Лабораторная работа №3

Wang Yao

RUDN University, Moscow, Russian Federation

3 января 2026

Цель работы

Изучить принципы шифрования гаммированием, реализовать два подхода (конечная гамма и линейный конгруэнтный генератор) и провести сравнительный анализ их характеристик.

Ход лабораторной работы

Введение в гаммирование

• **Определение**: Наложение гаммы (псевдослучайной последовательности) на открытый текст

• **Историческое развитие**: - Схема однократного использования (one-time pad) - Гаммирование с конечной гаммой - Гаммирование с генератором ПСП

• **Основное преимущество**: Высокая скорость и простота реализации

• **Ключевой принцип**:

$$c_i = p_i \oplus \gamma_i$$

Математические основы

Основные операции: - Шифрование: $c_i = (p_i + \gamma_i) \mod N$ - Дешифрование: $p_i = (c_i - \gamma_i) \mod N$

Алфавитное кодирование: а = 1, б = 2, в = 3, ..., я = 32, пробел = 0

Модуль $N = 33$

Реализация конечной гаммы

• **Метод**: Использование заранее подготовленной гаммы фиксированной длины

• **Особенности**: - Простая реализация - Ограниченная длина гаммы - Повторное использование снижает безопасность

Линейный конгруэнтный генератор (LCG)

Математическая модель:

$$\gamma_i = (a \cdot \gamma_{i-1} + b) \mod m$$

Параметры генератора: - a - множитель - b - приращение - m - модуль - γ_0 - начальное значение (seed)

Сравнительный анализ методов

Параметр	Конечная гамма	LCG гамма
Безопасность	Низкая	Средняя
Простота	Высокая	Средняя
Периодичность	Короткая	Длинная
Реализация	Простая	Сложная
Ключевое пространство	Ограниченное	Большое

Криптоанализ и уязвимости

Общие уязвимости: - Статистический анализ шифротекста - Возможность восстановления гаммы при известном открытом тексте - Ограниченная периодичность псевдослучайных последовательностей

Специфические уязвимости: - Конечная гамма: повторное использование, ограниченная длина - LCG: предсказуемость последовательности, линейная зависимость

Вывод

Изучили принципы и методы шифрования гаммированием, реализовали два подхода: с использованием конечной гаммы и линейного конгруэнтного генератора.

Основные выводы:

• **Теоретическая ценность**: Понимание принципов потокового шифрования

• **Практическая значимость**: Основа для изучения современных потоковых шифров

• **Образовательные результаты**: - Реализация двух подходов к гаммированию - Сравнительный анализ методов - Понимание ограничений и уязвимостей

• **Итоговый вывод**: Гаммирование остается важным классом криптографических алгоритмов, сочетающим простоту реализации с потенциально высокой стойкостью при правильном использовании.

Литература

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