Базовая технология безопасности - Шифрование

Выполнил ученик 10 А класса
МОУ «СОШ №12 ЗАТО Шиханы»
Веселов Алексей

Проблемный вопрос

Для чего служит шифрование? Что оно из себя представляет? Важно ли знать его функции и значение?

Актуальность

В наше время шифрование имеет огромное значение. Его применение находят очень важным многие люди. Поэтому следует иметь представление о таком явлении, как шифрование.

Цель:

создать презентацию по теме «Базовая технология безопасности – Шифрование»

Задачи:

- собрать информацию по теме
- выступить на конференции

Содержание

Что такое безопасность? Безопасность информации?

- **Безопасность** — отсутствие какого-либо риска, в случае реализации которого возникают негативные последствия (вред) в отношении кого-либо или чего-либо.
- **Безопасность информации** (данных) — состояние защищённости информации (данных), при котором обеспечиваются её (их) конфиденциальность, доступность и целостность.

Защита данных

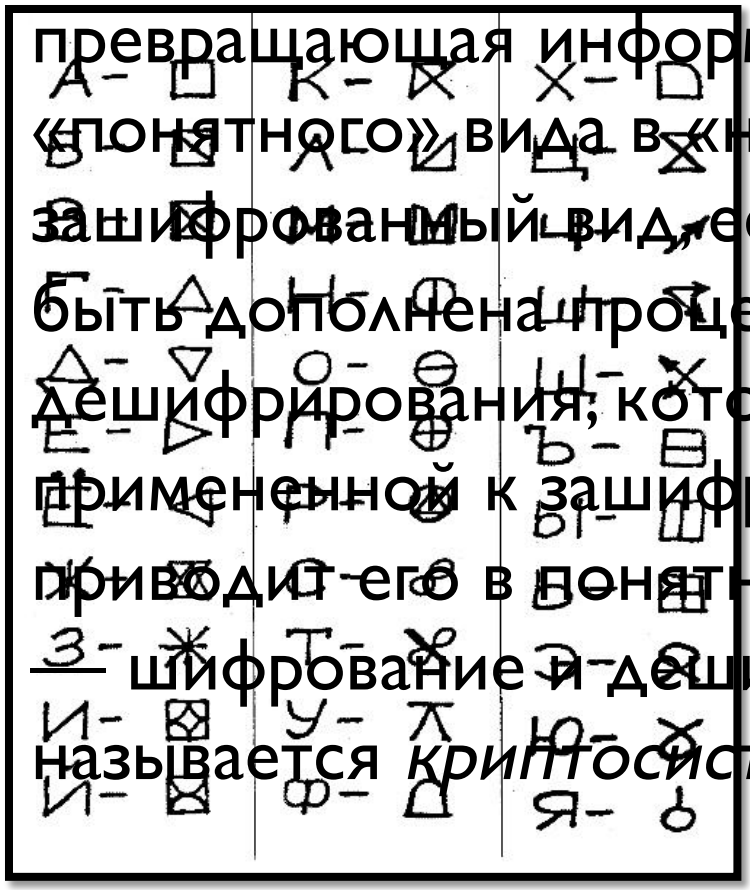
В разных программных и аппаратных продуктах, предназначенных для защиты данных, часто используются одинаковые подходы, приемы и технические решения. К таким базовым технологиям безопасности относятся шифрование, аутентификация, авторизация, аудит и технология защищенного канала.

Шифрование

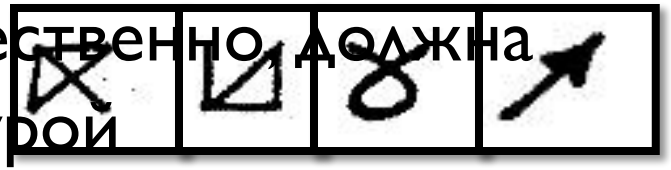
Шифрование — обратимое преобразование информации в целях скрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации.

Криптосистема

Любая процедура шифрования, превращающая информацию из обычного «понятного» вида в «нечитабельный» зашифрованный вид, естественно должна быть дополнена процедурой дешифрирования, которая, будучи применённой к зашифрованному тексту, снова приводит его в понятный вид. Пара процедур шифрование и дешифрирование называется *криптосистемой.*



Шифрование информации

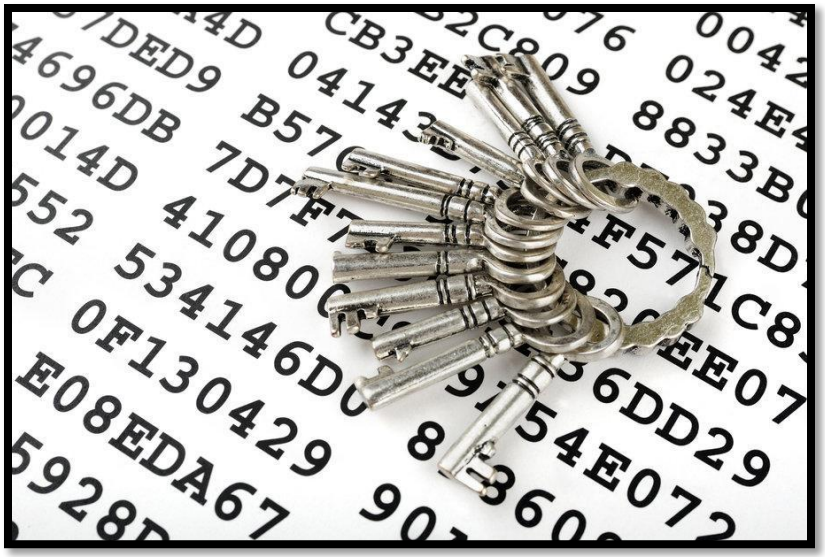


Дешифрование информации

КЛЮЧ

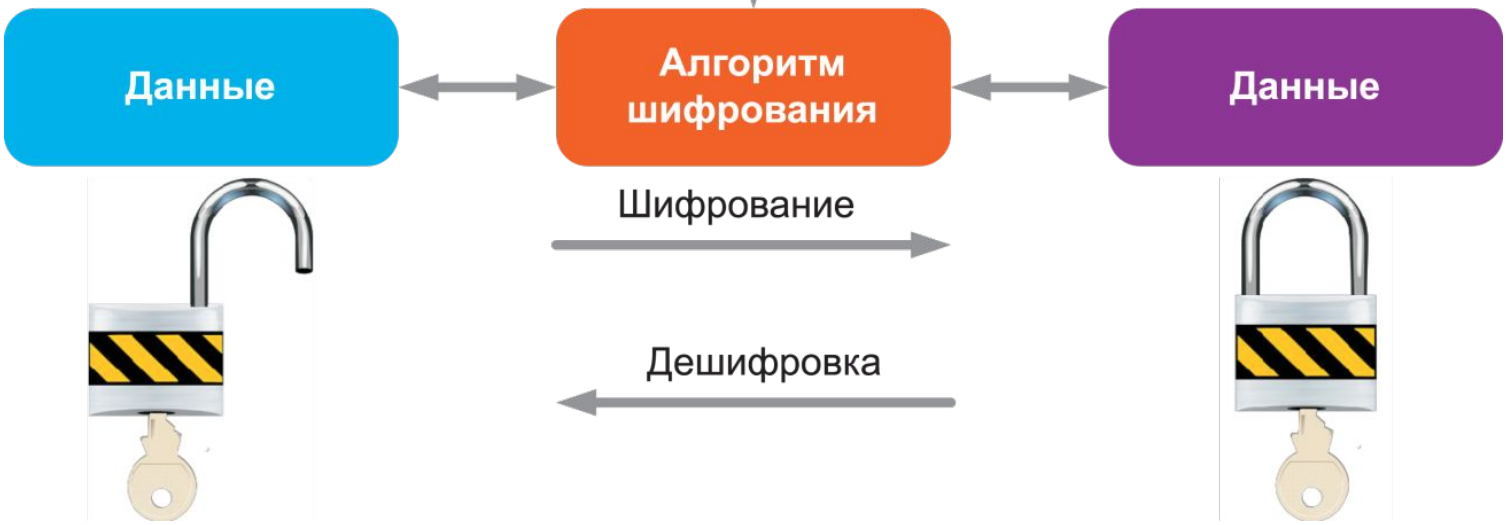
Секретный ключ

В современных алгоритмах шифрования предусматривается наличие параметра — *секретного ключа*, секретность которого определяет стойкость шифра.



Раскрытие алгоритма шифрования

Алгоритм шифро
считается *раскрытым*, если найдена
процедура, позв подобрать
ключ за реальное время.

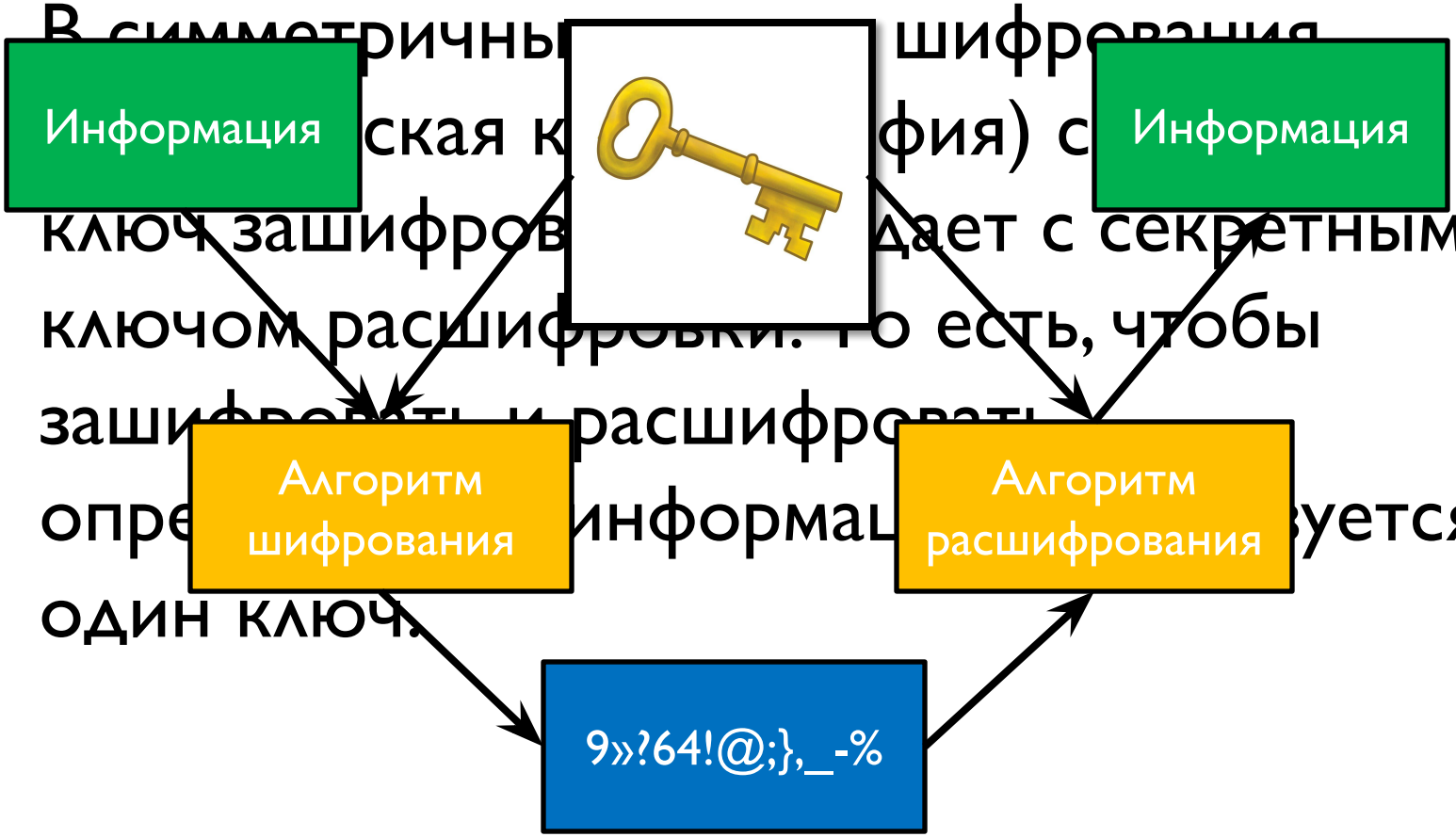


Подразделение криптосистем:

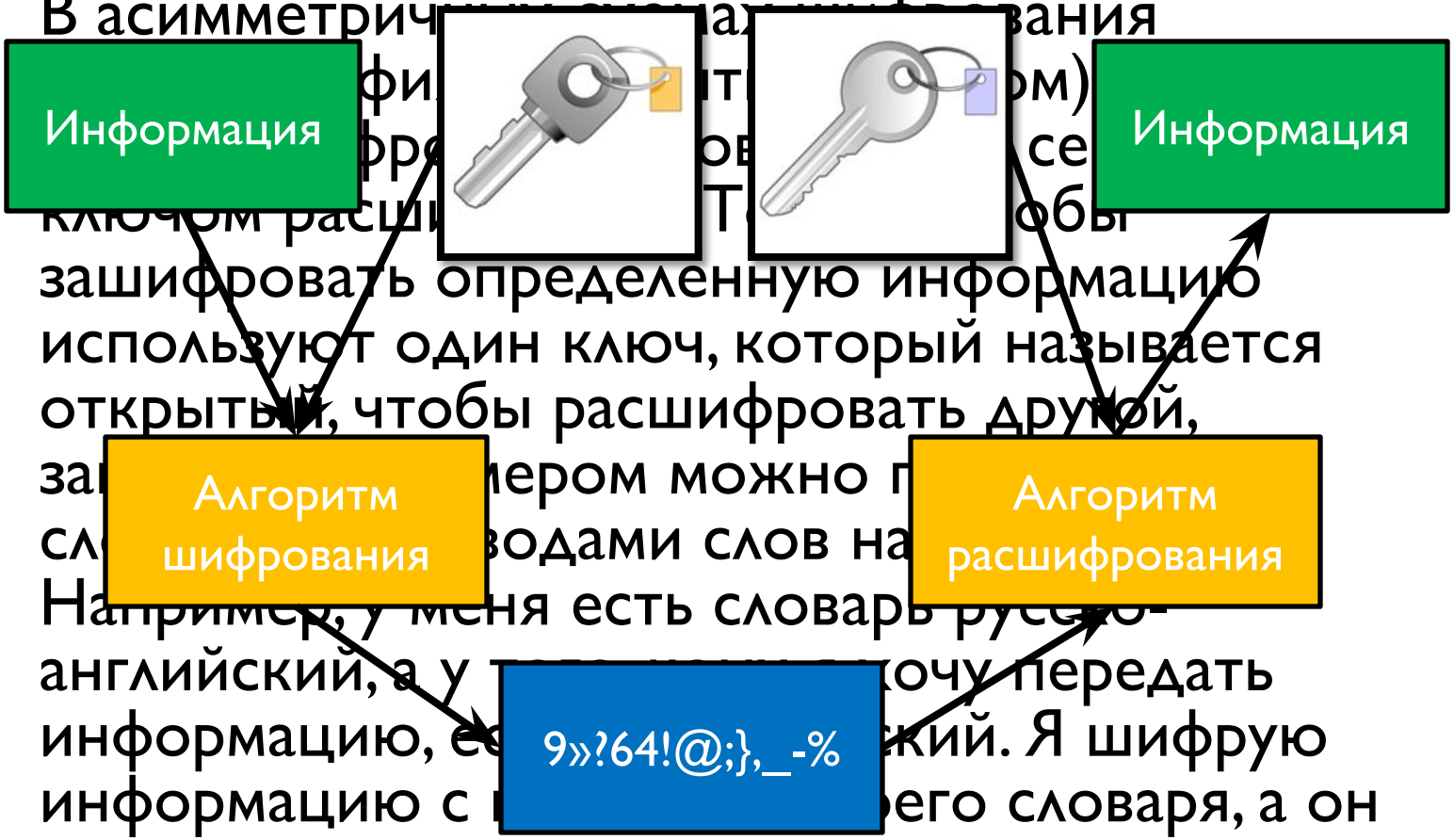
- симметричная: один ключ
- ассиметричная: два ключа

Симметричные

В симметричны шифрования
ская к фия) с
ключ зашифров дает с секретным
ключом расшифровки. То есть, чтобы
зашифровать и расшифровать
опре информац уется
один ключ.



Асимметричные



В асимметрич ания
фи ом)
ффр се
ключом расш обы
зашифровать определенную информацию
используют один ключ, который называется
открытый, чтобы расшифровать другой,
за мером можно
сл водами слов на
Например, у меня есть словарь русско-
английский, а у очу передать
информацию, е кий. Я шифрую
информацию с его словаря, а он
расшифровывает с помощью своего.

Самое главное при шифровании:

- хранить ключи шифрования и расшифрования (открытый не обязательно) в секрете
- пользоваться проверенными временем алгоритмы (например, DES, PGP). Эти алгоритмы, хоть и известны, но от этого их эффективность не снижается
- не злоупотреблять шифрованием
- соблюдать правовые нормы

Источники

- https://ru.wikipedia.org/wiki/Шифрование
- http://bourabai.kz/os/lecture22.htm
- https://ru.wikipedia.org/wiki/Ключ_(криптография)
- https://studfiles.net/preview/4001838/page:5/
- https://yandex.ru/images/

Спасибо за внимание!