**Лабораторная работа 2**

**Симметричные потоковые криптографические системы**

**Цель работы:** освоить навыки применения методов подстановки, аналитических преобразований, гиммирования и маршрутной перестановки.

**Краткие теоретические сведения.**

Криптосистемы подразделяются на симметричные и асимметричные (или системы с открытым ключом).

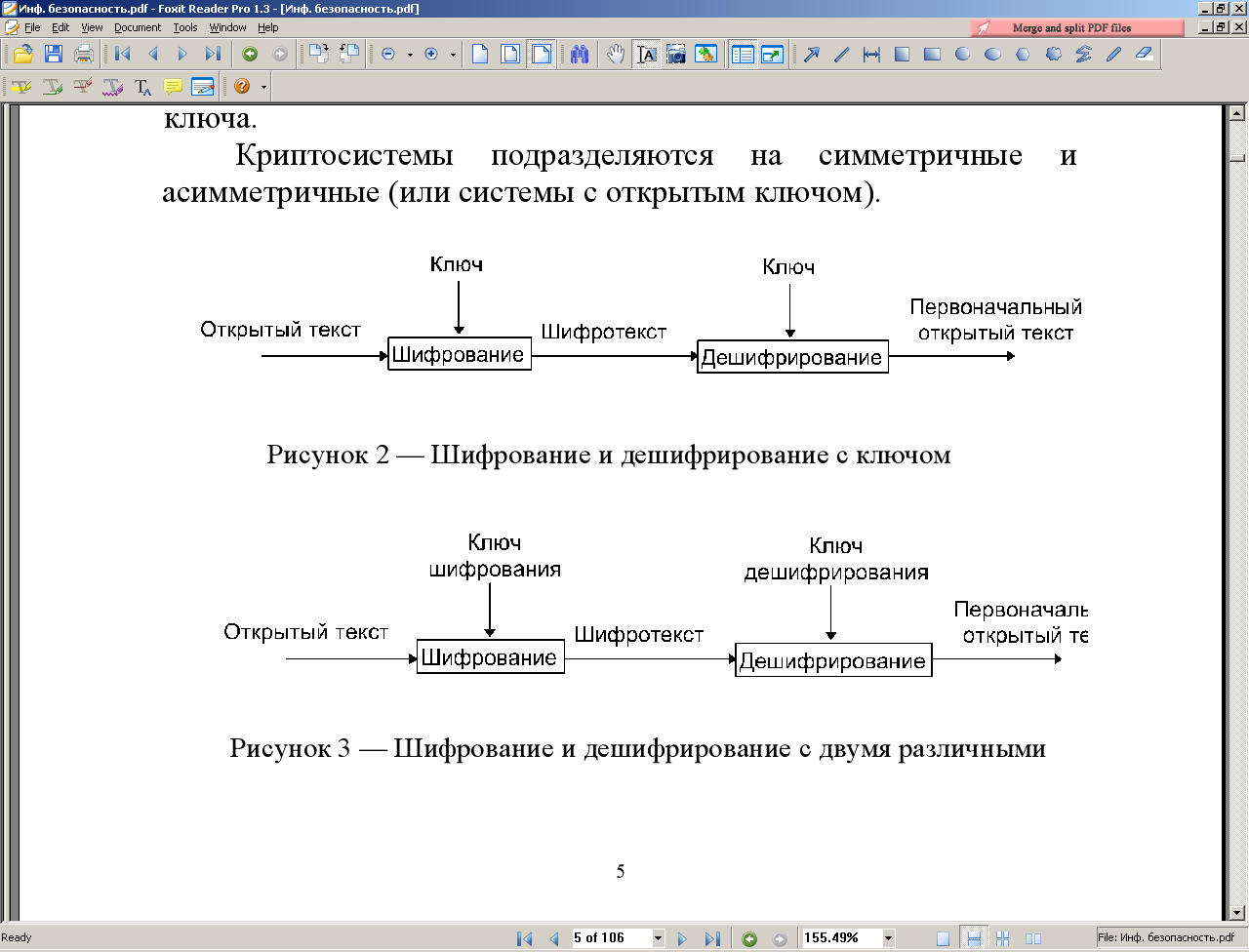


Рисунок 1 — Шифрование и дешифрирование с одним ключом

В симметричных криптосистемах для зашифрования и для расшифрования используется один и тот же ключ.

Все многообразие существующих симметричных криптографических методов можно свести к следующим классам преобразований: (рисунок 2):

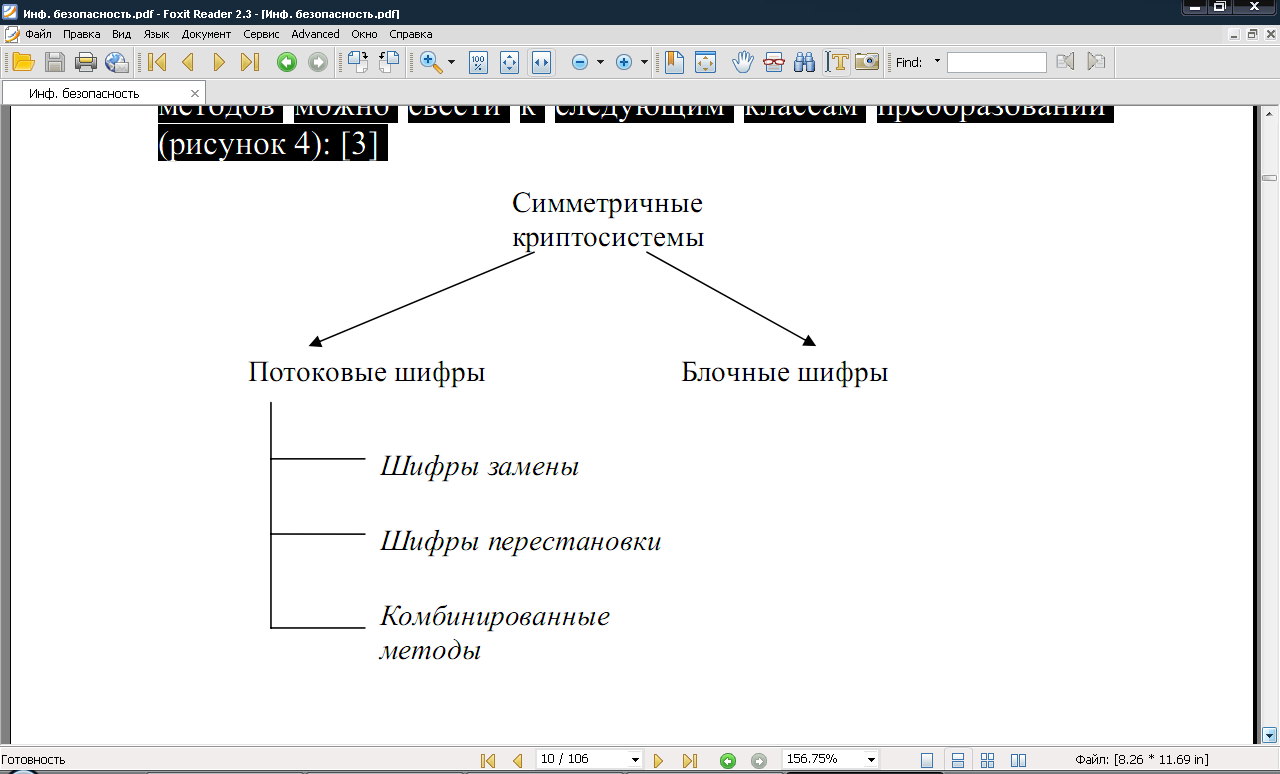


Рисунок 2 – Классификация симметричных криптосистем

**Задание.**

Разработать приложение, выполняющее шифрование и дешифрование текста в соответствии с заданным алгоритмом (табл.1).

Изменение ключа (или лозунга) не должно требовать изменения кода программы.

Протестировать работу приложения на не менее чем трех текстах от 10 до 20 символов.

Таблица 1

|  |  |
| --- | --- |
| Криптографическая система | Вариант |
| **Задание 1** | |
| Шифр Плейфера (русский алфавит). | 1, 7, 13, 19, 25 |
| Шифр Плейфера (латинский алфавит). | 2, 8, 14, 20, 26 |
| Таблица Виженера (русский алфавит). | 3, 9, 15, 21, 27 |
| Таблица Виженера (латинский алфавит). | 4, 10, 16, 22, 28 |
| Гаммирование (операция сложения по модулю, равному номеру варианта) | 5, 11, 17, 23, 29 |
| Многократное наложение гамм | 6, 12, 18, 24, 30 |
| **Задание 2** | |
| Метод умножения матриц | 1, 4, 7, 10, 13, 16, 19, 22, 25, 28 |
| Метод полиномов | 2, 5, 8, 11, 14, 17, 20, 23, 26, 29 |
| Экспоненциальный шифр | 3, 6, 9, 12, 15, 18, 21, 24, 27, 30 |
| **Задание 3** | |
| Поворотная решетка | 1-10 |
| Решетка Кардано | 11-20 |
| Вертикальная перестановка | 21-30 |

**Электронный отчет должен содержать**

Титульный лист

Название работы

Цель

Задание

Описание алгоритма

Текст программы с комментариями

Тесты, выполненные вручную

Иллюстрации правильности выполнения тестов программой

Содержательный вывод (копия цели выводом не является).

**Контрольные вопросы и задания.**

1. Кратко охарактеризовать сущность методов изученных при лабораторной выполнении работы.
2. Описать алгоритм одной из криптосистем, представленных в таблице 1.
3. Что является ключом в криптосистеме, представленной в задании, указанном преподавателем?
4. Предложить другой вариант ключа для криптосистемы, используемой при выполнении одного из заданий.
5. Зашифровать «вручную» предложенную преподавателем фразу одним из методов, содержащихся в задании к лабораторной работе (не обязательно в Вашем варианте).
6. Расшифровать «вручную» предложенную преподавателем фразу, зная метод, которым она зашифрована.