АПОУ ВО «Вологодский колледж связи и информационных технологий»

АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ

Фастовец Даниил Леонидович,
Студент
Трошкин Павел Евгеньевич,
Руководитель

Вологда, 2019 год

АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ

Цель работы – проанализировать алгоритмы шифрования данных.

Для достижения поставленной цели были определены следующие задачи -

1) Изучить назначение и структуру алгоритмов шифрования;

2) Рассмотреть алгоритм симметричного шифрования;

3) Разобрать структуру алгоритмов шифрования;

4) Рассмотреть типы атак на алгоритмы шифрования;

АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ

Объект работы – Атаки на алгоритмы шифрования данных.

Предмет работы – Криптография,шифрование,атаки на алгоритмы шифрования.

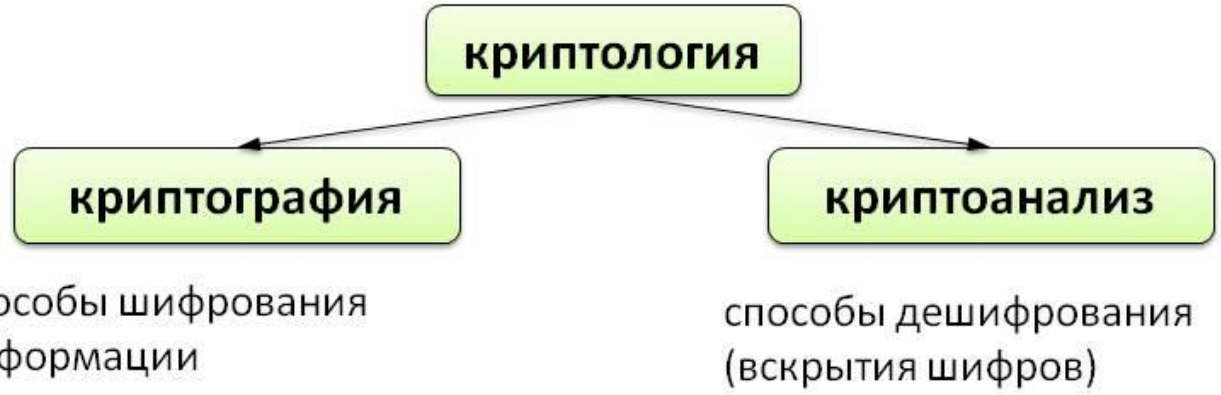
АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ

Шифрование

Один из методов защиты информации от неправомерного доступа – это *шифрование*, то есть кодирование специального вида.

Шифрование – это преобразование (кодирование) открытой информации в зашифрованную, недоступную для понимания посторонних.

Методы шифрования и расшифровывания сообщения изучает наука **криптология**



АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ

АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ

АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ

АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ

АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ

Атака при наличии известного шифртекста.

АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ

Активное воздействие на шифратор.

АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ

Атака с выбором открытого текста.

АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ

1. Изучение области использования
2. Выбор длины секретного ключа.
3. Выбор расписания использования ключа
4. Выбор базовых криптографических примитивов и разработка криптосхемы
5. Оценивание потребляемых ресурсов для реализации алгоритма шифрования
6. Оценивание производительности шифра
7. Рассмотрение стойкости к возможным типам криптоаналитических атак
8. Модифицирование алгоритма с учетом предварительного анализа
9. Выполнение детального анализа модифицированного шифра
10. Выполнение статистических тестов и специальных экспериментов.

АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ

ЗАКЛЮЧЕНИЕ

В ходе проведенного анализа я выяснил, что шифрование информации зависит не только от стойкости и силы использованного алгоритма, но и от того, насколько качественно разработан шифратор, который, собственно, и выполняет шифрование. Касательно самих атак метод грубой силы гораздо более ресурса затратная по сравнению с атаками, использующими крипто аналитические методы. Примерами могут служить линейный криптоанализ и дифференциальный криптоанализ

СПАСИБО ЗА ВНИМАНИЕ!