МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

федеральное государственное бюджетное образовательное учреждение высшего образования

**«Вологодский государственный университет»**

**Институт математики, естественных и компьютерных наук**

**Информатика и вычислительная техника**

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 8**

Изучение симметричного блочного алгоритма шифрования IDEA.

Дисциплина: «Защита информации»

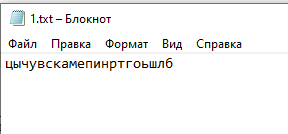
Направление подготовки: 09.03.01. Информатика и вычислительная техника

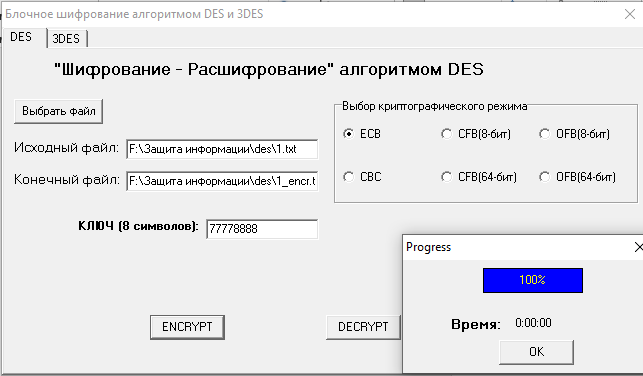
|  |  |
| --- | --- |
| Руководитель | Давыдова.Е.Н |
| Выполнили студенты | Пчелкина О.С. |
| Группа, курс | 4Б09 ВМ-41 4 курс |
| Дата сдачи | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Дата защиты | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(подпись преподавателя)* |

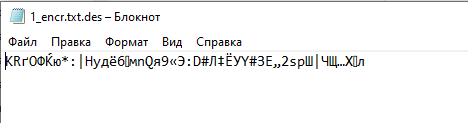
Вологда

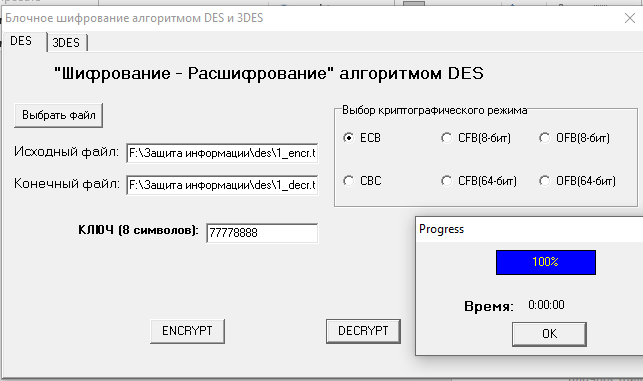
2023 г.

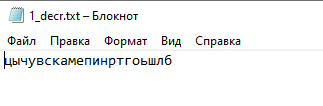
1.Ознакомление с файл-программой DES.ехе. Зашифруйте какой-нибудь файл очень небольшого размера DESом в режиме ЕСВ.



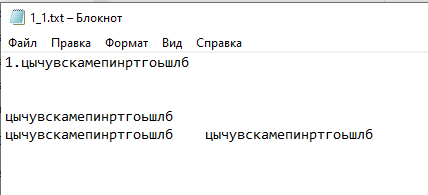


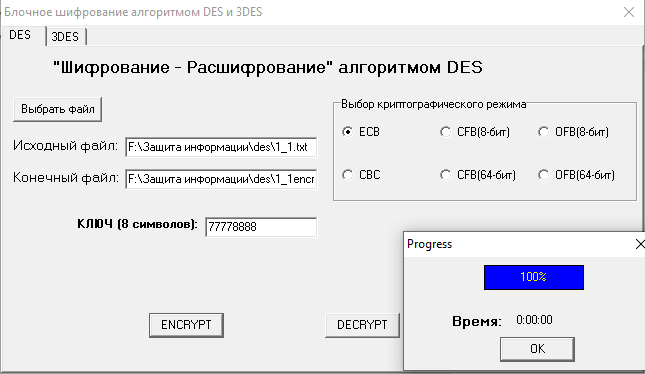


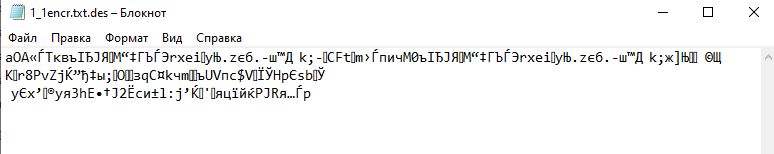


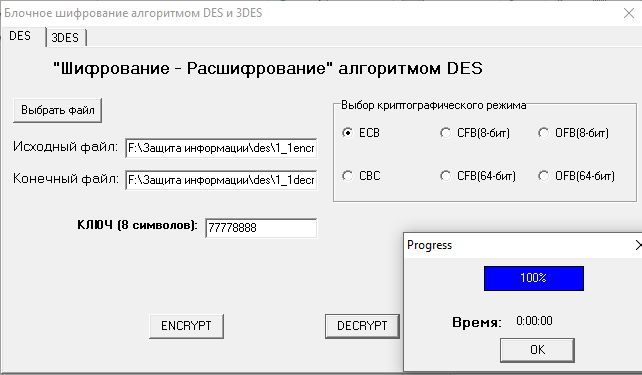


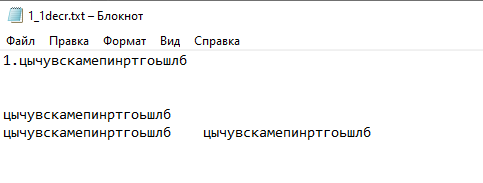
1.1Измените немного исходный файл и снова зашифруйте DESом в режиме ЕСВ. Таким образом, меняя структуру исходного файла, посмотрите, как она заставляет меняться структуру шифртекста для режима ЕСВ.





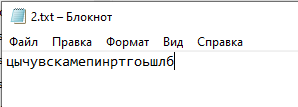


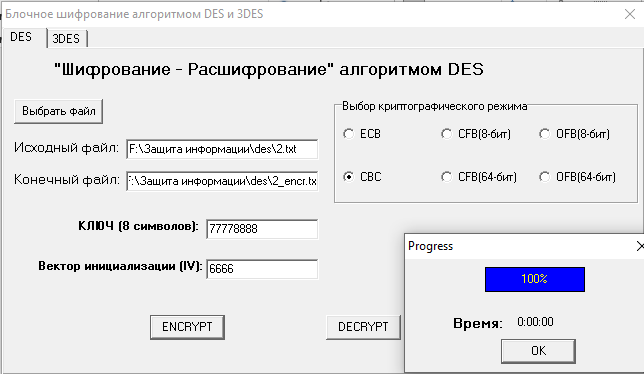


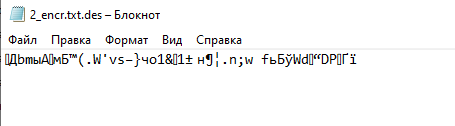


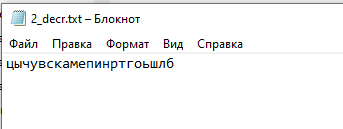
2.Проделайте все тоже самое по пункту 1. с режимами СВС,CFB(любой), OFB(любой).

CBC

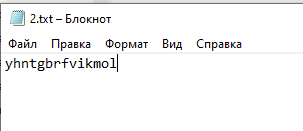


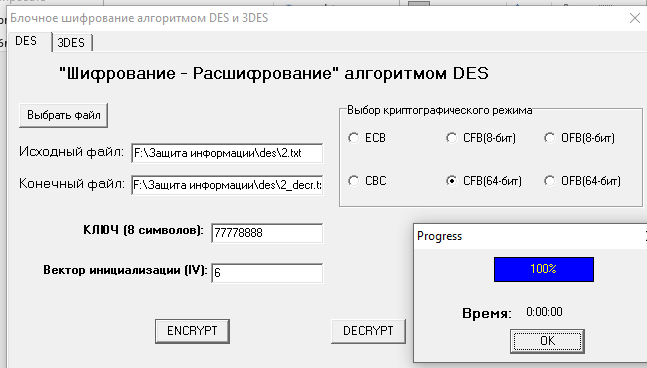


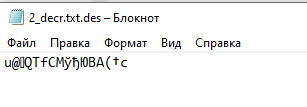


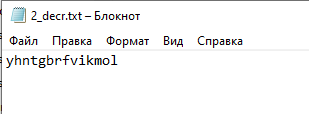


CFB(64)

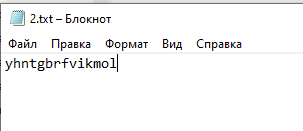


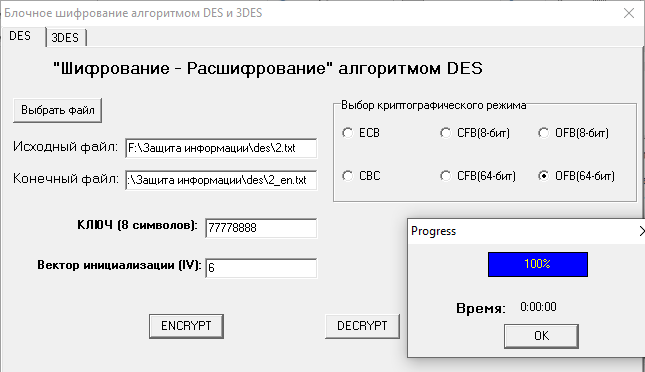


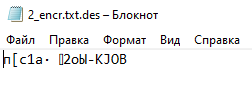


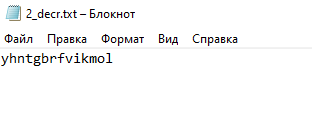


OFB(64)

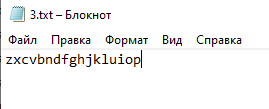


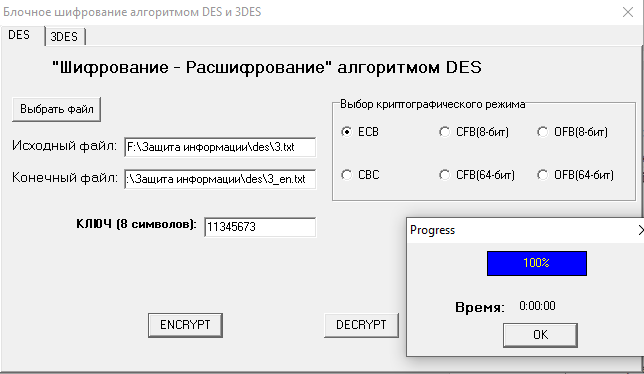


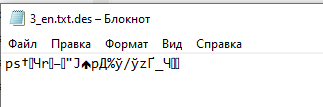




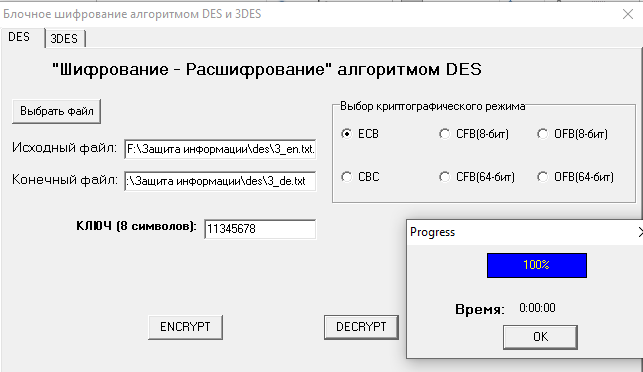
3.Зашифруйте какой-нибудь файл небольшого размера в различных режимах. Измените хотя бы один бит в ключе и расшифруйте файл.

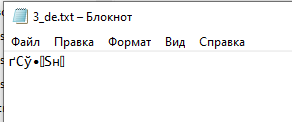




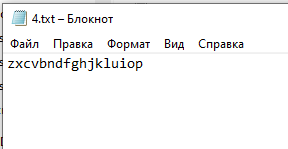


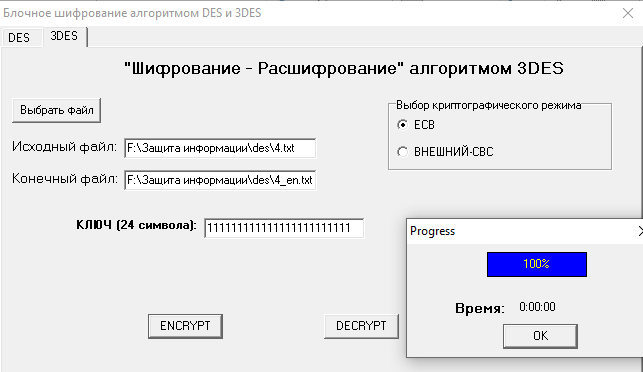
Изменение 1 символа в ключе

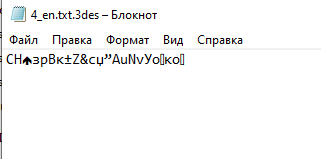


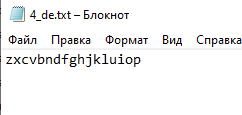


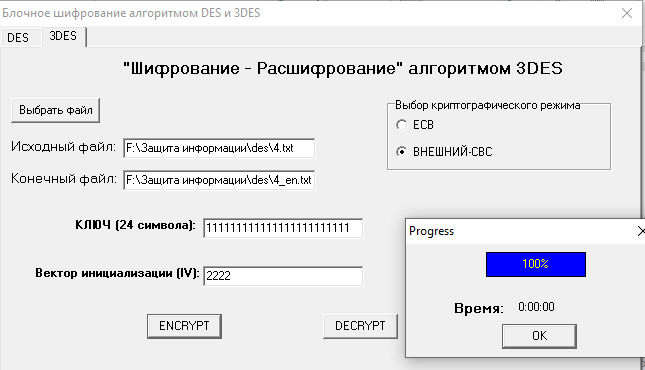
4. Зашифруйте какой-нибудь файл небольшого размера в различных режимах не ЕСВ (включая 3DES). Попробуйте зашифровать тот же файл с тем же ключом, но с другими IV.

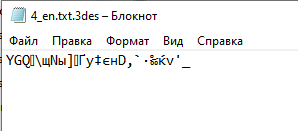


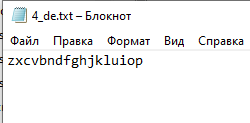




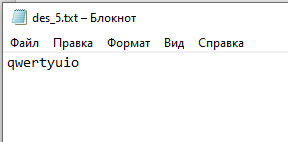


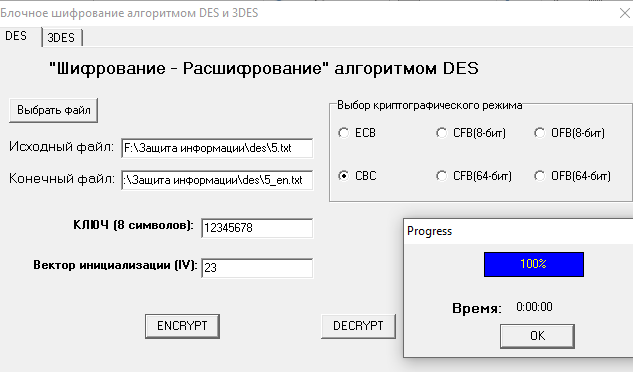


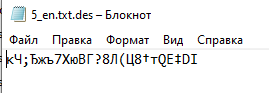


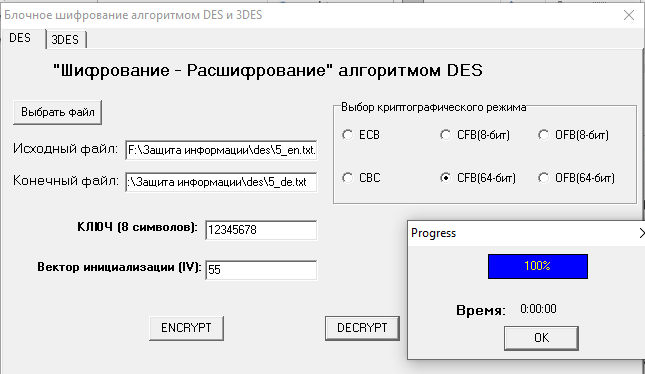


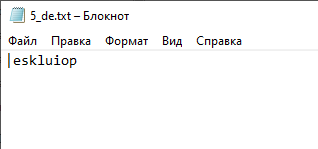
5. Попробуйте зашифровать файл в различных режимах не ЕСВ и расшифровать их тем же ключом, но совершено другим векторм инициализации.





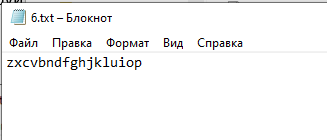


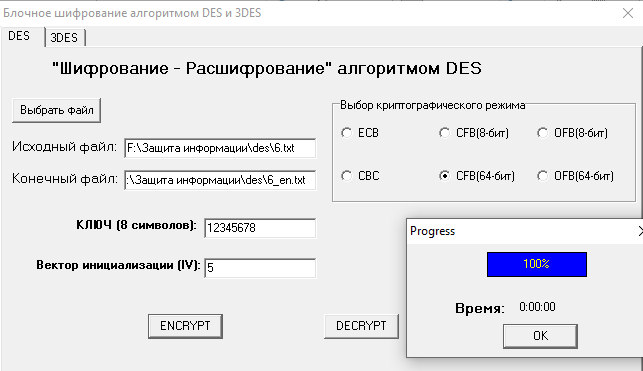


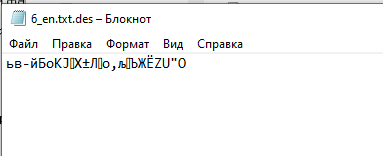


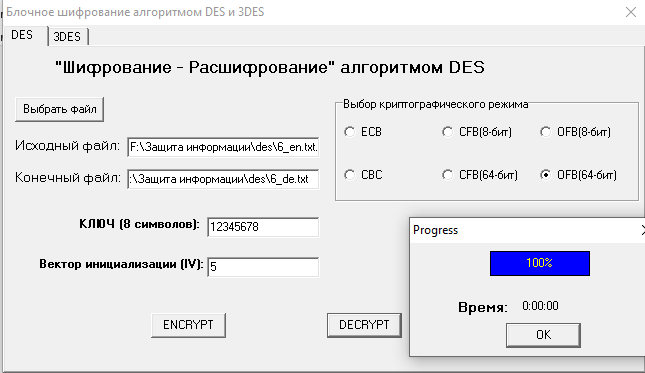
6.Попробуйте зашифровать файл в различных режимах, а расшифровывать другими режимами.

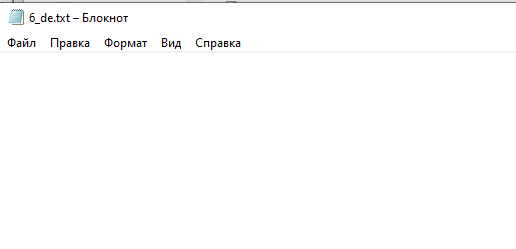
CFB(64)



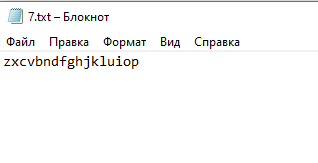


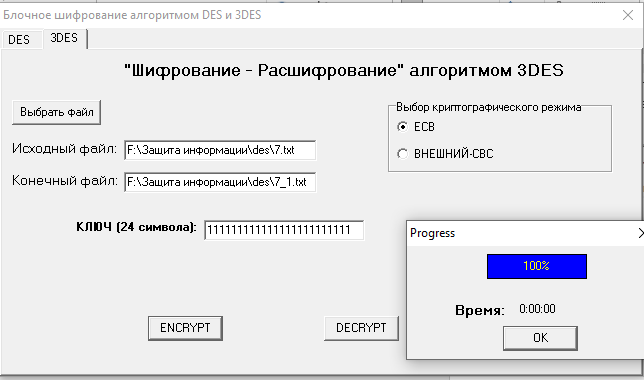


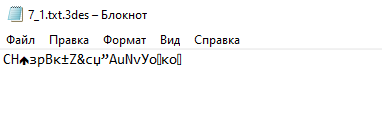


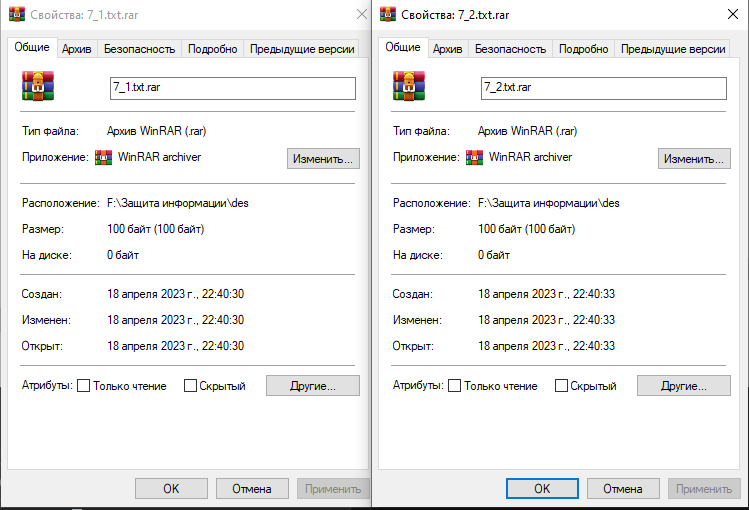


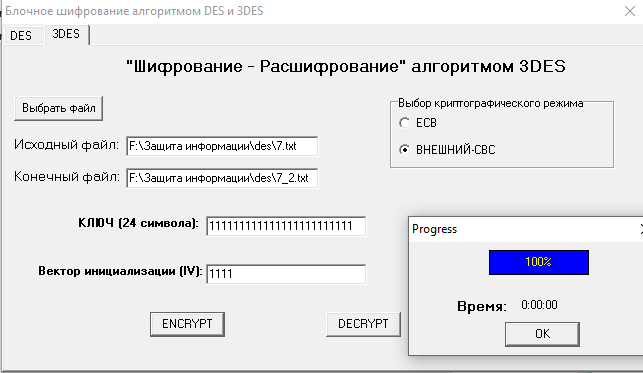
7.Зашифруйте какой-нибудь файл в различных режимах (включая 3DES). Затем попробуйте заархивировать шифртескты каким-нибудь архиватором. Сравните процент сжатия в различных режимах.

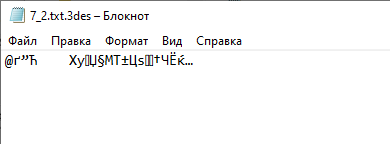




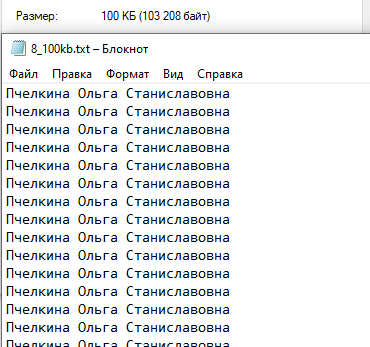


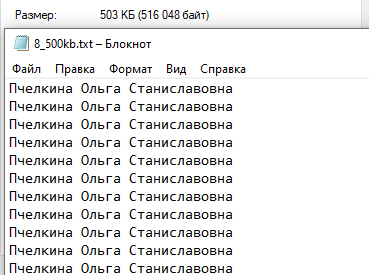


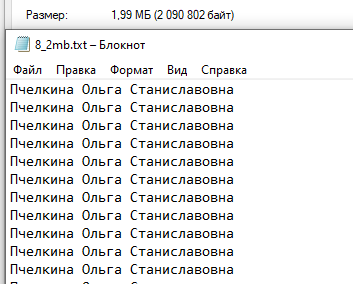




8. Проверка скорости работы алгоритмом и режимов. Вы должны провести эксперимент по шифрованию файлов алгоритмами DES и 3DES в различных режимах. Файлы можно взять размером 100кб, 500кб, 2мб. Занести результаты в таблицу







|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Алгоритм | Режим | Операция | Время  (с)  100кб | Время  (с)  500кб | Время  (с)  2мб | Скорость  (байт/с)  100кб | Скорость  (байт/с)  500кб | Скорость  (байт/с)  2мб |
| DES | ЕСВ | Шифрование | 13 | 52 | 187 | 7876,923 | 9846,154 | 1401,84 |
| Расшифрование | 13 | 53 | 186 | 7876,923 | 9660,377 | 1409,376 |
| СВС | Шифрование | 15 | 49 | 193 | 6826,667 | 10448,98 | 1358,259 |
| Расшифрование | 15 | 51 | 194 | 6826,667 | 10039,22 | 1351,258 |
| CFB(8) | Шифрование | 67 | 314 | 1264 | 1528,358 | 1630,573 | 207,3924 |
| Расшифрование | 67 | 314 | 1266 | 1528,358 | 1630,573 | 207,0648 |
| CFB(64) | Шифрование | 15 | 56 | 188 | 6826,667 | 9142,857 | 1394,383 |
| Расшифрование | 14 | 57 | 188 | 7314,286 | 8982,456 | 1394,383 |
| OFB(8) | Шифрование | 69 | 321 | 1268 | 1484,058 | 1595,016 | 206,7382 |
| Расшифрование | 68 | 320 | 1267 | 1505,882 | 1600 | 206,9013 |
| OFB(64) | Шифрование | 14 | 54 | 192 | 7314,286 | 9481,481 | 1365,333 |
| Расшифрование | 14 | 55 | 194 | 7314,286 | 9309,091 | 1351,258 |
| 3DES | ECB | Шифрование | 41 | 193 | 728 | 2497,561 | 2652,85 | 360,0879 |
| Расшифрование | 41 | 192 | 728 | 2497,561 | 2666,667 | 360,0879 |
| Вн. СВС | Шифрование | 43 | 190 | 730 | 2381,395 | 2694,737 | 359,1014 |
| Расшифрование | 43 | 191 | 729 | 2381,395 | 2680,628 | 359,594 |

Вывод: в ходе лабораторной работы зашифровали и дешифровали выбранные файлы, проверили алгоритм на помехоустойчивость и криптостойкость, а также проверили скорость работы алгоритма небольшого и большого файлов.