Шифры простой замены

Теория, реализация и анализ

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

Содержание

1. Введение в шифры замены

• **Шифр простой замены -** замена символов открытого текста на символы шифроалфавита • **Моноалфавитная подстановка -** каждый символ заменяется фиксированно • **Историческое значение**: древнейшие криптографические методы • **Применение**: образовательные цели, основы криптографии

2. Шифр Цезаря

• **История**: использовался Юлием Цезарем в I веке до н.э. • **Математическая модель**:

$$T^j(a) = (a + j) mod m$$

• **Ключ**: величина сдвига j • **Пример**:
Исходный: “VENI VIDI VICI”
Зашифрованный: “YHQL YLGL YLFL”

3. Шифр Атбаша

• **Принцип**: зеркальное отображение алфавита • **Математическая модель**:

$$T(a) = (m - 1 - a)$$

• **Особенность**: отсутствие ключа, фиксированное преобразование
• **Пример для русского алфавита**:
а → я, б → ю, в → э, …, я → а

4. Криптоанализ и уязвимости

Уязвимости шифра Цезаря: - Малое пространство ключей $(m-1)$ вариантов - Сохранение частотных характеристик - Уязвимость к частотному анализу

Уязвимости шифра Атбаша:

- Отсутствие ключа
- Самодвойственность
- Уязвимость к частотному анализу

5. Сравнительный анализ

Параметр	Цезарь	Атбаш
Пространство ключей	$m - 1$	1
Сложность взлома	Низкая	Очень низкая
Гибкость	Есть	Нет
Историческое значение	Высокое	Среднее

6. Заключение и выводы

• **Теоретическая ценность**: изучение основ криптографии • **Практическая значимость**: образовательные цели • **Криптостойкость**: низкая, не пригодны для защиты информации • **Рекомендации**: использовать только для обучения основам криптографии

• **Вывод**: Шифры простой замены служат отличным инструментом для понимания базовых принципов криптографии, но абсолютно не пригодны для современных требований информационной безопасности.

Спасибо за внимание!