**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра Информатики**

отчет

**по лабораторной работе №3**

**по дисциплине «Защита информации в компьютерных сетях»**

Тема: Исследование схем разделения секрета

|  |  |  |
| --- | --- | --- |
| Студент гр. 6373 |  | Солодов М.П. |
| Преподаватель |  | Копыльцов |

Санкт-Петербург

2018

**Цель работы:** Ознакомиться с различными схемами разделения секретных ключей, которые используются в криптографических системах для предотвращения их несанкционированного использования.

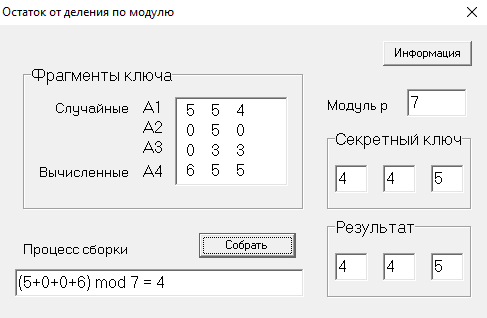
**Протокол.**

**1. Схема разделения секрета среди участников при пороге равном.**

Число участников .

Модуль .

Секретный ключ:



Вычисление A4:

Вычисление ключа:

**2. Разделение секрета среди n участников при произвольном пороге k.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| 71 | 73 | 79 | 83 | 89 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| 50 | 13 | 74 | 76 | 51 |

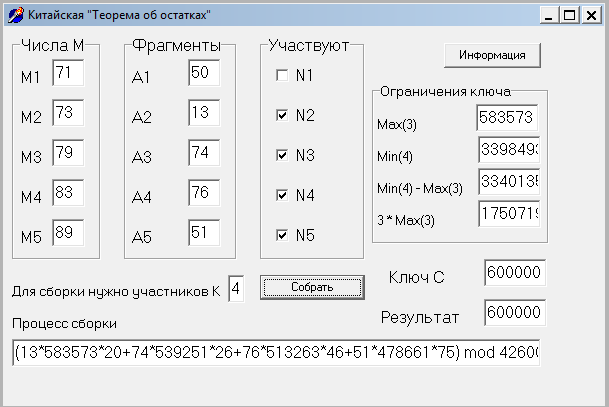
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
| 4 | 600000 | 583573 | 33984931 | 33401358 | 1750719 |

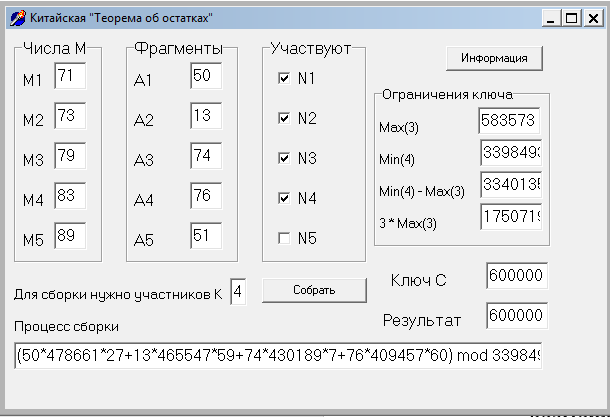
Фрагменты вычисляются по формуле

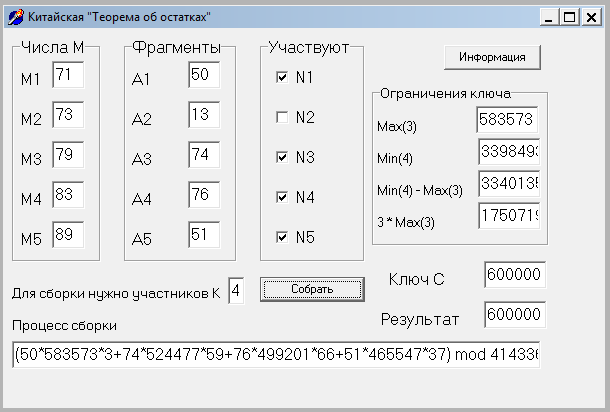
.

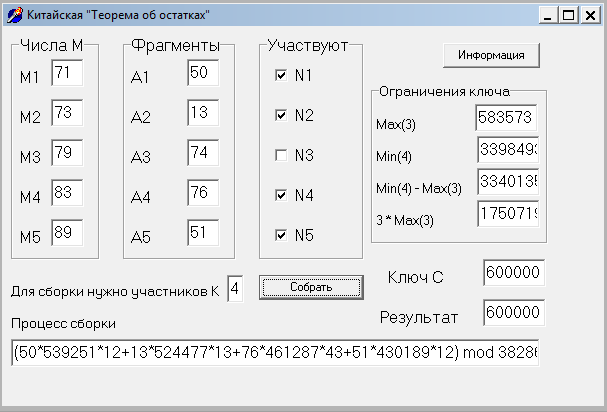
.

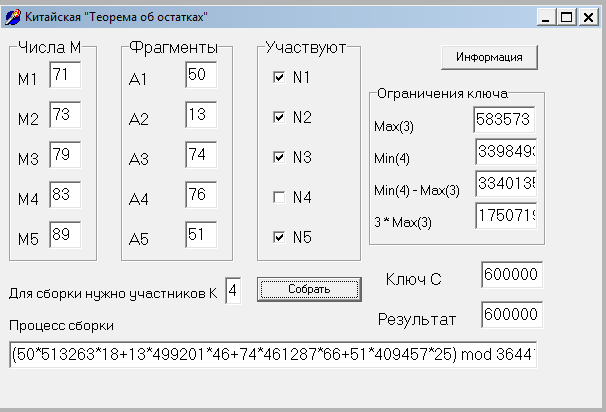
Проверка восстановления ключа для всех участников .



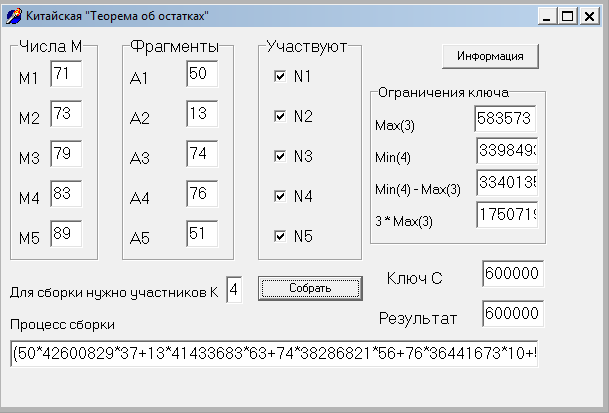




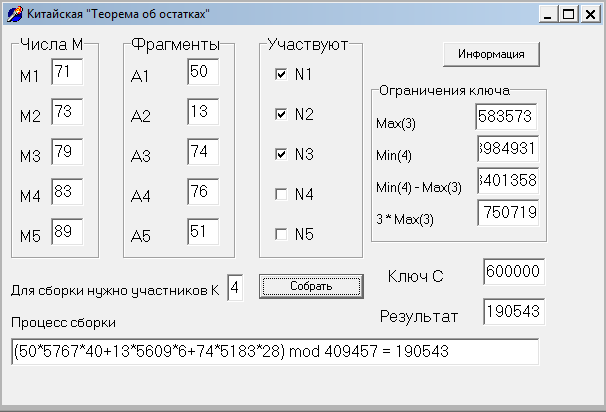




При числе участников :



При числе участников



Участники:

Вычисленный ключ: .

Истинный ключ находится из условия .

Количество возможных значений

4. **Разделение секрета среди участников при пороге , основанное на свойствах равновесных кодов.**

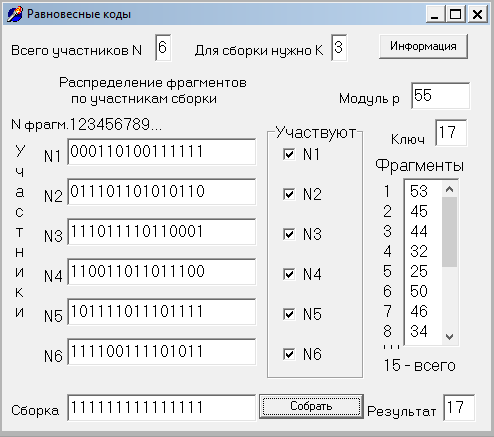
|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

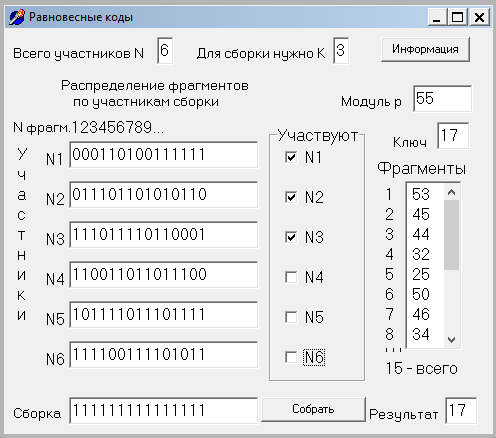
Сгенерированные фрагменты: .

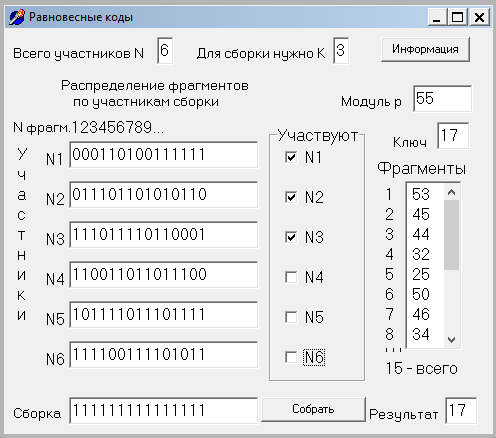
Сформируем равновесный код

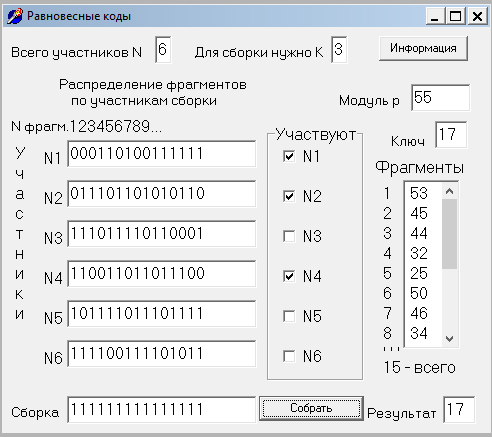
Таблица владения фрагментами:

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

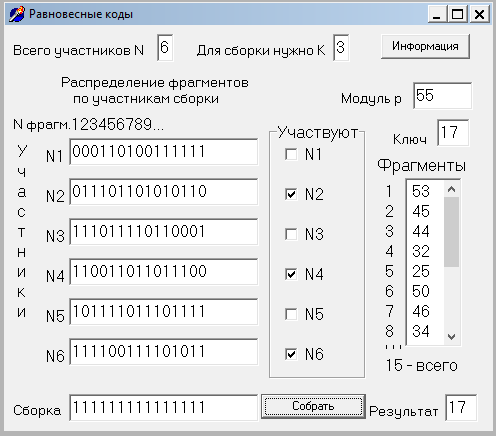
Случай, при числе участвующих равном N.

При числе участвующих равном K.

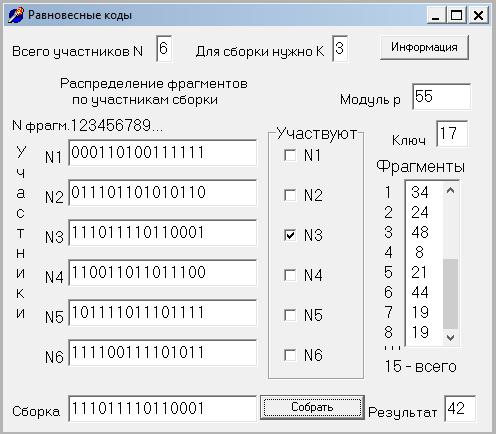
При числе участвующих равном K.



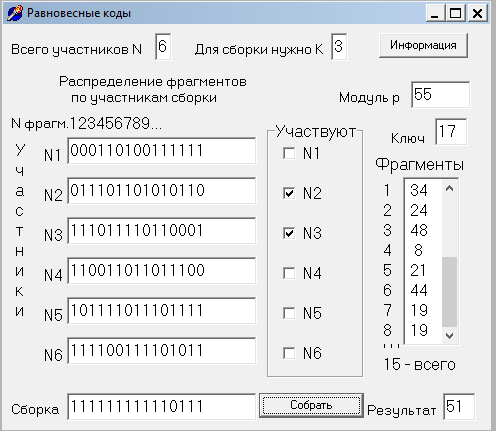
При числе участвующих равном K.



При числе участвующих равном K.

При числе участвующих

Видно, что результат отличается от Ключа.



При числе участвующих

Видно, что результат отличается от Ключа.