УДК 004.056.55

Студ. А.А. Бестемяникова
Науч. рук. ассист. Д.В. Сазонова
(кафедра информационных систем и технологий, БГТУ)

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ШИФРОВАНИЯ ПЛЕЙФЕРА, ВЕРНАМА, ВИЖЕНЕРА И КАРДАНО

Криптография играет ключевую роль в защите информации, и выбор алгоритма шифрования напрямую влияет на безопасность данных. В данной работе проводится сравнительный анализ четырёх методов: шифра Виженера, шифра Плейфера, шифра Вернама и решётки Кардано. Каждый из них имеет уникальные особенности, определяющие их криптостойкость, область применения и уязвимости.

Шифр Виженера [1]. Шифр Виженера – это полиалфавитный шифр подстановки, который является усложнённой версией шифра Цезаря. В нём для шифрования используется ключевое слово, которое определяет сдвиг для каждого символа открытого текста. Например, при шифровании слова «ATTACKATDAWN» с ключом «LEMON» получиться «LXFOPVEFRNHR». Каждая буква ключа определяет сдвиг в алфавите: A (0) + L (11) → L (11), T (19) + E (4) → X (23) и так далее. Этот метод обладает рядом преимуществ: он устойчив к простому частотному анализу (в отличие от шифра Цезаря) и легко реализуется даже вручную. Однако при коротком или повторяющемся ключе он становится уязвим к атаке Казиски и методу Кирхгофа. Формула шифра:

$$C_i = (P_i + K_{i \bmod len(K)}) \bmod N,$$

где C_i – символ шифротекста, P_i – символ открытого текста, K – ключ, N – мощность алфавита.

Шифр Плейфера. Более совершенным методом является шифр Плейфера, основанный на использовании биграмм. Изобретен в 1854 году английским физиком Чарльзом Уитстоном. Алгоритм использует квадрат 5×5, заполненный буквами. Шифрование происходит путём замены пар символов по определённым правилам: если буквы находятся в одной строке, они заменяются на соседние справа; если в одном столбце – на нижние; в остальных случаях образуют прямоугольник, и берутся противоположные углы.

Этот метод обладает повышенной устойчивостью к частотному анализу, так как заменяет пары символов. Однако он уязвим к атакам на основе известного открытого текста и требует предварительной подготовки таблицы. По сравнению с Виженером, Плейфер устойчивее к частотному анализу, но сложнее в реализации.

Шифр Вернама. Изобретен в 1917 году. Совершенно иной подход демонстрирует шифр Вернама (одноразовый блокнот), обеспечивающий абсолютную криптографическую стойкость. В этом методе каждый бит открытого текста складывается с битом случайного ключа с помощью операции XOR. Например, для шифрования буквы «А» (01000001) с ключом 10011010 получаем шифротекст 11011011.

Главное преимущество этого метода – его абсолютная стойкость при соблюдении трёх условий: ключ должен быть истинно случайным, использоваться только один раз и быть равным по длине сообщению. Однако на практике этот метод непрактичен для больших объёмов данных, так как требует передачи ключа, сравнимого по размеру с самим сообщением.

Схема передачи сообщений с использованием шифрования методом Вернама показана на рис.1 [3].

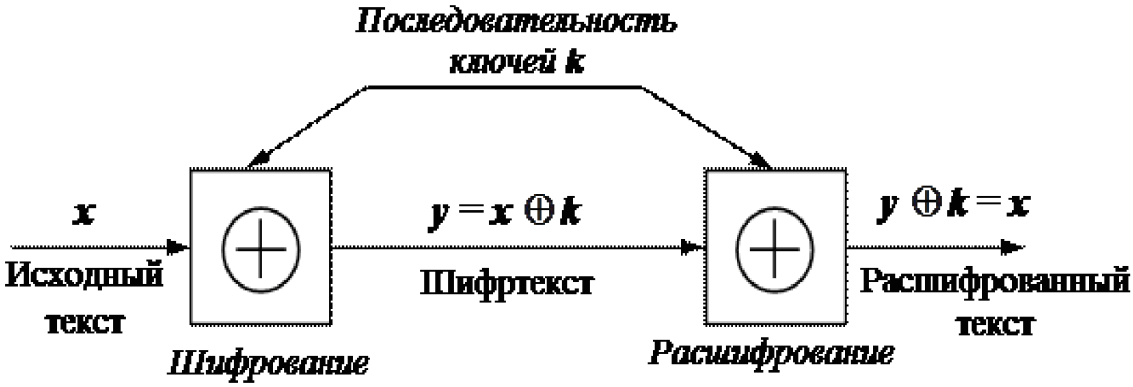

Рисунок 1 – Схема шифрования и расшифрования сообщений по методу Вернама

Решетка Кардано. Предложена в 1550 году Джероламо Кардано [4]. Решетка Кардано представляет собой скорее метод стеганографии, чем классического шифрования.

Этот метод основан на использовании трафарета с отверстиями, который накладывается на текст, а видимые через отверстия символы образуют секретное сообщение. Например, при наложении решетки на текст «ДОМА УЮТНО» могут быть выделены буквы Д, О, Н, образующие слово «ДОН».

Главное достоинство этого метода – простота использования и возможность комбинирования с другими методами шифрования. Однако он крайне уязвим, если злоумышленник узнает шаблон решётки и ее положение, и подходит только для коротких сообщений, так как сложность шифра – сочинить маскирующий текст так, чтобы он выглядел связно и естественно. Анализ выше представленных алгоритмов представлен в таблице 1

Таблица 1 – Анализ алгоритмов

Критерий	Виженер	Плейфер	Вернам	Кардано
Тип шифра	Полиалфавитный	Биграммный	Потоковый (XOR)	Трафаретный
Криптостойкость	Средняя	Средняя	Абсолютная	Низкая
Уязвимости	Частотный анализ	Известный текст	Повтор ключа	Угадывание решетки
Сложность взлома	$O(n^2)$	$O(n^2)$	Невозможен	$O(n)$
Применимость	Короткие сообщения	Тексты	Секретные данные	Ручное шифрование

Проведя сравнительный анализ этих четырёх методов, можно сделать следующие выводы. Шифр Виженера остаётся хорошим выбором для базовой защиты информации, особенно когда важна простота реализации. Шифр Плейфера обеспечивает более высокий уровень безопасности за счёт использования биграмм, но требует более сложной подготовки. Шифр Вернама является единственным из рассмотренных методов, обеспечивающим абсолютную криптографическую стойкость, но его практическое применение сильно ограничено из-за требований к ключу.

Решетка Кардано представляет в большей степени исторический интерес и может использоваться скорее для сокрытия факта передачи сообщения, чем для его криптографической защиты.

ЛИТЕРАТУРА

1. Шифр Виженера [Электронный ресурс] / Главная страница – Режим доступа: https://ru.ruwiki.ru/wiki/Шифр_Виженера – Дата доступа: 30.03.2025

2. Шифр Плейфера [Электронный ресурс] / Главная страница – Режим доступа: https://ru.ruwiki.ru/wiki/Шифр_Плейфера – Дата доступа: 30.03.2025

3. Шифр Вернама [Электронный ресурс] / Главная страница – Режим доступа: https://lektsii.org/13-85247.html – Дата доступа: 30.03.2025

4. Решетка Кардано [Электронный ресурс] / Главная страница – Режим доступа: https://fb.ru/article/544483/2023-reshetka-kardano-opisanie-osobennosti-vidyi – Дата доступа: 30.03.2025