Шифры перестановки

Теория, реализация и анализ

Студент: Ван Яо
Группа: НФИмд-01-25
РУДН, 2025

Содержание

1. 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

2. 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

3. 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

4. Шифрование решетками

• Автор: Эдуард Флейснер (1881 год)

• Принцип работы:

Создание вращающейся решетки размером 2k × 2k

Последовательное заполнение в 4 положениях (0°, 90°, 180°, 270°)

Чтение по столбцам согласно паролю

• Процесс создания решетки:

Создание базового квадрата k × k с числами $1 - k^2$

Поворот и объединение в большой квадрат

Вырезание отверстий для записи текста

5. Сравнительный анализ

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

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

7. 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

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

Спасибо за внимание!