Лабораторная работа №2

Wang Yao

RUDN University, Moscow, Russian Federation

3 января 2026

Цель работы

Изучить основные принципы и методы шифров перестановки, включая маршрутное шифрование, шифр Виженера и шифрование решетками. Проанализировать их криптостойкость и историческое значение.

Ход лабораторной работы

Введение в шифры перестановки

• **Определение**: Криптографические алгоритмы, изменяющие порядок символов без изменения их содержания

• **Основной принцип**: Перестановка символов открытого текста согласно определенному правилу

• **Историческое значение**: Широко использовались в военной и дипломатической переписке

• **Ключевое требование**: Равенство длин ключа и исходного текста

Маршрутное шифрование

• **История**: Разработано Франсуа Виетом, использовалось Мата Хари

• **Алгоритм**: - Текст записывается в таблицу m × n построчно - Столбцы переупорядочиваются по алфавитному порядку пароля - Шифртекст формируется чтением по столбцам

Шифр Виженера

• **История**: Опубликован в 1585 году, считался нераскрываемым до 1863 года

• **Принцип работы**: Многоалфавитная замена с использованием ключевого слова

• **Математическая модель**:

$$C_i = (P_i + K_i) \pmod{m}$$

где P_i - буква открытого текста, K_i - буква ключа, m - размер алфавита

Шифрование решетками

- **Автор**: Эдуард Флейснер (1881 год)
- **Принцип работы**: - Создание вращающейся решетки размером $2k \times 2k$ - Последовательное заполнение в 4 положениях (0°, 90°, 180°, 270°) - Чтение по столбцам согласно паролю

Реализация и тестирование

Маршрутное шифрование: - Вход: “нельзя недооценивать противника” - Пароль: “пароль”, размер: 5×6 - Выход: “ЕЕНПНЗОАТАЬОВОКННЕЬВЛДИРИЯЦТИА”

Шифр Виженера: - Вход: “криптография серьезная наука” - Ключ: “математика” - Выход: “ЦРЪФЮОХШКФФЯГКЬЬЧПЧАЛНТШЦА”

Шифр решетками: - Вход: “договор подписали” - Пароль: “шифр”, k = 2 - Выход: “ОВОРДЛГПАПИОСДОИ”

Сравнительный анализ

Параметр	Маршрутное	Виженера	Решетки
Безопасность	Низкая	Средняя	Высокая
Сложность	Простая	Средняя	Высокая
Гибкость	Высокая	Средняя	Низкая
Тип ключа	Пароль	Ключевое слово	Пароль + решетка

Криптоанализ и уязвимости

Общие уязвимости: - Сохранение частотных характеристик языка - Уязвимость к анаграммному анализу - Ограниченное пространство ключей

Специфические уязвимости: - Маршрутное: угадывание размеров таблицы - Виженера: периодичность ключа (метод Казиски) - Решетки: сложность создания, но уязвимость при известной решетке

Вывод

Изучили основные методы шифров перестановки, включая маршрутное шифрование, шифр Виженера и шифрование решетками. Эти методы демонстрируют историческое развитие криптографических техник.

Основные выводы:

• **Теоретическая ценность**: Понимание исторического развития криптографии

• **Практическая значимость**: Основа для изучения современных алгоритмов

• **Криптостойкость**: Недостаточна для современных требований

• **Образовательная ценность**: Отличные примеры для изучения базовых принципов

• **Итоговый вывод**: Шифры перестановки демонстрируют эволюцию от простых к более сложным методам, подчеркивая важность как алгоритмической, так и физической безопасности в криптографии.

Литература

1. Основы криптографии: учебное пособие. — М.: Горячая линия-Телеком, 2020.