Лабораторная работа №1

Wang Yao

RUDN University, Moscow, Russian Federation

3 January, 2026 Moscow

Цель работы

Разобраться с основными принципами функционирования шифров замены. Изучить исторические шифры простой замены, их математические модели, уязвимости и применение в образовательных целях.

Ход лабораторной работы

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

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 текст: “VENI VIDI VICI”

Зашифрованный текст: “YHQL YLGL YLFL”

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

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

Сравнительный анализ

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

Вывод

Изучили основы функционирования шифров замены, включая шифры Цезаря и Атбаша. Эти шифры имеют важное теоретическое значение для понимания базовых принципов криптографии, но обладают низкой криптостойкостью из-за ограниченного пространства ключей и сохранения частотных характеристик текста.

Основные выводы:

- Шифры простой замены служат отличным инструментом для образовательных целей
- Они демонстрируют фундаментальные принципы криптографии
- Абсолютно не пригодны для современных требований информационной безопасности
- Рекомендуется использовать только для обучения основам криптографии

Литература

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