

# **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

1. Что такое безопасность? Безопасность информации?
2. Защита данных
3. Шифрование
4. Криптосистема
5. Секретный ключ
6. Раскрытие алгоритма шифрования
7. Подразделение криптосистем:
8. Симметричные
9. Асимметричные
10. Самое главное при шифровании

# 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 «понятного» вида в «нечитабельный» вид, естественно, должна

быть дополнена процедурой дешифрования, которая, будучи примененной к зашифрованному тексту, снова приводит его в понятный вид. Пара процедур шифрования и дешифрования называется криптосистемой.

|       |       |       |
|-------|-------|-------|
| А - □ | К - ✕ | Х - □ |
| В - ▽ | Л - ▽ | Ц - ✕ |
| Г - △ | М - ⊙ | Ч - ✕ |
| Д - ▽ | Н - ⊙ | Ш - ✕ |
| Е - ▽ | О - ⊙ | Щ - ✕ |
| Ж - ▽ | П - ⊙ | Ъ - ▽ |
| З - * | Т - ✕ | Ы - ▽ |
| И - ▽ | У - ▽ | Ю - ✕ |
| Й - ▽ | Ф - ▽ | Я - ○ |

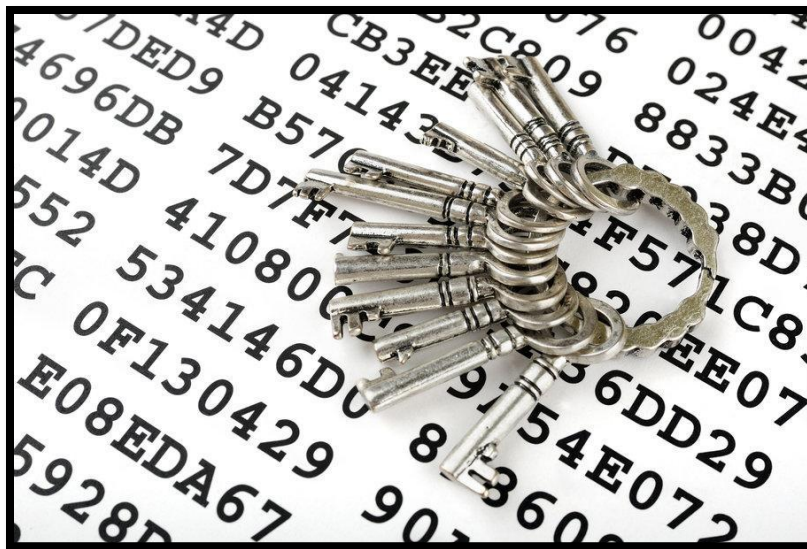


**КЛЮЧ**



# Секретный ключ

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

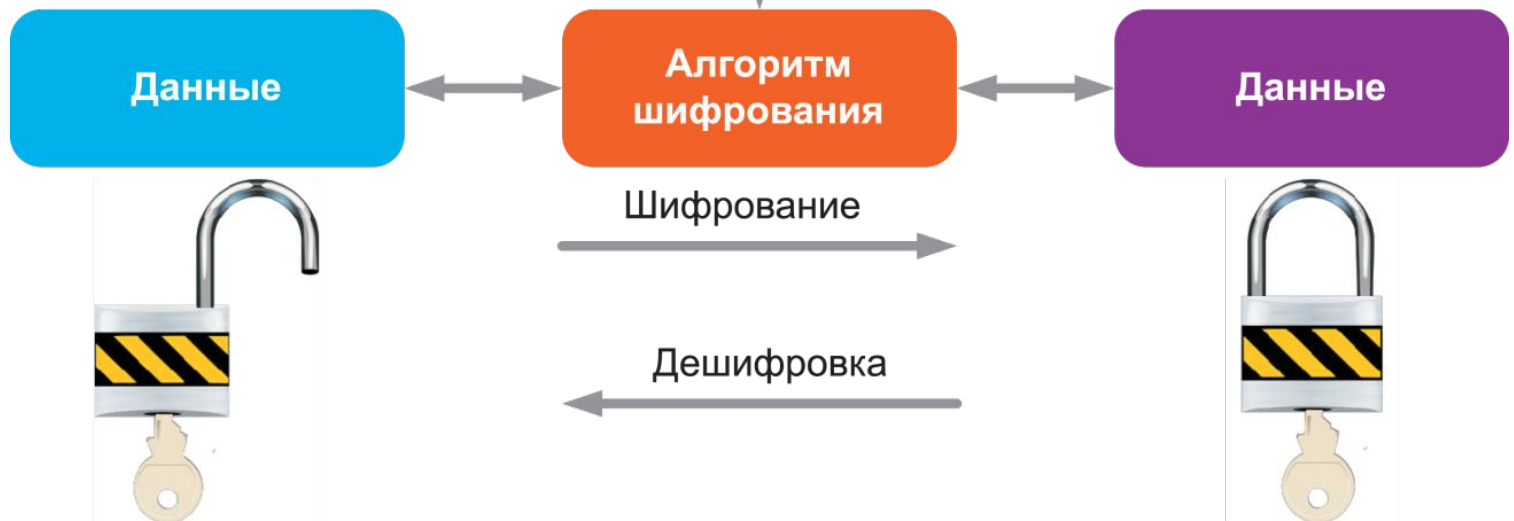


# Раскрытие алгоритма шифрования

Алгоритм шифрования считается *раскрытым*, если найдена процедура, позволяющая подобрать ключ за реальное время.

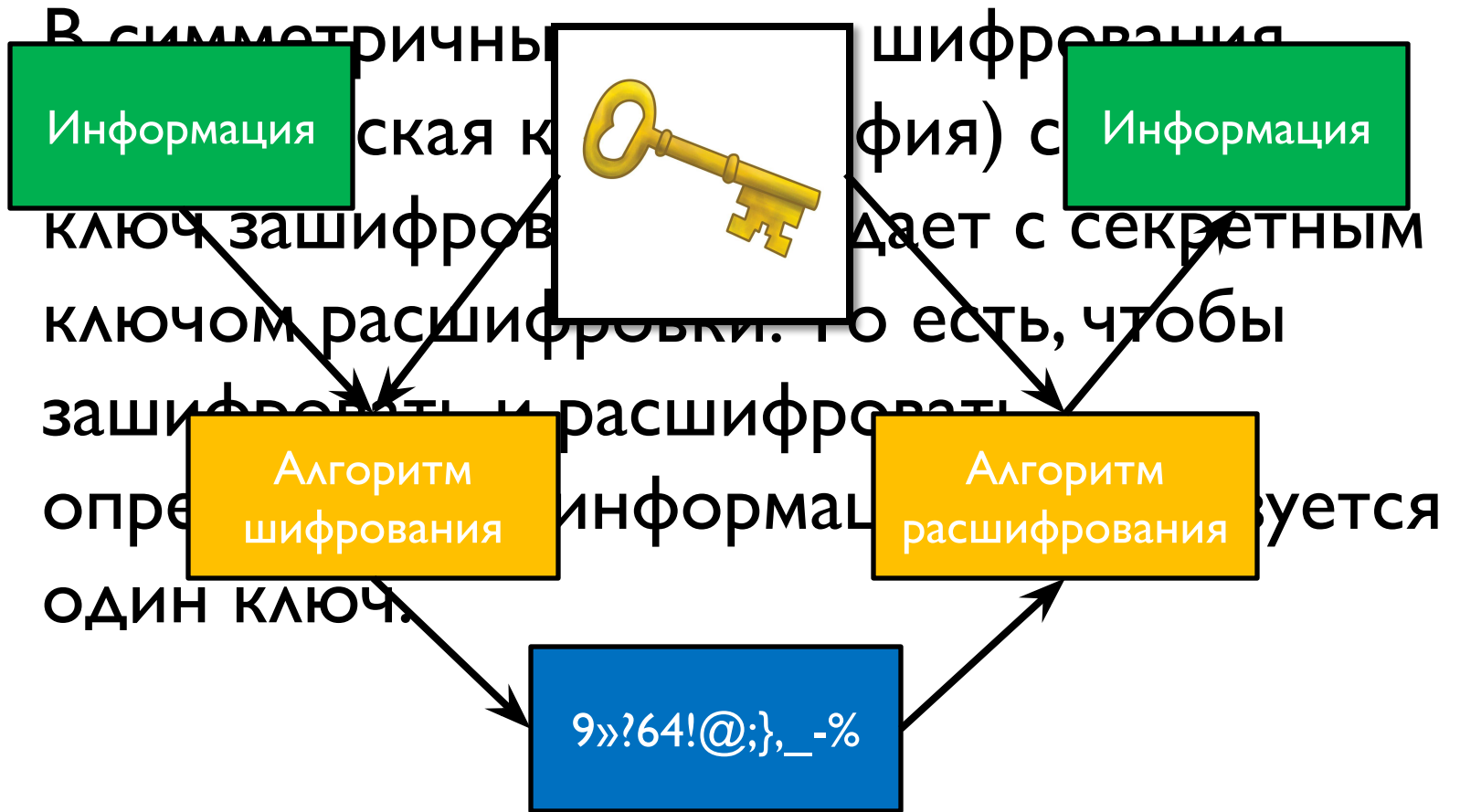


Ключ шифрования

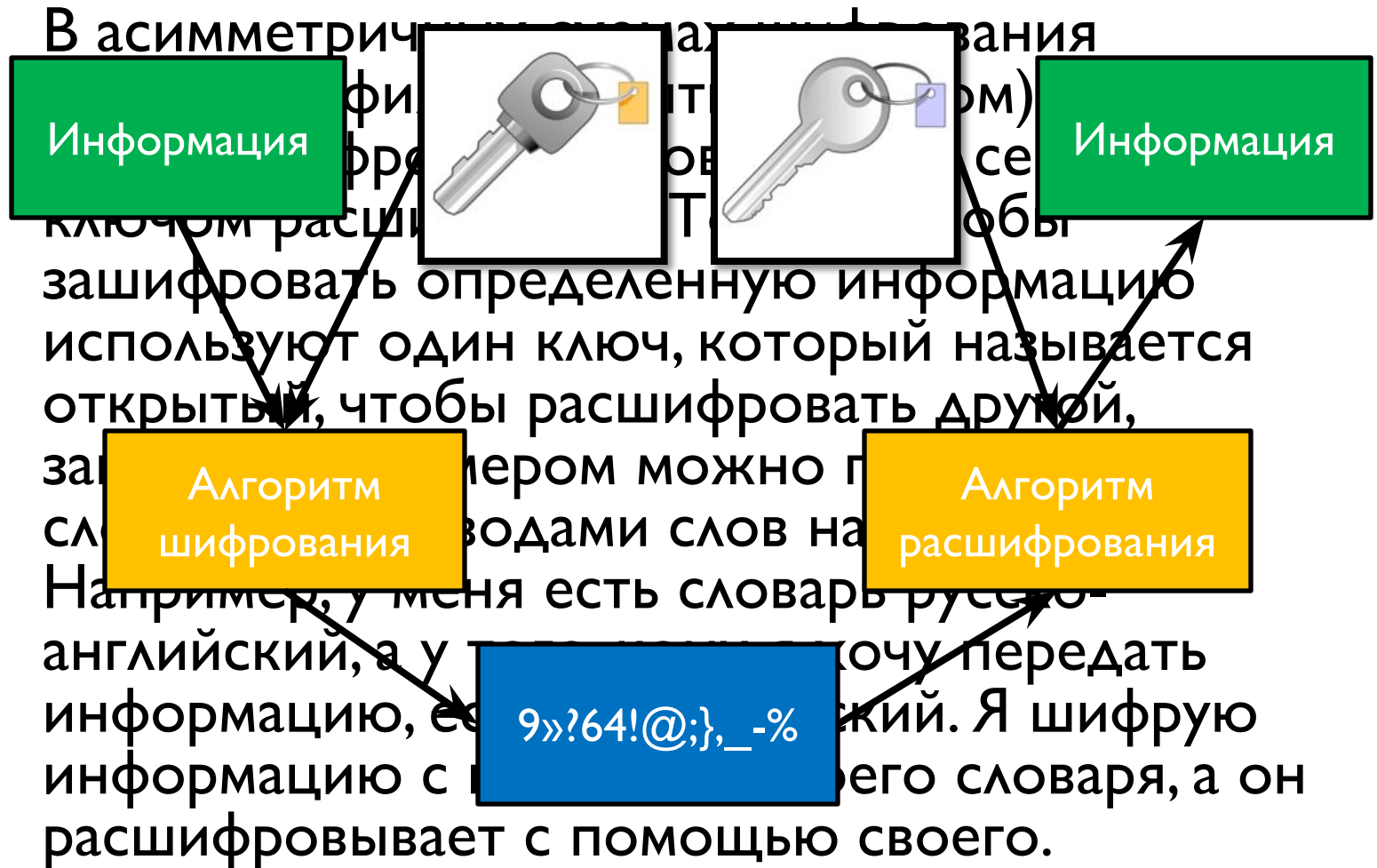




# Симметричные



# Асимметричные



# 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://ru.wikipedia.org/wiki/Ключ_(криптография))
- <https://studfiles.net/preview/4001838/page:5/>
- <https://yandex.ru/images/>



**Спасибо за  
внимание!**