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.

**5.1.** Ознакомление с файл-программой DES.ехе. Зашифруйте какой-нибудь файл (лучше тесковый) очень небольшого размера DESом в режиме ЕСВ. Просмотрите зашифрованный файл и опишите увиденное. Измените немного исходный файл и снова зашифруйте DESом в режиме ЕСВ. Просмотрите зашифрованный файл, сравните с предыдущим, зашифрованным и запишите выводы в отчет.Таким образом, меняя структуру исходног файла ( например, вставляя блоки открытого текста в различные участки файла), посмотрите как она заставляет меняться структуру шифртекста для режима ЕСВ.

**5.2.** Проделайте все тоже самое по пункту 5.1. с режимами СВС,CFB(любой), OFB(любой). Сделайте выводы по криптостойкости режимов.

**5.3.** Зашифруйте какой-нибудь файл небольшого размера, сравните длину шифрованного и исходного файлов. Объясните как это получилось.

**5.4.** Зашифруйте какой-нибудь файл небольшого размера в различных режимах. Измените хотя бы один бит в ключе и расшифруйте файл. Запишите выводы (сверьте длины).

**5.5.** 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. Запишите сравнения и выводы по структуре шифртекстов.

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

**5.7.** Поробуйте зашифровать файл в различных режимах, а ррасшифровывать другими режимами. Попробуйте зашифровать DESом, а расшифровать 3DESом. Запишите выводы.

**5.8**. Зашифруйте какой-нибудь файл в различных режимах (включая 3DES). Затем попробуйте заархивировать шифртескты каким-нибудь архиватором. Сравните процент сжатия в различных режимах. Сделайте выводы и объяснения.

**5**.**9.** 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 5.1. и сделать выводы.

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.