

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**



способы шифрования
информации

способы дешифрования
(вскрытия шифров)

АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ



АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ



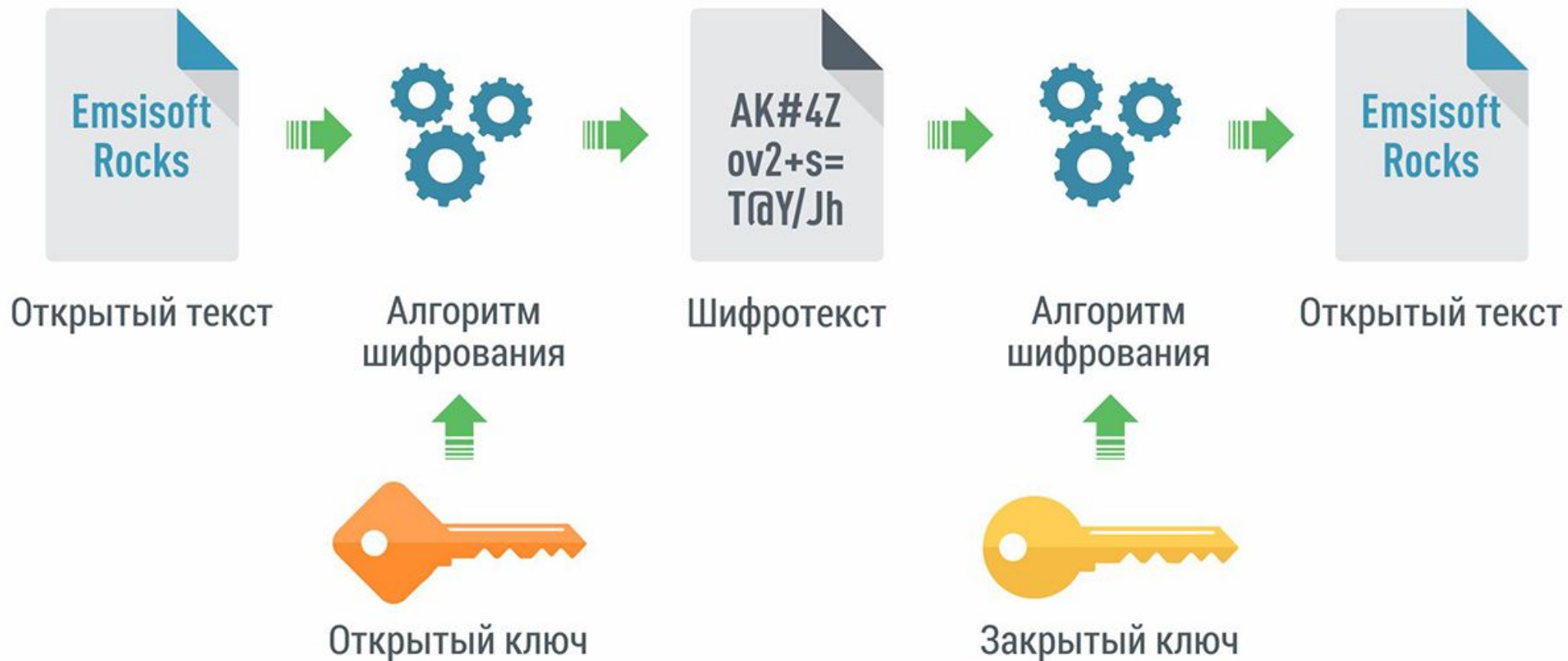
АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ

Симметричное шифрование



АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ

Асимметричное шифрование



АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ



Атака при наличии известного шифртекста.



АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ



Активное воздействие на шифратор.

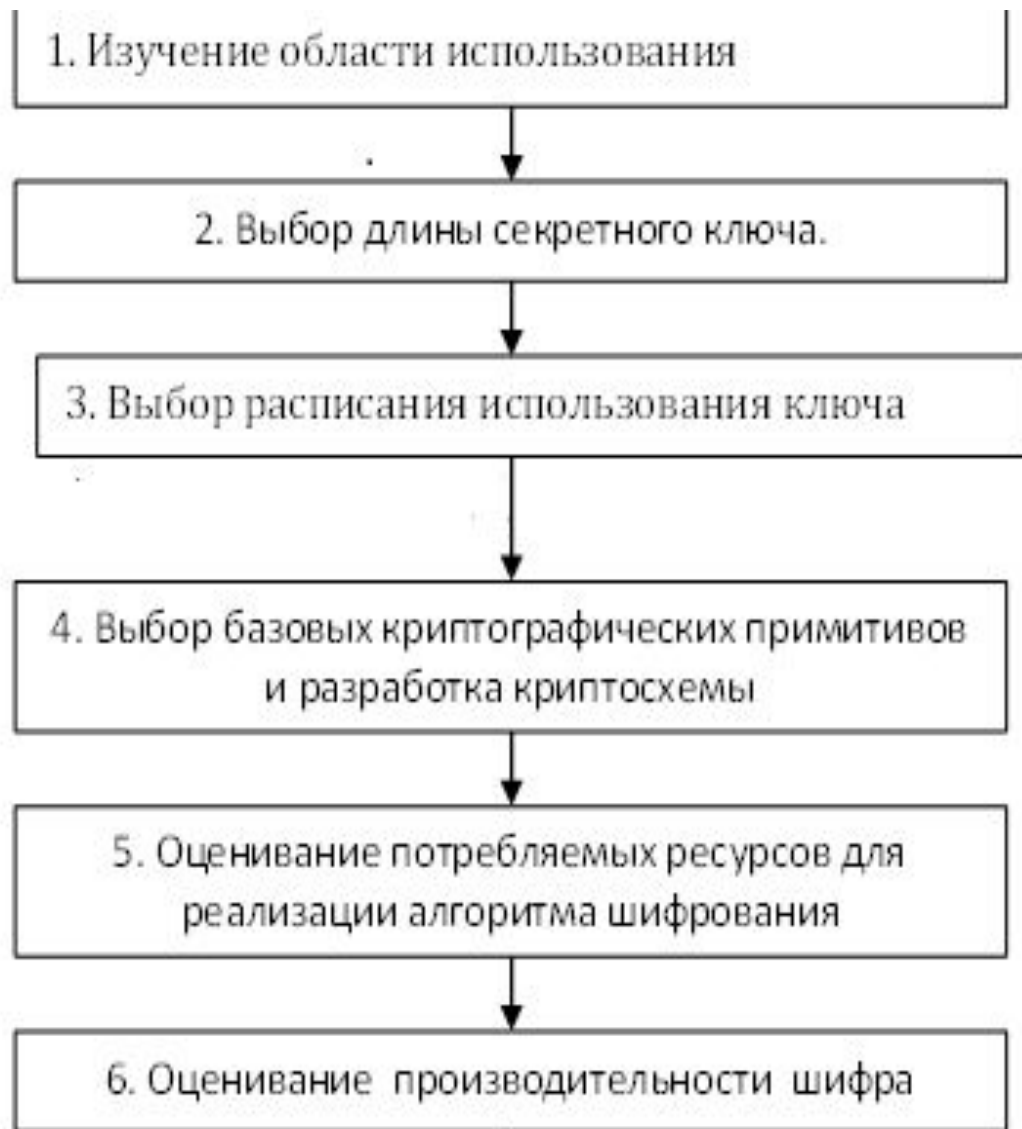


АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ

Атака с выбором открытого текста.



АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ



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 криптоаналитические методы. Примерами могут служить линейный криптоанализ и дифференциальный криптоанализ

АТАКИ НА АЛГОРИТМЫ ШИФРОВАНИЯ



СПАСИБО ЗА ВНИМАНИЕ!