**ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ**

**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»**

**(СПбГУТ)**

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Дисциплина ОКОК

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ**

**ИЗУЧЕНИЕ КРИПТОПРОТОКОЛА С РАЗДЕЛЕНИЕМ СЕКРЕТНЫХ ДАННЫХ МЕЖДУ ПОЛЬЗОВАТЕЛЯМИ.**

Направление/специальность подготовки:

11.03.02 Инфокоммуникационные технологии и системы связи

*(код и наименование направления/специальности)*

Студент:

Громов А. А. ИКТЗ-83

*(Ф.И.О., № группы) (подпись)*

Проверил:

Профессор Яковлев В.А., д.т.н.

*(Ф.И.О) (подпись)*

**Цель работы:**

Закрепить знания, полученные на лекциях дисциплин “Основы криптографии с открытым ключом “ и “Криптографические протоколы” по теме «протоколы разделения секрета».

**Ход работы:**

**Часть 1.**

Провести моделирование (n,m)-схемы разделения секретов с заданными параметрами: (n=5, m=3, p=17) и параметрами в таблице 1.

| **№ вар** | **Секрет k** | **a1** | **a2** |
| --- | --- | --- | --- |
| **4** | **8** | **10** | **13** |

1. Записать полином h(x).
2. Найти тени
3. Восстановить секрет по теням 1,3,5 нечетные варианты, 2,3,4- четные варианты.

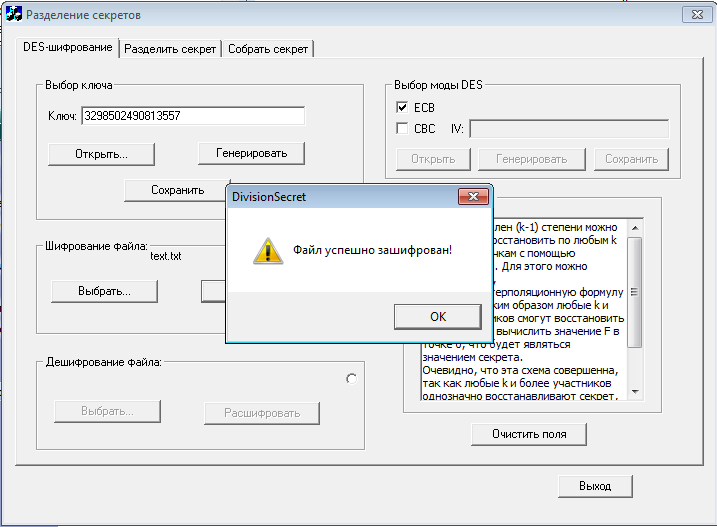
Для восстановления секрета по теням, используем интерполяционную формулу Лагранжа.

**В полученном полиноме 8 - основной секрет.**

**Часть 2. Разделение сеансового ключа**

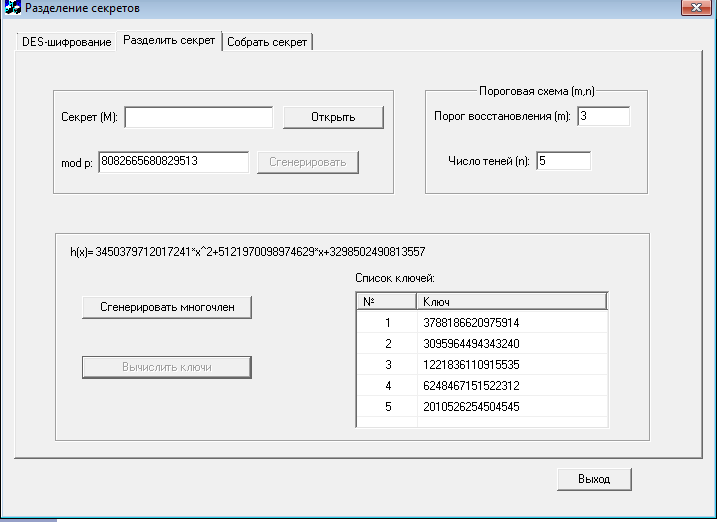
Для выполнения работы используется программа “ DivisionSecret” .

1. Перейти к программе “DivisionSecret”.
2. Создать произвольные текстовые файлы объемом не более 50-100 слов.
3. Зашифровать файл, полученный в п. 1, iшифром DES (AES) при помощи случайно сгенерированного ключа. Сохранить сгенерированный ключ в своем файле



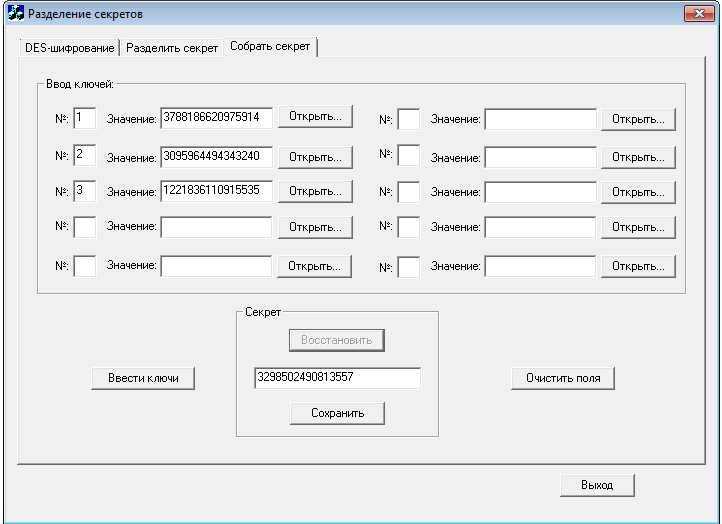
1. Выбрать параметры (*n,m)* схемы разделения секретов,

где *n<10,m<4*ипроизвести разделение “секрета”(ключа), взятого из файла по п.3.

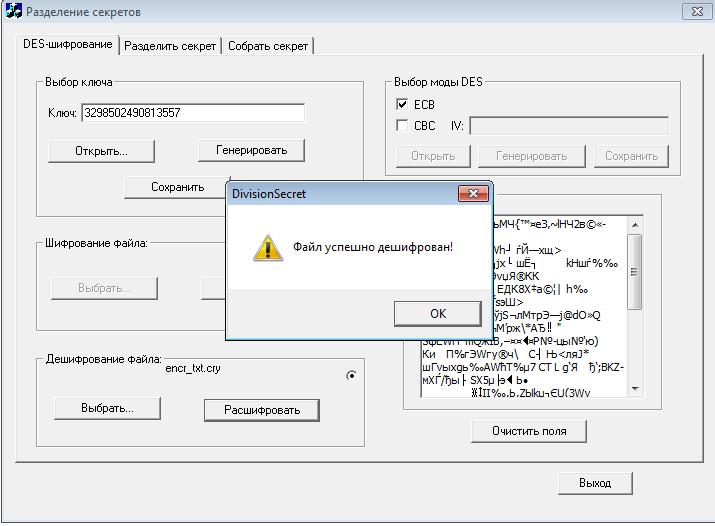


1. Восстановить основные ключи по их произвольно выбранным *m* теням.

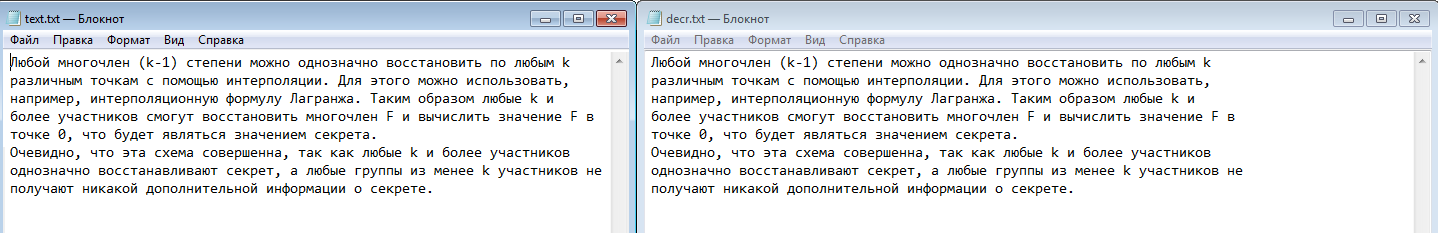
m = 3, поэтому нам требуется всего три ключа для восстановления секрета.



1. По ключам, полученным в п. 5, расшифровать алгоритмом DES (DES), полученные ранее криптограммы.

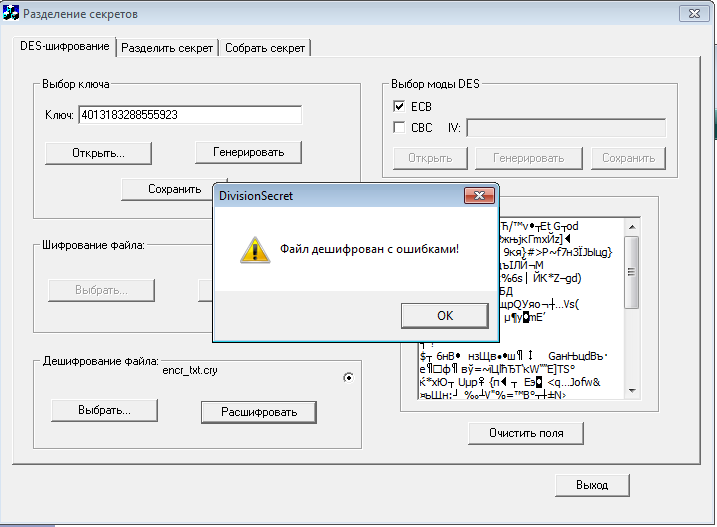


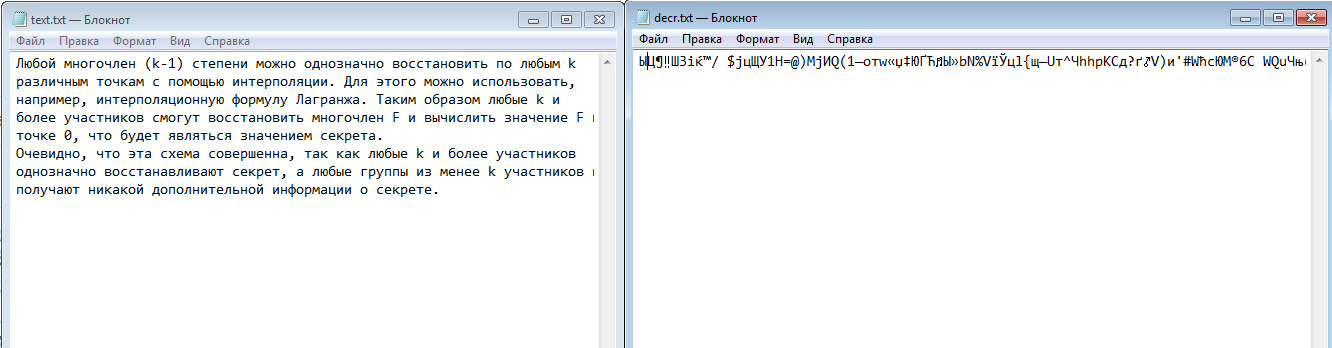
1. Проверить правильность дешифрования путем непосредственного сравнения с исходными файлами.



Текст расшифрованного файла совпадает с текстом исходного.

1. Изменив произвольные цифры в тенях, выбранных по п. 5, попытаться выработать основные ключи и дешифровать сообщения.





Текст расшифрованного файла не совпадает с текстом исходного.

**Вывод:**

В ходе выполнения данной лабораторной работы были закреплены знания по теме «Протоколы разделения секретов».