«Криптография»

Индивидуальное задание состоит из 2х блоков заданий:

1. вычислительные основы криптографических алгоритмов

2. программирование простейшего алгоритма

В письменной части показывать промежуточные вычисления (при возведении в степени, нахождении обратных величин и т.п.

**Блок 1. Письменная часть**

**Задание 1.1.**

Осуществить подпись сообщения со своей фамилией и именем в соответствии со следующими параметрами. Метод создания подписи определяется как (n1 mod 3)+1, где n – номер в списке, а список методов следующий:

1. RSA
2. Эль-Гамаль
3. ГОСТ на основе Эль-Гамаля

В зависимости от вида подписи, взять параметры P – простое число, ближайшее к числу (2∙n)+10, а для Q – аналогичное определенное число 3∙n +5. Индивидуальные параметры для подписи двух пользователей следует вычислить по формуле:

((i+1)∙n) mod 50 +10, где i – номер пользователя, n – номер варианта. Проверить, будет ли подтверждена подпись при изменении автора сообщения без изменения подписи.

**Задание 1.2.**

Промоделировать расчет между собой 3х лиц в следующем порядке: первый человек снимает в банке сумму K в купюрах, указанных в таблице; после чего передает сумму L1 первому пользователю, и L2 второму пользователю, после чего те передают деньги в банк. Показать процедуру расчета и изменение состояния счетов в банке, если пользователь 2 принесет деньги раньше, чем пользователь 3. В качестве типа идентификации купюры использовать «слепую» подпись для купюр, где первая цифра соответствует номинации купюры. При этом в качестве параметров банка использовать P – простое число, ближайшее к числу (2∙n)+10, а для Q – аналогичное определенное число 3∙n +5. Вариант определить по формуле (m mod 10) +1, где m - номер в списке группы.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| вариант | Виды купюр | | | Состояния счетов | | | Снятая сумма | Оплата 1 | Оплата 2 |
| П1 | П2 | П3 |
| 1 | 1 | 3 | 5 | 10 | 11 | 12 | 10 | 3 | 7 |
| 2 | 1 | 2 | 5 | 12 | 1 | 3 | 12 | 8 | 4 |
| 3 | 1 | 5 | 10 | 13 | 2 | 7 | 13 | 4 | 8 |
| 4 | 1 | 3 | 10 | 12 | 7 | 3 | 12 | 7 | 6 |
| 5 | 1 | 3 | 5 | 15 | 6 | 3 | 13 | 7 | 6 |
| 6 | 1 | 2 | 5 | 31 | 2 | 4 | 27 | 15 | 15 |
| 7 | 1 | 5 | 10 | 17 | 3 | 2 | 17 | 17 | 5 |
| 8 | 1 | 3 | 10 | 15 | 4 | 2 | 12 | 8 | 4 |
| 9 | 1 | 3 | 5 | 11 | 3 | 1 | 10 | 4 | 8 |
| 10 | 1 | 2 | 5 | 12 | 4 | 5 | 11 | 9 | 2 |

**Задание 1.3.**

Осуществить проверку возможности использования эллиптической кривой с заданными параметрами (таблица 1). Определить точки эллиптической кривой путем перебора. Осуществить шифрование с помощью заданной эллиптической кривой, предварительно сформировав все необходимые данные для сети из 2х человек. Зашифровать и дешифровать инициалы (предварительно перевести их в число от 0 до p-1). Вариант определить по формуле (m mod 9) +1, где m - номер в списке группы.

Таблица 2.

Параметры эллиптической кривой

|  |  |  |  |
| --- | --- | --- | --- |
| № | a | b | p |
| 1 | 1 | 1 | 11 |
| 2 | 1 | 5 | 11 |
| 3 | 1 | 6 | 11 |
| 4 | 2 | 4 | 11 |
| 5 | 3 | 2 | 11 |
| 6 | 3 | 9 | 11 |
| 7 | 4 | 4 | 11 |
| 8 | 4 | 7 | 11 |
| 9 | 5 | 1 | 11 |

**1.4. Дополнительное задание**

Осуществить расчет количества точек эллиптической кривой, заданной в таблице 2.

### Блок 2. Программная часть

**Задание 2.1.**

Разработать алгоритмы, интерфейс и реализовать программное обеспечение, осуществляющее дешифрование текста путем взлома шифротекста, если заданы открытые параметры ключей.

Замечание: где возможно, использовать ускоренные алгоритмы для получения необходимых остатков при умножении.

### Список вариантов

|  |  |
| --- | --- |
|  | Алгоритм |
| 1 | взлом Диффи-Хеллмана (перебор) |
| 2 | взлом Шамира (перебор) |
| 3 | взлом Эль-Гамаля (перебор) |
| 4 | взлом RSA (перебор) |
| 5 | взлом шифра Цезаря |
| 6 | взлом шифра Трисемуса |
| 7 | взлом Диффи-Хеллмана (шаг младенца-великана) |
| 8 | взлом Шамира (шаг младенца-великана) |
| 9 | взлом Диффи-Хеллмана (перебор) |
| 10 | взлом RSA (шаг младенца-великана) |
| 11 | взлом Эль-Гамаля (шаг младенца-великана) |
| 12 | взлом Шамира (перебор) |
| 13 | взлом Диффи-Хеллмана (шаг младенца-великана) |
| 14 | взлом шифра Трисемуса |
| 15 | взлом шифра Цезаря |

**Задание 2.2.** Реализовать программное обеспечение, решающее одну из следующих задач (в зависимости от варианта – см. табл.).

1. Разработать программу, позволяющую генерировать подпись к сообщению некоторым пользователем, а также осуществить верификацию подлинности подписи. Требования: возможность перехода между различными пользователями (реализовать в виде множества пользователей с возможностью добавления нового); хранение очереди сообщений (чтобы можно было выбрать произвольное для верификации подписи); осуществление верификации пользователя по сообщению; определение перебором по данным пользователей автора сообщения.

2. Реализовать задачу «ментальный покер» для 2\*n+k карт (выбор по n карт каждым пользователем и k – прикуп). Предусмотреть возможность автоматической генерации действий вторым игроком, с хранением протокола операций (т.е. на форме осуществляются пользователем действия только одной стороны, а вторая – автоматически, случайно выбирая и перемешивая карты). Выбор действующего лица (1-й или 2-й) осуществляется пользователем.

3. Реализовать механизм расчета с помощью «электронных денег». Требования: возможность заведения счета для пользователей и учета движения денег (т.е. хранится группа пользователей с параметрами и счетом наличных); для расчета используются купюры 2х номиналов (т.е. необходимо раздельно хранить данные о номерах купюр, где это необходимо). Предусмотреть возможности расчета с другими пользователями в качестве получателей.

### Список вариантов

|  |  |  |
| --- | --- | --- |
| № п/п | № программы | Дополнительные параметры |
| 1 | 1 | RSA |
| 2 | 1 | Эль-Гамаля |
| 3 | 2 | – |
| 4 | 3 | Односторонняя функция |
| 5 | 3 | RSA |
| 6 | 1 | Эль-Гамаля |
| 7 | 1 | RSA |
| 8 | 2 | – |
| 9 | 3 | Односторонняя функция |
| 10 | 3 | RSA |
| 11 | 1 | RSA |
| 12 | 1 | Эль-Гамаля |
| 13 | 2 | – |
| 14 | 3 | Односторонняя функция |
| 15 | 3 | RSA |