**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ**

**Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет»**

**ИНСТИТУТ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

**по дисциплине «Введение в инженерную деятельность»**

**на тему: «** **Реализация протокола подбрасывания монеты по телефону»**

Выполнили: студенты гр. КТсо2-6

Шамильян Оксана Петровна

Жирнова Анна Ивановна

Принял: к.т.н. доцент кафедры БИТ

Ищукова Евгения Александровна

Таганрог – 2017

1. Цель:

Реализация протокола подбрасывания монеты по телефону с возможностью показать его уязвимые стороны.

1. Актуальность:

В современном мире каждый день возникают разного вида споры между людьми, которые находятся на значительном расстоянии друг от друга. Именно в таких случаях, для разрешения спора, и используется протокол подбрасывания монеты, который не является зависимым ни от одного из участников.

1. План реализации проекта:

Выделим несколько основных этапов, на которые следует опираться в ходе выполнения работы.

1) Изучение структуры протокола подбрасывания монеты и его

спецификации;

2) Изучение разновидностей протокола;

3) Написание программы.

Разберем каждый из этапов более подробно.

* 1. Изучение структуры протокола подбрасывания монеты и его спецификации.

Данный протокол является наиболее наглядным и простым и используется в тех случаях, когда участники удалены друг от друга и могут общаться между собой только по каналу связи. Если следовать обычной процедуре подбрасывания монеты, то первый участник честно выбирает значение «орел» или «решка», а второй участник всегда может выбрать значение, которое выгодно для него самого. Понятно, что задача легко решается, если есть третий независимый участник, который имеет закрытые каналы связи как с первым, так и со втором участником. Однако, в случае отсутствия третьей независимой стороны задача обретает невыполнимый характер.

Проблема была решена в 1982 году. На 24-й компьютерной конференции IEEE Мануэлем Блюмом была прочитана лекция под названием «Бросание жребия по телефону: протокол для решения неразрешимых проблем».

* 1. Изучение разновидностей протокола.

Существует несколько разновидностей протокола:

* Протокол Блюма-Микали;
* Протокол подбрасывания монеты (на основе проблемы дискретного логарифмирования);
* Протокол подбрасывания монеты для получения общего случайного бита (на основе проблемы дискретного логарифмирования).
  + 1. Протокол Блюма-Микали.

Два пользователя (П1 и П2) заранее договариваются о некоторой односторонней функции f.

П1: выбирает случайным образом число x∈X, где X – конечное множество натуральных чисел, среди которых равное количество четных и нечетных, затем вычисляет значение y=f(x)

П1→П2: y

П2: делает догадку, число х четное или нет. Если х – четное, с=0, если х – нечетное, с = 1

П2→П1: с

П1→П2: x

П2: проверяет f(x)=y.

* + 1. Протокол подбрасывания монеты (на основе проблемы дискретного логарифмирования).

Параметры протокола: p – большое простое число, g - порождающий элемент мультипликативной группы.

П1 : выбирает случайное x∈, вычисляет y= mod p.

П1→П2: y

П2→П1: догадка - бит с.

П1→П2: x

П2: проверяет mod p=y.

* + 1. Протокол подбрасывания монеты для получения общего случайного бита (на основе проблемы дискретного логарифмирования).

Параметры протокола: p – большое простое число, g - порождающий элемент мультипликативной группы .

П1: выбирает случайное x∈, вычисляет y= mod p.

П1→П2: y

П2: выбирает случайные b∈{0,1}, k∈, вычисляет r= mod p.

П2→П1: r

П1→П2: случайный c∈ {0,1}

П2→П1: b, k

П1: проверяет r= mod p. Если результат проверки положительный, то результатом выполнения протокола будет бит d=b⊕c.

Нужно заметить, что из значения r Пользователь 1 не может ничего узнать о бите *b* и поэтому вынужден посылать случайный бит *с*. Тогда возникает вопрос – может ли Пользователь 1 подменить значение b после получения бита с?

Проблема подмены бита:

Проблема подмены бита для данного алгоритма заключается в том, чтобы, не зная значений *y, g, p* найти такие *k1, k2,* чтобы .

* 1. Написание программы.

Перед тем как приступить к написанию программного кода, нужно ответить на несколько важных вопросов.

1. Кто будет выступать в роли пользователя?

Изучение работы протокола подбрасывания монеты по телефоны, является одним из этапов в изучении криптографии. Именно поэтому данный программный пакет разрабатывался для студентов с целью отработки навыков по реализации работы протокола.

1. В каком виде программа предстанет перед пользователем? (разработка интерфейса)

Для удобной работы был разработан соответствующий интерфейс, облегчающий работу с программой.

Программа осуществляет работу в трех направлениях:

1. Построение мультипликативной группы;
2. Работа протокола без подмены бита;
3. Работа протокола с подменой бита.

Для выбора одного из направления работы, было разработано меню, представленное на рисунке 1.

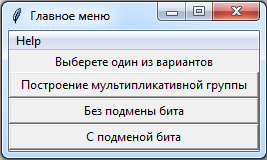


Рис.1. Главное меню

1. Как будет выбираться простое число «p» и порождающий элемент «g»?

Мультипликативная группа является неотъемлемой частью в работе протокола. Именно поэтому пользователь должен уметь правильно ее составлять. Для этого программа содержит в себе такое направление работы как «Построение мультипликативной группы», где пользователь может получить или закрепить навыки в построении мультипликативной группы.

На первом этапе построения мультипликативной группы от пользователя требуется ввести значение простого числа «p» и порождающего элемента мультипликативной группы «g», такого, что .

Ввод значение происходит в окне, представленном на рисунке 2.

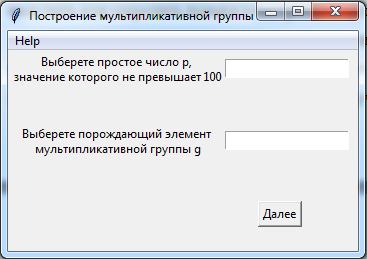


Рис.2 Ввод значений «p» и « g»

Если пользователь ввел значения, неудовлетворяющие вышеуказанным требованиям, то будет выведено сообщение об ошибке.

На рисунке 2, представлен вариант неправильного ввода значений (введенное число p не является простым).

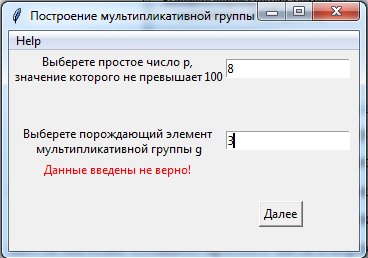


Рис.3. Вывод сообщения об ошибки

1. Как будет создаваться мультипликативная группа?

После ввода параметров на экране появляется окно, в котором осуществляется ввод посчитанных пользователем значений мультипликативной группы. Данное окно представлено на рисунке 4, в качестве примера были выбраны значения p = 7 и g = 3.

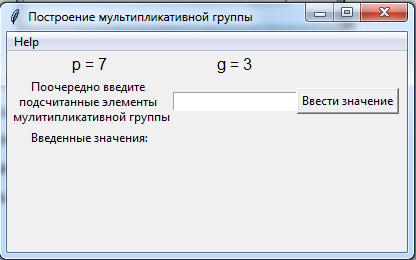


Рис.4. Окно для ввода значений элементов мультипликативной группы

Ввод подсчитанных значений осуществляется поочередно, т.е. после каждого введенного числа нажимается кнопка «Ввести значение».

Для подсчета значений мультипликативной группы нужно придерживаться следующему алгоритму действий.

1. Выбрать диапазон чисел l = [1 … p-1];
2. Вычислить значения элементов по формуле для всех чисел из диапазона l.

Каждое введенное число будет отображаться в поле «Введенные значения». Для завершения работы следует нажать кнопку «Завершить ввод».

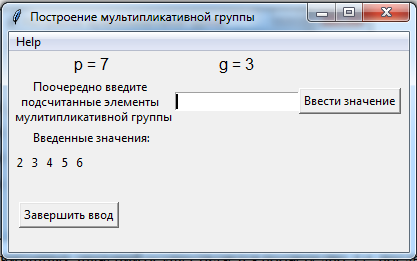
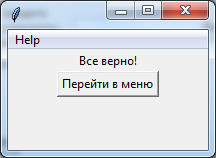
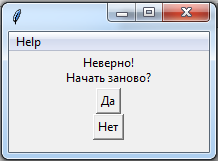


Рис.5. Ввод значений

После нажатия кнопки пользователю будет выведен результат о правильности введенных значений. Возможные варианты результатов представлены на рисунках 6(а) и 6(б).

a) б)

Рис.6. Вывод результатов

Если пользователь неверно ввел значения и на экран вывелся соответствующий результат (рис. 6(б)), то он может начать заново (нажать кнопку «Да») или вернуться в меню (кнопка «Нет»).

1. Как будет реализована работа протокола без подмены бита?

Выбрав второй пункт меню «Без подмены бита», пользователь начинает непосредственную работу с протоколом. Сперва пользователь вводит значения p и g, после чего, если значения верны, начинается работа по алгоритму протокола. На данном этапе пользователю не нужно самостоятельно вычислять элементы мультипликативной группы (Рис.7).

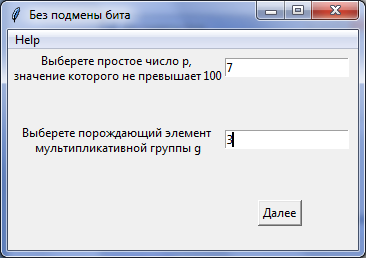


Рис.7 Ввод значений p и g

Алгоритм работы протокола подразумевает, что участие принимают два пользователя, поэтому в качестве пользователя 1 выступает компьютер, а в качестве пользователя 2 – пользователь.

Компьютером выбирается случайное число х, вычисляет функция .Значение y выводится на экран (Рис.8).

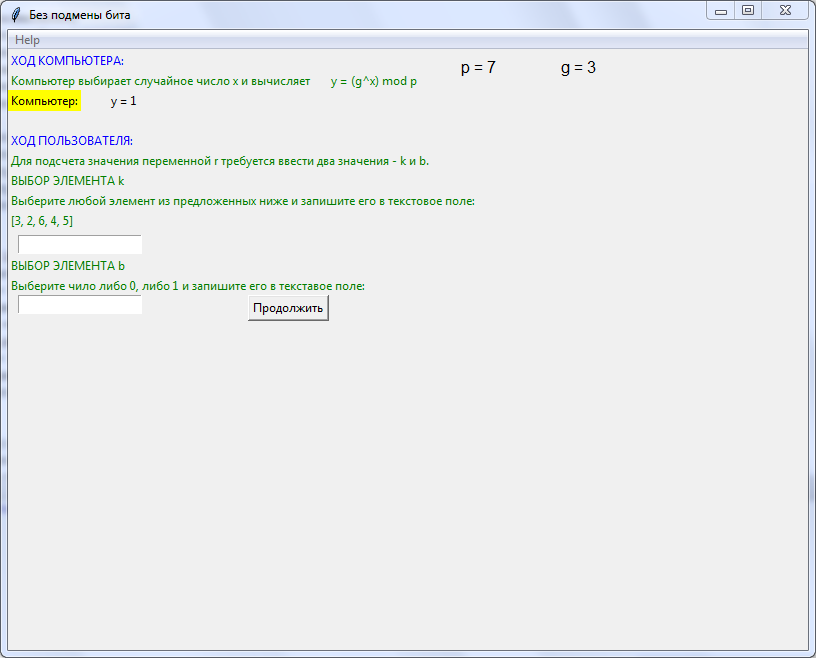


Рис.8 Значение y

После этого наступает очередь пользователя. На данном этапе происходит ввод чисел k и b. На экран выводится значение мультипликативной группы, а так же ряд подсказок для правильности выбора значений. Введя значения, необходимо нажать кнопку «Продолжить» (Рис.9)



Рис.9 Ввод значений k и b

Значение k выбирается из мультипликативной группы, значение  
.

Выполняется обработка введенных значений k и b, если данные некорректны, то выводится сообщение об ошибке. Если же данные введены правильно, работа программы продолжается и на экран выводиться поле для ввода значения r. Данное значение считается по формуле . После ввода r нажимается кнопка «продолжить», выполняется проверка на корректность. Если данные введены неправильно – выводится сообщение об ошибке, иначе значение r передается пользователю 1 (при этом значения k и b на этом этапе не передаются пользователю 1) (Рис.10).

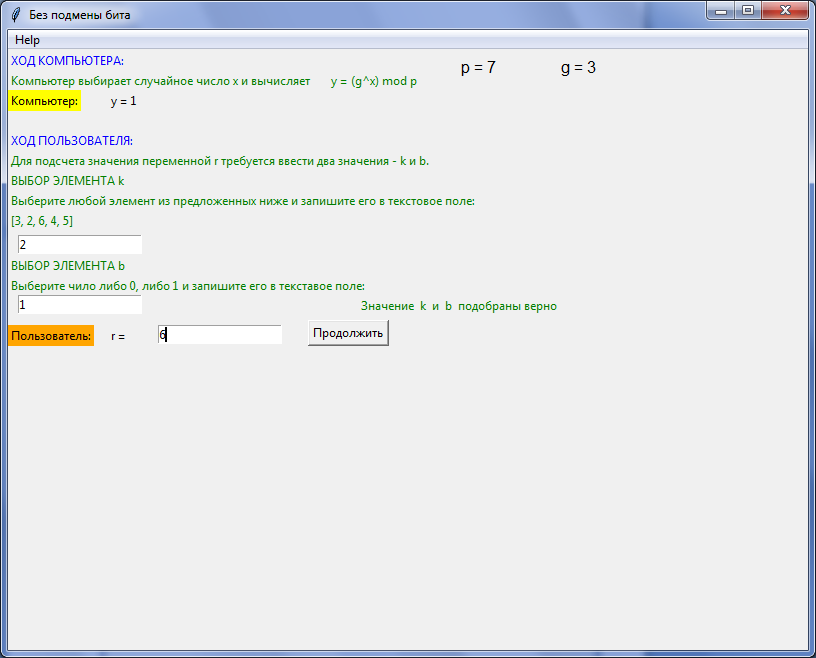


Рис.10 Ввод значения r

На этом этапе ход пользователя заканчивается и наступает очередь компьютера (пользователя 1).

Случайным образом компьютер выбирает число . И передает его пользователю 2, т.е. значение с выводится на экран.

Наступает через пользователя и компьютеру передаются введенные ранее значения k и b. Передача данных происходит автоматически во избежание подмены значений k и b.

После передачи k и b на экран выводится результат выполнения протокола (Рис.11).

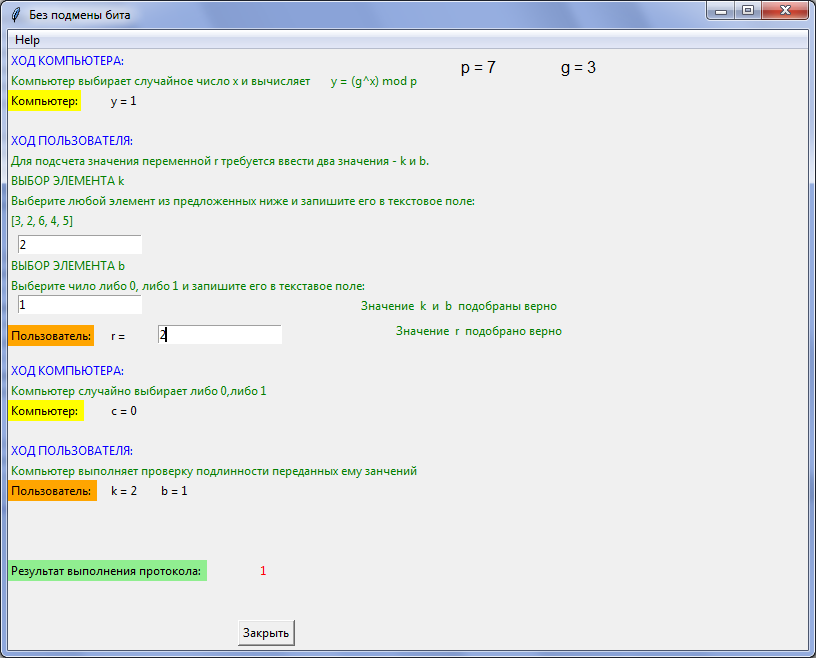


Рис. 11 Результат выполнения протокола

Результатом выполнения протокола является общий бит d, вычисленный по формуле .

1. Как будет реализована работа протокола с подменой бита?

Выбрав третий пункт меню, пользователь имеет возможность начать работу над проблемой подмены бита.

Вначале, так же как и в предыдущем пункте пользователю предлагается ввести *p* и *g,* для построения мультипликативной группы (Рис. 12).

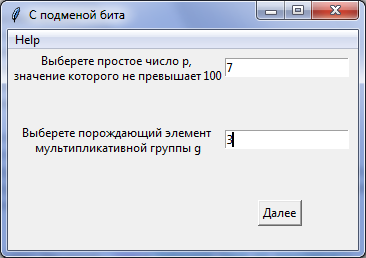


Рис.12 Ввод значений p и g

Построение осуществляется автоматически и пользователь сразу переходит к работе с протоколом.

Первые шаги в алгоритме работы протокола с подменой бите аналогичны алгоритму без подмены.

Пользователь получает от компьютера посчитанный *y.*

Пользователь выбирает значение *k1* из мультипликативной группы (элементы группы выведены на экран) и . Нажимает кнопку «Продолжить» и вводит посчитанное значение *r*. Опять нажимает кнопку «Продолжить». После нажатия кнопки выполняется проверка введенных значений, и если все верно очередь переходит к Компьютеру (Рис.13).



Рис.13 Ввод k и b

На данном шаге Компьютер передает пользователю случайный бит .

Ход переходит к Пользователю. На данном этапе Пользователь должен передать Компьютеру значения *k* и *b*, и если при работе протокола без подмены бита пользователь передавал значения, использовавшиеся ранее для подсчета *r*, то теперь Пользователь должен найти такую пару *k2* и *b2*, что . При этом (Рис.14).

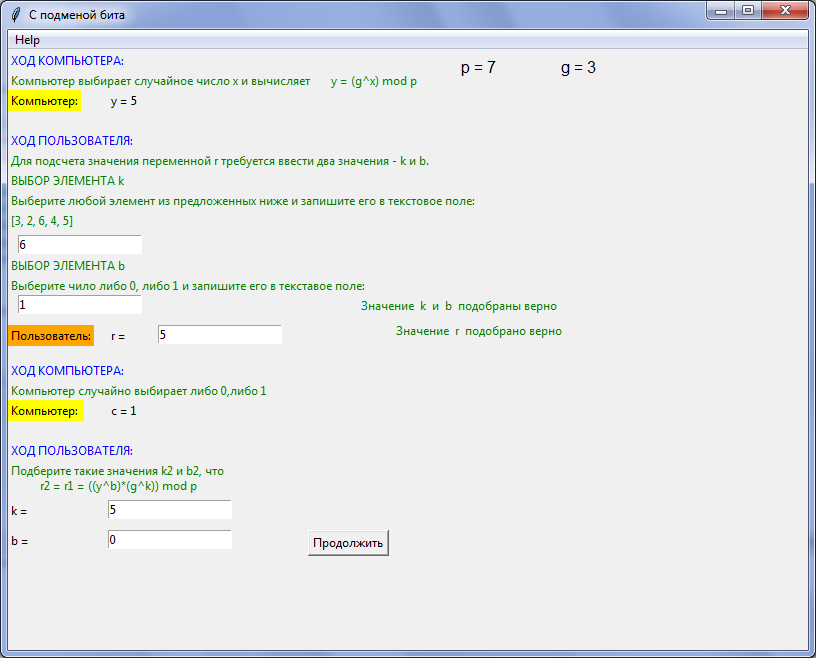


Рис.14 Подбор значений k и b

После ввода значений и нажатия кнопки «Продолжить» выполняется проверка введенных значений, и если все верно выводится результат выполнения протокола (Рис.15).

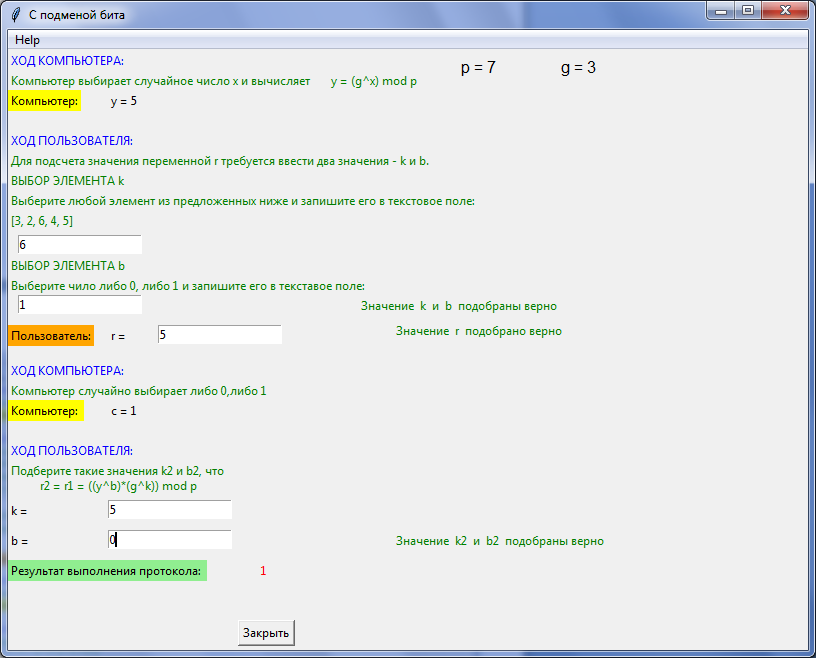


Рис.15 Результат выполнения протокола

1. Смена ролей.

Для лучшего понимания работы протокола, реализована функция, позволяющая пользователю меняться ролями с компьютером. При этом алгоритм работы протокола остается неизменным.

1. Хранение данных о пользователе.

Так как данный программный комплекс направлен на обучение, то будет полезно отслеживать статистику.

Данные хранятся в базе данных «BD Browser for SQLtie» в таблице users.

Таблица users содержит в себе несколько полей, а именно:

1. first name – имя пользователя;
2. second name – фамилия пользователя;
3. group – номер группы;
4. try 1 – общее количество попыток создать мультипликативную группу;
5. plus 1 – количество правильно введенных данных при создании мультипликативной группы;
6. try 2 – общее количество попыток работы с протоколом без подмены бита;
7. plus 2 – количество правильно введенных данных при работе с протоколом без подмены бита;
8. try 3 – общее количество попыток работы с протоколом с подменой бита;
9. plus 3 – количество правильно введенных данных при работе с протоколом с подменой бита;

Каждый пользователь может посмотреть данные своей статистики во вкладке «Статистика» на панели инструментов.

1. Информация о программе.

Если у пользователя возникают вопросы о работе программы или о работе протокола, то всю необходимую информацию он может получить, открыв вкладку «Help» на панели инструментов.

4. Заключение.

Подводя итоги можно сказать, что программа по реализации протокола подбрасывания монеты действительно актуальный проект. Часто возникают ситуации, в которых два участника должны обмениваться некоторой информацией, но каждый из них может оказаться обманщиком. В таких ситуациях данный протокол незаменим. И поэтому информация о том как работает протокол, о его сильных и слабых сторонах является весьма полезной. Именно поэтому данный программный комплекс направлен на получение и отработку навыков.