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)*

Санкт-Петербург
2021г

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). $h(x) = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \dots + a_1x + a_0$

$h(x) = 13x^2 + 10x + 8$

2. Найти тени $k_i = h(x_i)$, где $x_i = (1, 2, 3, 4, 5)$

$k_1 = h(1) = \left(13 * 1^2 + 10 * 1 + 8\right) mod\ 17 = 14$

$k_2 = h(2) = \left(13 * 2^2 + 10 * 2 + 8\right) mod\ 17 = 12$

$k_3 = h(3) = \left(13 * 3^2 + 10 * 3 + 8\right) mod\ 17 = 2$

$k_4 = h(4) = \left(13 * 4^2 + 10 * 4 + 8\right) mod\ 17 = 1$

$k_5 = h(5) = \left(13 * 5^2 + 10 * 5 + 8\right) mod\ 17 = 9$

3. Восстановить секрет по теням 1,3,5 нечетные варианты, 2,3,4- четные варианты.

$k_2 = 12,\ k_3 = 2,\ k_4 = 1$

Для восстановления секрета по теням, используем интерполяционную формулу Лагранжа.

$$h(x) = \left[\frac{12(x-3)(x-4)}{(2-3)(2-4)} + \frac{2(x-2)(x-4)}{(3-2)(3-4)} + \frac{1(x-2)(x-3)}{(4-2)(4-3)}\right] mod\ 17 =$$

$$\left[\frac{12(x^2-7x+12)}{2} - \frac{2(x^2-6x+8)}{1} + \frac{1(x^2-5x+6)}{2}\right] mod\ 17 =$$

$$= \left[12(x^2 - 7x + 12) - 4(x^2 - 6x + 8) + 1(x^2 - 5x + 6)\right] * 2^{-1} mod\ 17 =$$

$$= \left[9x^2 - 65x + 118\right] * 9\ mod\ 17 = \left[81x^2 - 585x + 1062\right] mod\ 17 =$$

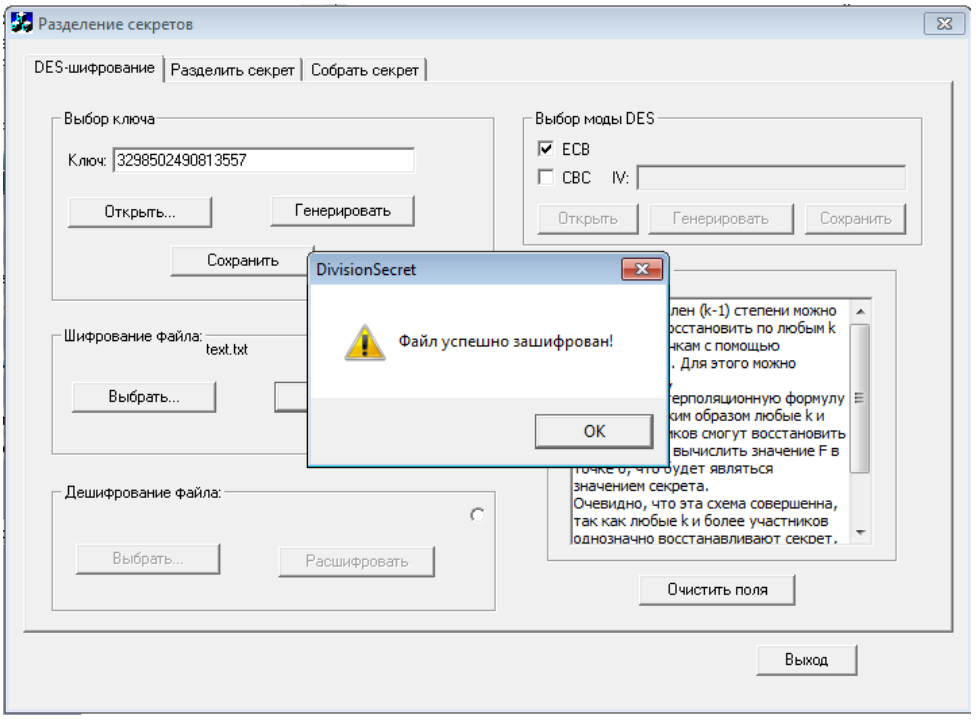
$$= 13x^2 + 10x + 8$$

В полученном полиноме $k = a_0 = 8$ - основной секрет.

Часть 2. Разделение сеансового ключа

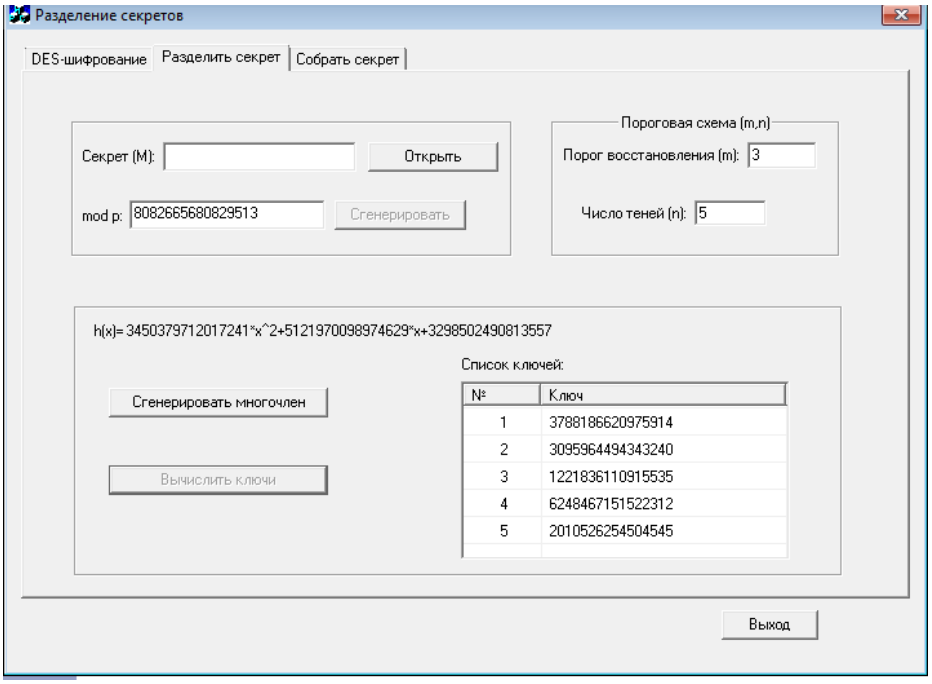
Для выполнения работы используется программа “ DivisionSecret” .

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



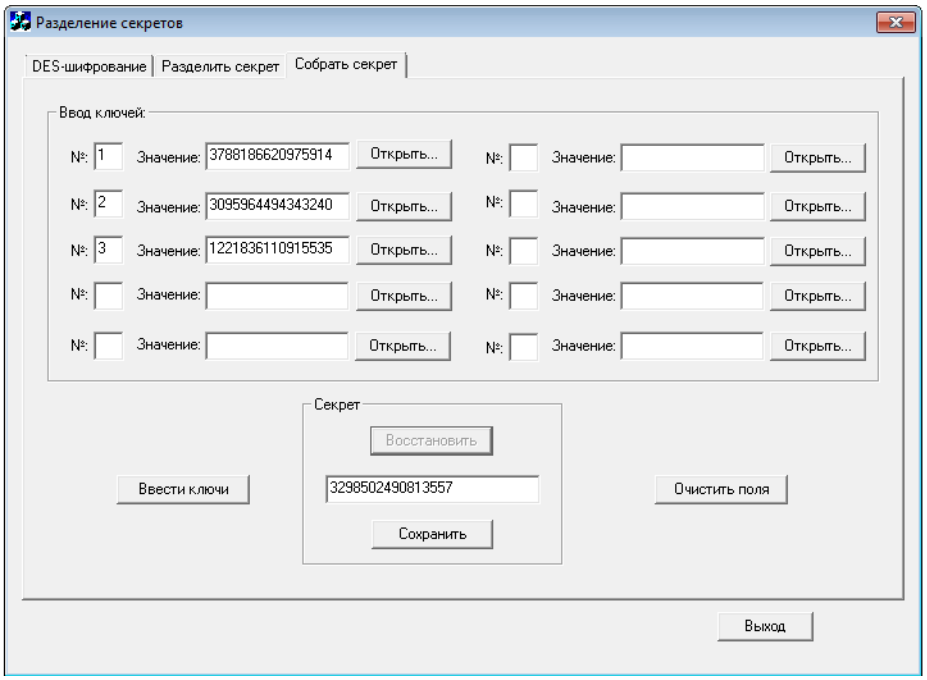
4. Выбрать параметры (*n,m)* схемы разделения секретов,

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

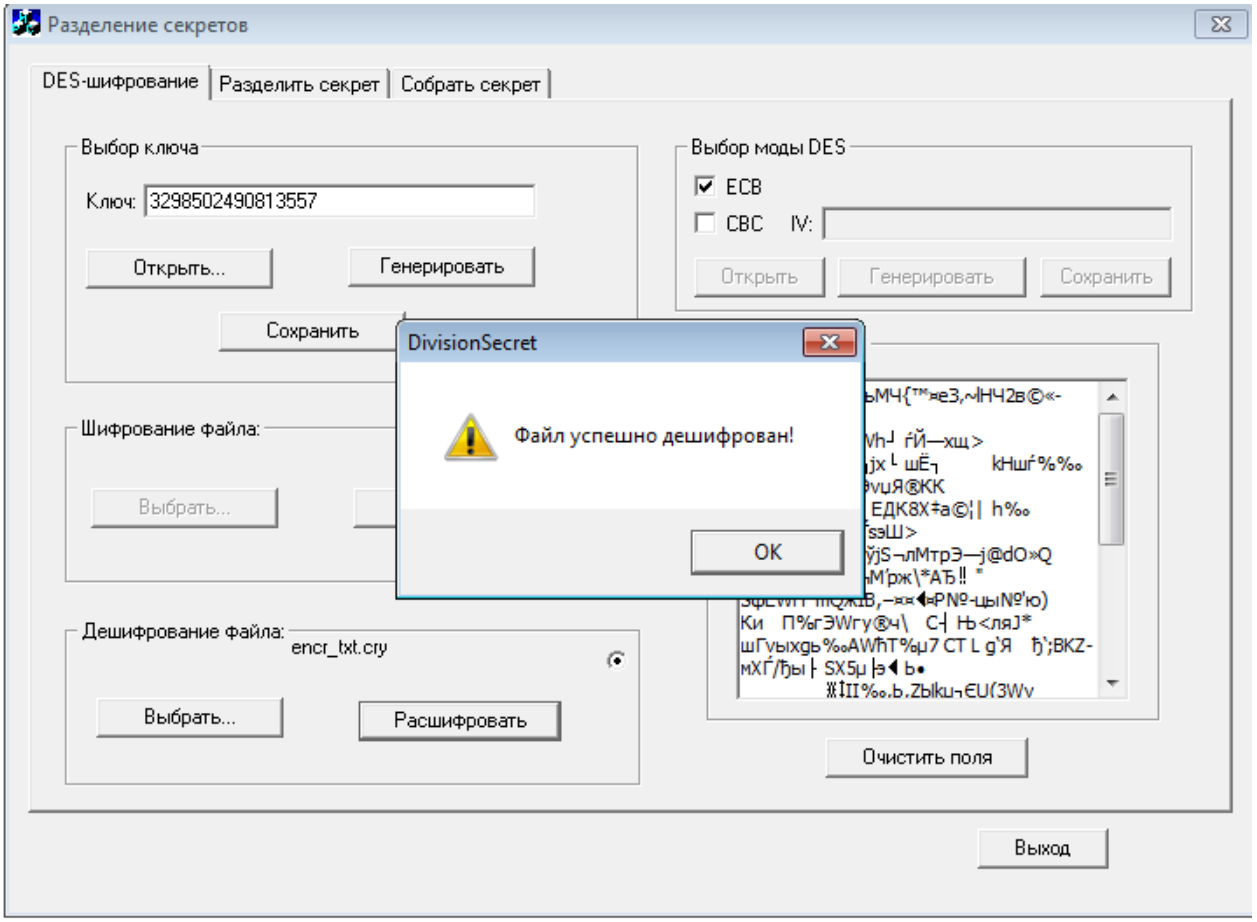


5. Восстановить основные ключи по их произвольно выбранным *m* теням.

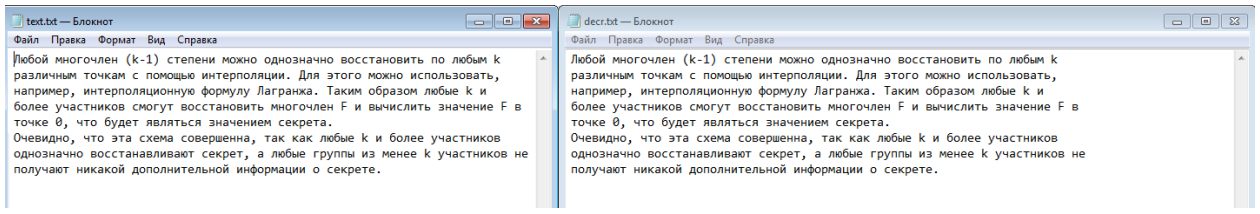
m = 3, поэтому нам требуется всего три ключа для восстановления секрета.



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

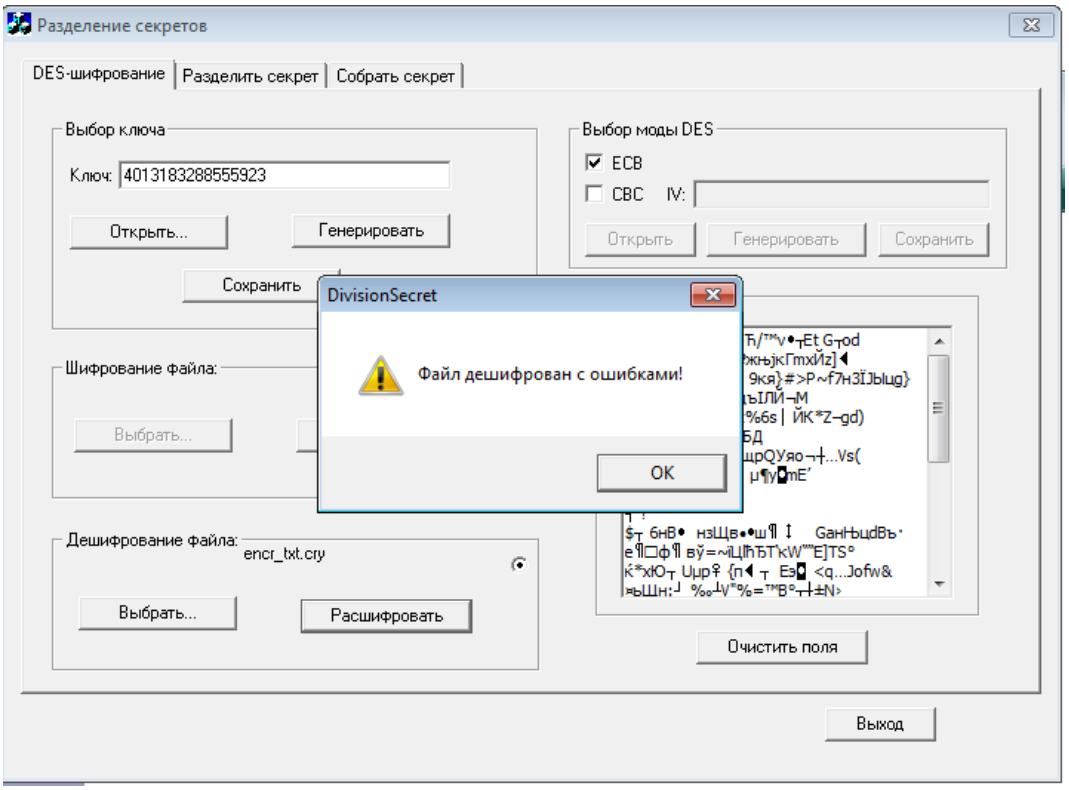


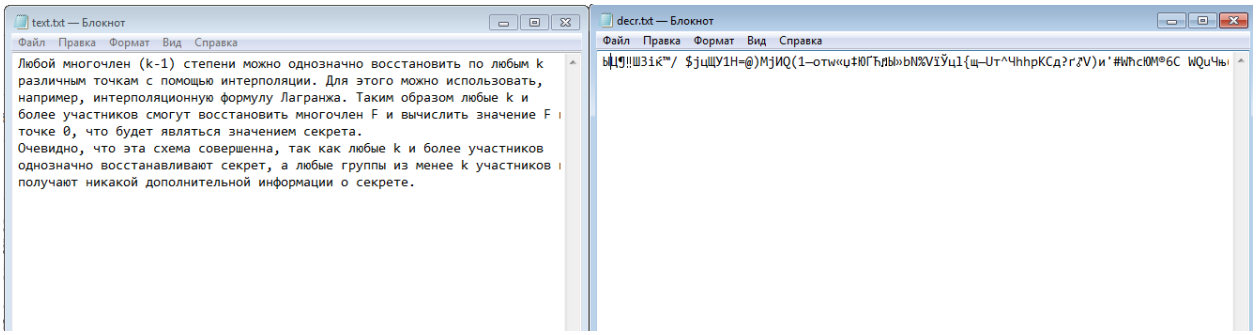
7. Проверить правильность дешифрования путем непосредственного сравнения с исходными файлами.



Текст расшифрованного файла совпадает с текстом исходного.

8. 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».