**Подготовил: Подкопаев Андрей Игоревич, ЕТ-225**

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**Лабораторная работа «Криптоанализ алгоритма Рабина»**

## Общая информация

Необходимо разработать модуль лабораторной работы «Криптоанализ алгоритма Рабина».

Окно лабораторной работы должно иметь собственно основное окно, и 5 кнопок (см. рисунок 1):

1. теория;
2. текст задания;
3. пример выполнения задания;
4. получение задания;
5. проверка ответа.

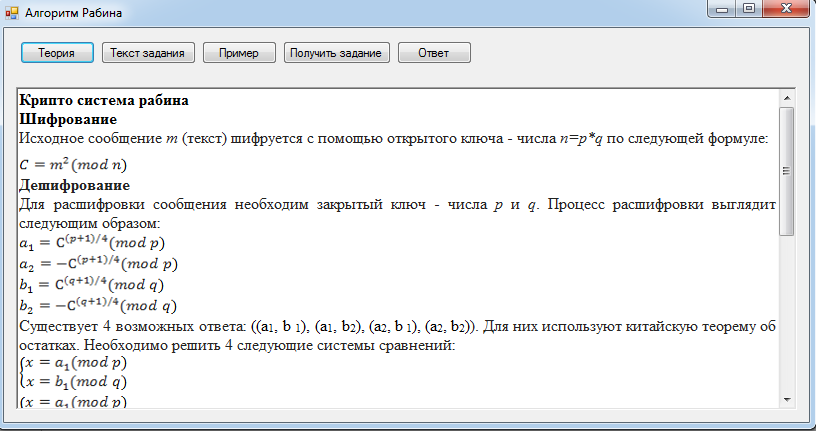


Рисунок 1

Кнопки «Теория», «Текст задания» и «Пример» изменяют содержание основного окна на содержимое соответствующих им блоков. Кнопка «Получить задание» должна вызывать стандартное диалоговое окно выбора папки. Кнопка «Ответ» вызывает содержимое блока «Ответ» в отдельной форме. По умолчанию основное окно отображает блок «Теория».

## Блоки «Теория», «Текст задания» и «Пример»

Теоретический материал и текст задания, которые необходимо отобразить, приведёны в приложении.

**Текст блока «Теория»**

**Криптосистема Рабина**

**Шифрование**

Исходное сообщение *m* (текст) шифруется с помощью открытого ключа — числа *n=p\*q* по следующей формуле:

**Дешифрование**

Для расшифровки сообщения необходим закрытый ключ — числа *p* и *q*. Процесс расшифровки выглядит следующим образом:

Существует 4 возможных ответа: ((a1, b1), (a1, b2), (a2, b1), (a2, b2)). Для них используют китайскую теорему об остатках. Необходимо решить 4 следующие системы сравнений:

Каждая система решается следующим образом:

– это общий модуль

Найти:

Решить сравнения:

После решения систем на выходе получиться 4 возможных исходных текста из которых правильным является только один.

**Текст блока «Текст задания»**

**Задание на лабораторную работу**

Расшифровать шифротекст, зашифрованный криптосистемой Рабина, при условии, что исходный текст является текстом на русском языке.

**Порядок действий**

1. Разложить открытый ключ n на простые множители p и q.
2. Извлечь из каждого числа Ci квадратный корень по модулю p\*q
3. Учитывая, что исходное сообщение – текст на русском языке, в котором каждый символ заменялся кодом символа из кодировки windows-1251 и при кодировании использовалась формула Mi = c1\*65536+c2\*256+c3, где c1, c2, c3 – первый, второй и третий символ соответственно, выбрать подходящие корни и раскодировать исходное сообщение.

**Текст блока «Пример»**

**Пример алгоритма Рабина**

1. Боб выбирает  и .

2. Боб вычисляет .

3. Боб объявляет  открытым и сохраняет  и  в секрете.

4. Алиса хочет передать исходный текст  . Она вычисляет и передает зашифрованный текст  Бобу.

5. Боб получает  и вычисляет четыре значения:

Боб имеет четыре возможных ответа — (a1, b1), (a1, b2),(a2, b1), (a2, b2) и использует китайскую теорему об остатках, чтобы найти четыре возможных исходных текста: 116, 24, 137 и 45. Обратите внимание, что только второй ответ — исходный текст Алисы. Боб должен принять решение исходя из ситуации. Обратите внимание также, что все четыре ответа при возведении во вторую степень по модулю дают зашифрованный текст , переданный Алисой.

## Получение задания

Блок должен содержать кнопку «Получить задание», при нажатии на которую вызывается окно для ввода пути, по которому задание сохраниться в виде текстового файла (см. рисунок 2). На данной форме также находиться кнопка "Обзор", по нажатию которой вызывается стандартный диалог выбора папки.

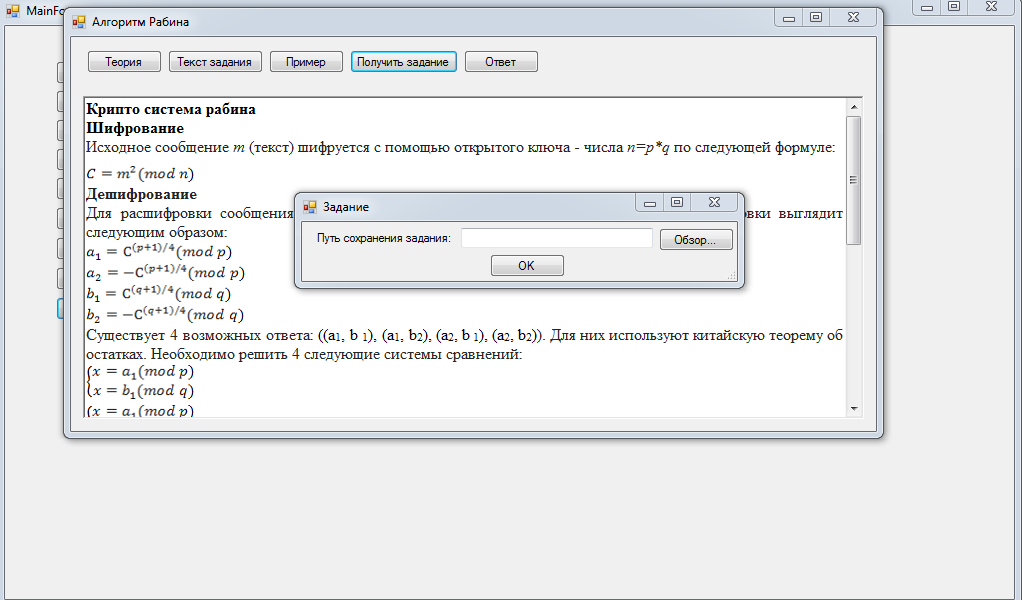


Рисунок 2

Выдаваемое задание должно соответствовать году обучения, семестру и варианту, выбранных в главном меню. Генерировать нужно таким образом, чтобы оно оставалось неизменным для одного и того же года, семестра, номера бригады и лабораторной работы.

Шаги генерации:

1. выбрать случайным образом отрывок текста на русском языке (допустима только кириллица и знак «пробел») из ресурсов проекта, а именно – из файла Sholohov.txt. Отрывок должен быть взят таким образом, чтобы первый символ отрывка был началом слова, а длина отрывка была кратна трем и составила 75 и более символов, также окончание фразы не должно обрываться на полуслове;
2. закодировать каждый символ отрывка соответствующим значением из кодировки windows-1251;
3. выбрать случайным образом два простых числа их ресурсов проекта, а именно – из файла primesforRabin.txt.
4. перемножить два простых числа по формуле , где – открытый ключ;
5. использовать формулу Mi = c1\*65536+c2\*256+c3, где c1, c2, c3 – первый, второй и третий символ соответственно;
6. зашифровать Mi с помощью шифра Рабина по следующей формуле: , где — зашифрованное значение Mi.

Заданием, которое выдаётся пользователю, является шифротекст.

## Проверка ответа

Блок проверки должен содержать поле для ввода текста, а также кнопку «Проверить» (см. рисунок 3), при нажатии на которую вызывается процедура проверки по окончании, которой уведомляется пользователь о правильности ответа. В строке ответа необходимо убирать все символы, кроме заглавных букв русского алфавита. Также необходимо убирать все лишние пробелы в конце и в начале строки.

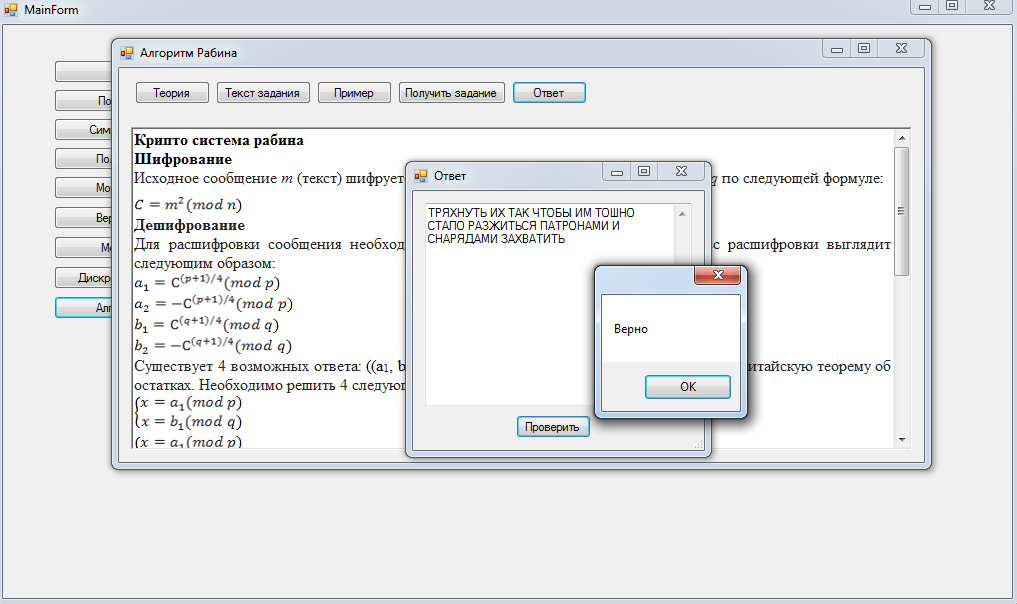


Рисунок 3

## Требования к тестированию

При тестировании разработанной программы необходимо обработать следующие исключительные ситуации:

1. Для блока «Получение задания»:

* выход за пределы общего текста при выборе отрывка для генерации задания;
* несуществующий путь для ввода полученного задания;
* незаданный путь для ввода полученного задания;

1. Для блока «Проверка ответа»:

* выход за пределы общего текста при генерации правильного ответа;
* лишние символы при сравнении строки ответа студента и правильного ответа.

При несуществующем или незаданном пути пользователю должны быть выведены соответствующие сообщения.

Выход за пределы общего текста должен быть предотвращен на этапе разработки программы.

При сравнении строки ответа студента и правильного ответа все лишние символы в строке ответа должны быть исключены.

## Требования к программной документации

Для создания программной документации необходимо разработать руководство пользователя на основе «ГОСТ 19.505-79. ЕСПД. Руководство оператора. Требования к содержанию и оформлению». Это руководство должно включать в себя следующие разделы:

* назначение программы;
* условия выполнения программы;
* выполнение программы;
* сообщения пользователю.