**Лабораторная работа 1**

**Шифрование и дешифрование на основе классических криптосистем**

**Цель работы:** освоить основные понятия криптологии, научиться применять простейшие криптосистемы.

**Краткие теоретические сведения.**

Проблемой защиты информации путем ее преобразования занимается **криптология.**

Криптология разделяется на два направления - криптографию и криптоанализ.

Цели этих направлений прямо противоположны.

**Криптография** занимается поиском и исследованием методов преобразования информации с целью скрытия ее содержания.

Сфера интересов **криптоанализа** - исследование возможности расшифровывания информации без знания ключей,

Основные направления использования криптографических методов - передача конфиденциальной информации по каналам связи (например, электронная почта),

установление подлинности передаваемых сообщений,

хранение информации (документов, баз данных) на носителях в зашифрованном виде.

Итак, криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

В качестве информации, подлежащей шифрованию и расшифрованию, будут рассматриваться тексты, построенные на некотором алфавите.

**Шифрование данных** - процесс преобразования открытых данных в зашифрованные данные (шифртекст, криптограмму) при помощи ключа.

Вместо термина «открытые данные» часто употребляются термины открытый текст и исходный текст, а вместо «зашифрованные данные» — шифрованный текст.

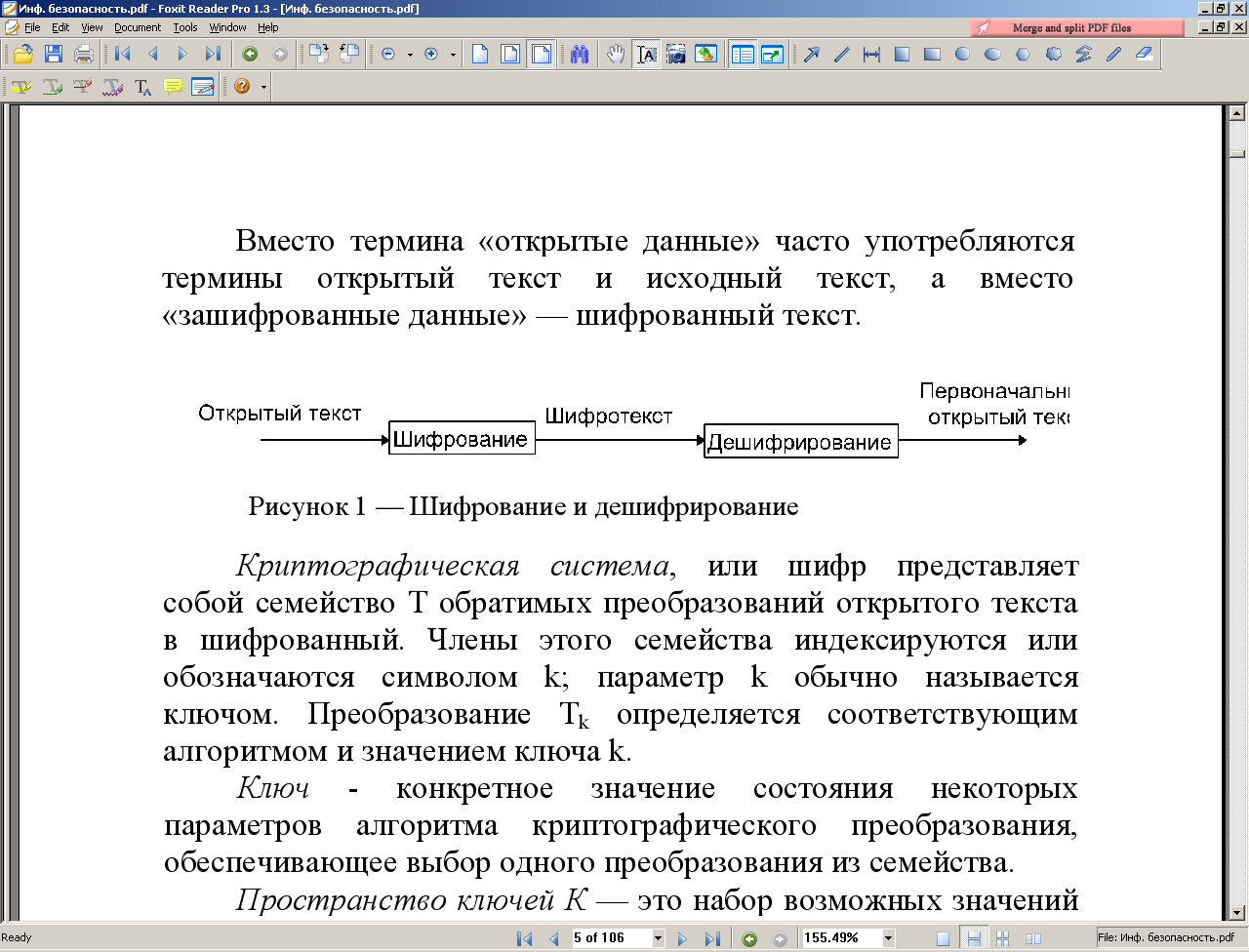


Рисунок 1 — Шифрование и дешифрирование

**Криптографическая система**, или шифр представляет собой семейство Т обратимых преобразований открытого текста в шифрованный. Члены этого семейства индексируются или обозначаются символом k; параметр k обычно называется ключом.

Преобразование Т определяется соответствующим k алгоритмом и значением ключа k.

**Ключ** - конкретное значение состояния некоторых параметров алгоритма криптографического преобразования, обеспечивающее выбор одного преобразования из семейства.

**Пространство ключей К** — это набор возможных значений ключа.

**Задание.**

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

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

Таблица 1

|  |  |
| --- | --- |
| Криптографическая система | Вариант |
| **Задание 1** | |
| Шифр Цезаря (шаг сдвига соответствует варианту). | Четные варианты |
| Цифровая система тайнописи (соответствие цифр и букв выбрать самостоятельно). | Нечетные варианты |
| **Задание 2** | |
| Квадрат Полибия (для латинского алфавита) | 1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31 |
| Квадрат Полибия (для русского алфавита) | 2, 5, 8, 11, 14, 17, 20, 23, 26, 29 |
| Магический квадрат | 3, 6, 9, 12, 15, 18, 21, 24, 27, 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. Дать определение понятия «криптосистема», «шифрование», дешифрование», «ключ», «семейство ключей».
2. Сравнить понятия «криптология», «криптоанализ», «криптография».
3. Описать алгоритм одной из криптосистем, представленных в таблице 1.
4. Что является ключом в криптосистеме, представленной в задании, указанном преподавателем?
5. Предложить другой вариант ключа для криптосистемы, используемой при выполнении одного из заданий.
6. Зашифровать «вручную» предложенную преподавателем фразу одним из методов, содержащихся в задании к лабораторной работе (не обязательно в Вашем варианте).
7. Расшифровать «вручную» предложенную преподавателем фразу, зная метод, которым она зашифрована.