Федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский политехнический университет Петра Великого»

Основы криптографической защиты информации

Преподаватель: Горелов С. В.

Работу выполнили: Берещук Д.О

Константинова М.П

Кириллов Н.К

Биоинженерия и биоинформатика 4750601/50001

Санкт-Петербург 2025

Введение

- Криптография — основа современной информационной безопасности.
- Задачи криптографии:
  1. Конфеденциальность
  2. Целостность
  3. Аутентификация
  4. Неотказуемость

История

- **50 г. до н.э Шифр Цезаря** — классический пример шифра подстановки. Каждая буква меняется ту, которая стоит в алфавите на фиксированное число позиций дальше

  ПРИВЕТ - ТУЛЕИХ

- **XX век Энигма** — электромеханическая роторная машина, использовавшаяся нацистской Германией. Ее взлом командой Алана Тьюринга стал триумфом криптоанализа и доказал важность секретности **ключа**

Базовые понятия
На примере шифра Цезаря

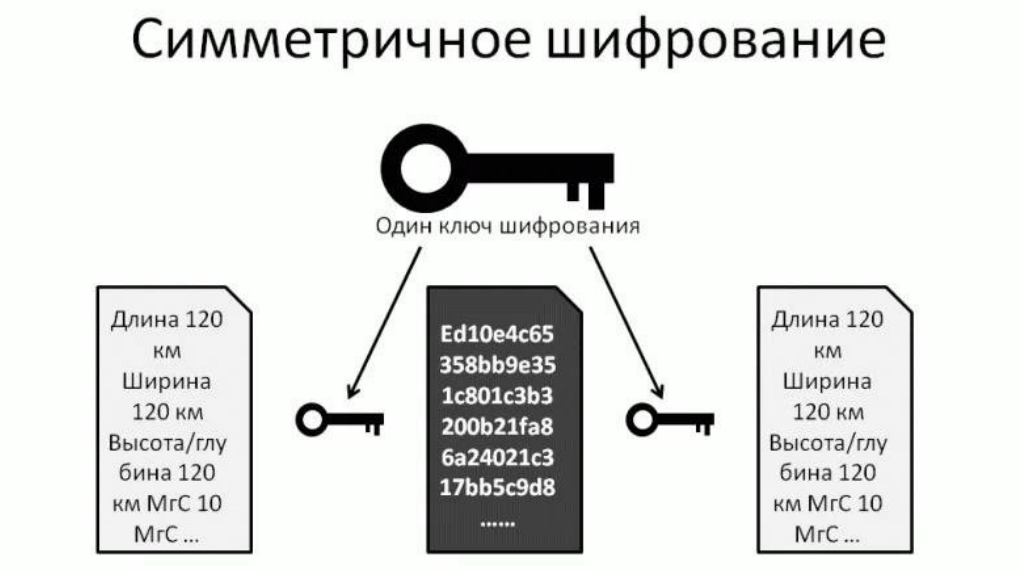
- **Исходный текст -** ПРИВЕТ
- **Шифротекст -** ТУЛЕИХ
- **Алгоритм шифрования -** Сдвиг каждой буквы на К позиций вперед
- **Ключ** — Число К=3. Секретная информация, известная только отправителю и получателю
- **Расшифрование** — обратный процесс с использованием ключа

Таблица для сдвига, равного 3.

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В

Симметричное шифрование

- Шифрование и расшифрование проводятся с помощью одного ключа
- Плюсы — высокая скорость
- Минусы — проблема безопасной передачи ключа второй стороне



Асимметричное шифрование

- Используется пара ключей: **открытый и закрытый**.
- **Открытый** доступен всем, им можно только зашифровать данные.
- **Закрытый** хранится в секрете, им можно только расшифровать данные

Совместное использование методов шифрования на примере мессенджера Телеграм (гибридное шифрование)

- **Шаг 1. Установка безопасного канала (начало чата)**

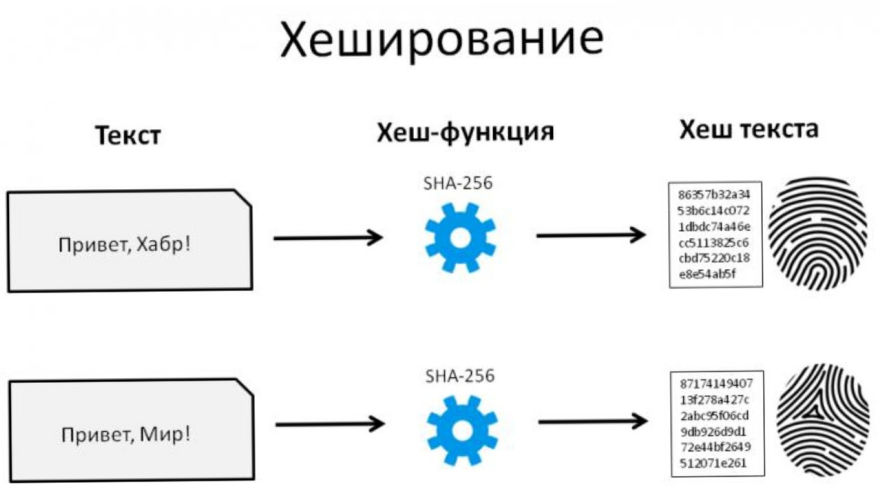
  Передача симметричного ключа с помощью асимметричного шифрования

- **Шаг 2. Обмен сообщениями**

  -Все сообщения шифруются симметричным ключом

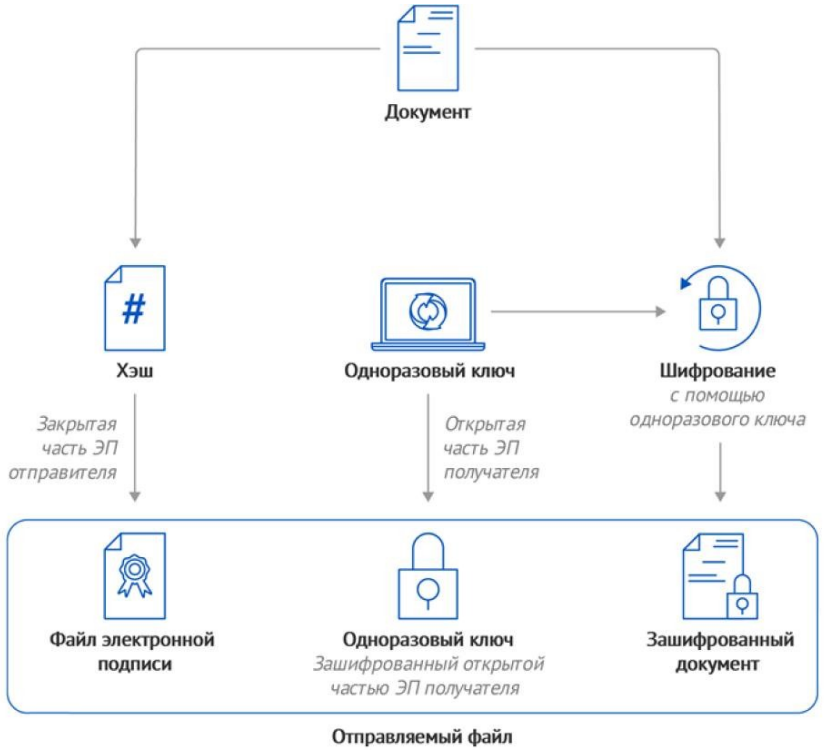
Хеширование

- **Хеширование** — преобразование данный в фиксированный дайджест без возможности обратного восстановления
- **Св-ва хеш-функции**: детерминированность (один вход, один выход), необратимость (нельзя восстановить исходные данные), устойчивость к коллизиям (разные входы, разные выходы)
- **Применение**: проверка целостности файлов,хранение паролей, блокчейн



Цифровая подпись

- **Задача**: подтвердить авторство и целостность сообщения
- **Как работает**:
  1. Отправитель хеширует сообщение
  2. Шифрует хеш своим закрытым ключом
  3. Отправляет
  4. Получатель проверяет



Цифровые сертификаты

- Цифровой сертификат — электронный документ, связывающий открытый ключ с субъектом (человек, сервер)
- Содержит: открытый ключ, имя владельца, срок действия, подпись удостоверяющего центра (CA)
- Процесс проверки: клиент получает сертификат сервера, проверяет подпись CA, использует открытый ключ сервера для шифрования

Вывод

- Криптография эволюционировала от простых шифров до сложных математических систем
- Симметричное и асимметричное копирование дополняют друг друга
- Хеширование, подписи, и сертификаты решают задачи целостности и аутентификации