчке на области, в которой указано допущенное количество ошибок, появляется окно с промежуточными результатами выполнения задания, приведенное на рисунке 74.

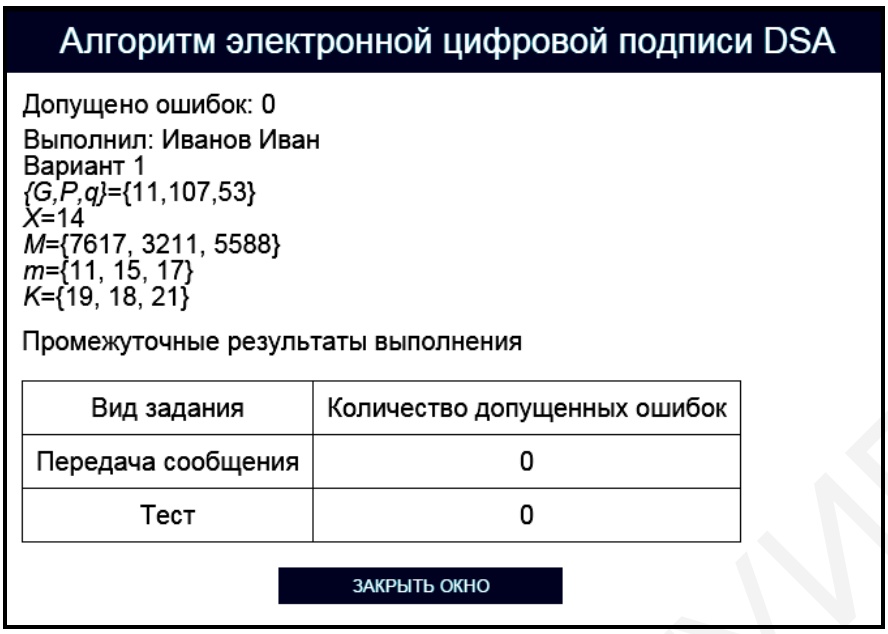



Рисунок 74 – Окно с промежуточными результатами выполнения задания программы, реализующей алгоритм электронной цифровой подписи DSA

Для возврата в окно реализации основных этапов алгоритма электронной цифровой подписи DSA необходимо нажать кнопку «Закрыть окно».

При щелчке на области, в которой указаны загруженные исходные данные, появляется окно подтверждения смены индивидуального задания (см. рисунок 10). Для изменения условия индивидуального задания необходимо щелкнуть на гиперссылке «Подтвердить выход», для возврата в окно реализации основных этапов алгоритма электронной цифровой подписи DSA – на гиперссылке «Отмена».

Выход в главное окно программы (см. рисунок 68) обеспечивается нажатием кнопки «Выход в главное меню» (см. рисунок 71). При этом появляется окно подтверждения выхода в главное окно программы (см. рисунок 11). Для выхода в главное окно программы необходимо щелкнуть на гиперссылке «Подтвердить выход», для возврата в окно реализации основных этапов алгоритма электронной цифровой подписи DSA – на гиперссылке «Отмена».

Задание по передаче сообщения с использованием алгоритма электронной цифровой подписи DSA считается выполненным, если все предлагаемые задания завершены успешно.

12.2.3 После выполнения заданий по передаче сообщения с использованием алгоритма электронной цифровой подписи DSA заполните таблицу 22.

Таблица 22 – Результаты исследования работы криптосистемы, реализующей алгоритм электронной цифровой подписи DSA

| Номер шага (этапа) реализации | Наименование | Описание работы криптосистемы |
|---|---|---|
| | | |

*Примечание – Числа указывать в десятичной системе счисления.*

12.2.4 Выполните тестовые задания.

Для выполнения тестовых заданий необходимо в главном окне программы (см. рисунок 68) нажать кнопку «Тест» и в появившемся окне, показанном на рисунке 75, ознакомиться с инструкцией и нажать кнопку «Начать тест».


Рисунок 75 – Окно с инструкцией по выполнению тестовых заданий программы, реализующей алгоритм электронной цифровой подписи DSA

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

12.2.5 По результатам выполнения тестового задания заполните таблицу 23.

Таблица 23 – Результаты выполнения тестового задания 12.2.4

| Вопрос | Правильный ответ |
|---|---|
| | |

*Примечание – Числа указывать в десятичной системе счисления.*

Лабораторное задание считается выполненным, если все предлагаемые задания завершены успешно. При этом на экран выводится окно, показанное на рисунке 76, а.

Лабораторное задание считается не выполненным, если на экран выводится окно, показанное на рисунке 76, б. В этом случае необходимо нажать кнопку «Выполнить еще раз» и заново выполнить пункты 12.2.1 … 12.2.5.

12.2.6 Продемонстрируйте выполнение практического задания преподавателю дисциплины.

### 12.3 Содержание отчета

1 Цель лабораторной работы.

2 Структурная схема криптосистемы после выполнения восьми шагов алгоритма электронной цифровой подписи DSA.

3 Условия выбора открытого и секретного ключей, используемых в алгоритме электронной цифровой подписи DSA.

4 Таблица с исходными данными, соответствующими индивидуальному варианту задания.

5 Таблицы с результатами выполнения задания.

6 Выводы по результатам выполнения задания.

7 Ответы на контрольные вопросы.


а


б

а – задание выполнено; б – задание не выполнено

Рисунок 76 – Окно с заключительными результатами выполнения задания программы, реализующей алгоритм электронной цифровой подписи DSA

### 12.4 Контрольные вопросы

1 Каким образом осуществляется аутентификация электронных документов и их авторов с помощью алгоритма электронной цифровой подписи DSA?

2 Какие требования необходимо выполнить для обеспечения высокого уровня информационной безопасности при реализации алгоритма электронной цифровой подписи DSA?

3 Какую длину должны иметь простые числа, используемые в алгоритме электронной цифровой подписи DSA?

4 Какие преимущества имеет криптографическая система на базе алгоритма электронной цифровой подписи DSA в сравнении с криптосистемами, в которых применяется алгоритм электронной цифровой подписи RSA?

5 Какое практическое применение находит алгоритм электронной цифровой подписи DSA?

## ЛИТЕРАТУРА

1 Тимофеев, А. М. Криптографическая защита информации : пособие / А. М. Тимофеев. – Минск : БГУИР, 2018. – 44 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 Введение в теоретико-числовые методы криптографии : учеб. пособие / М. М. Глухов [и др.]. – СПб. : Лань, 2011. – 400 с.

5 Стохастические методы и средства защиты информации в компьютерных системах и сетях / М. А. Иванов [и др.]. – М. : Кудиц-Пресс, 2009. – 512 с.

6 Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – 3-е изд. – М. : Изд. центр «Академия», 2008. – 336 с.

7 Защита информации в компьютерных сетях. Практический курс : учеб. пособие / А. Н. Андрончик [и др.] ; под ред. Н. И. Синадского. – Екатеринбург : УГТУ-УПИ, 2008. – 248 с.

8 Жданов, О. Н. Методы и средства криптографической защиты информации : учеб. пособие / О. Н. Жданов, В. В. Золотарев. – СибГАУ : Красноярск, 2007. – 217 с.

9 Бабаш, А. В. Криптография / А. В. Бабаш, Г. П. Шангин ; под ред. А. П. Шерстюка и Э. А. Применко. – М. : СОЛОН-ПРЕСС, 2007. – 512 с.

10 Смарт, Н. Криптография / Н. Смарт. – М. : Техносфера, 2005. – 528 с.

11 Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. – М. : Академический Проспект : Трикста, 2005. – 544 с.

12 Криптографическая защита информации [Электронный ресурс]. – Режим доступа : https://erud.bsuir.by/?PageID=83978&menuItemID=null&prop_id=21721%3B217. – Дата доступа : 27.07.2019.

Св. план 2020, поз. 33

*Учебное издание*

**Тимофеев** Александр Михайлович

# КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

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

Подписано в печать 05.02.2020. Формат 60х84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 6,63. Уч.-изд. л. 7,2. Тираж 35 экз. Заказ 377.

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