Шейкин В.В., НИУ ВШЭ

Использование криптосредств при подготовке специалистов по ИБ

Что такое криптография?

Криптография – метод шифрования **данных**, прочитать которые сможет **только адресат**, у которого есть **ключ** к шифру.

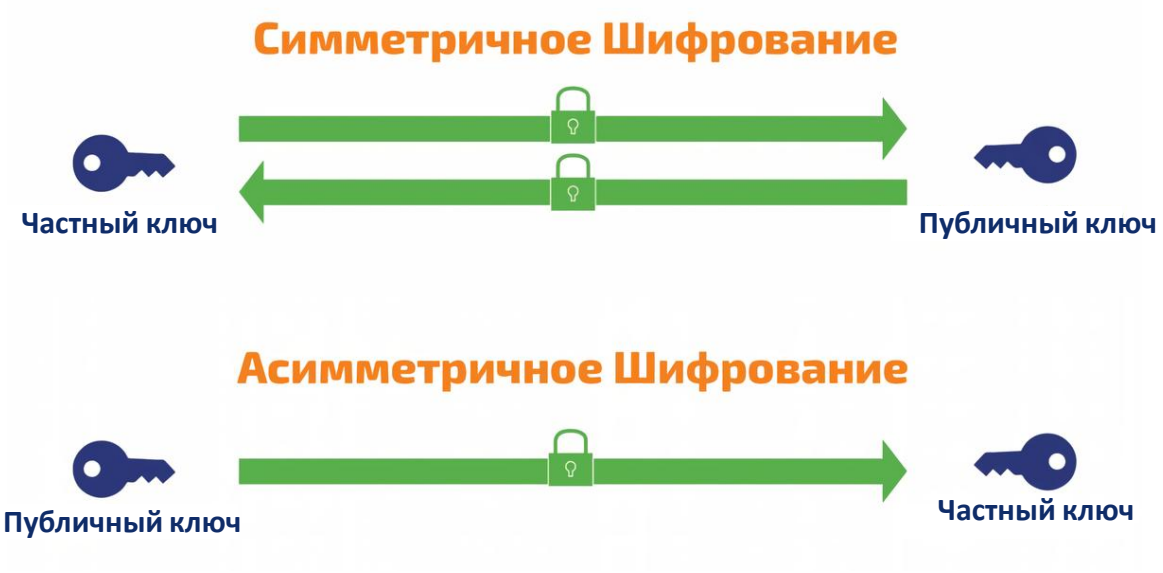
Криптографические алгоритмы используются при разработке *различных* протоколов шифрования данных, включая 128- и 256-битное шифрование, протокол **SSL** и протокол **TLS.**

Эффективное шифрование: от симметричного ключа к системе с открытым ключом в криптографии

Самый простой – **шифрование с симметричным ключом**.

Система с открытым ключом: в этом случае у каждого пользователя есть два ключа: открытый и закрытый.

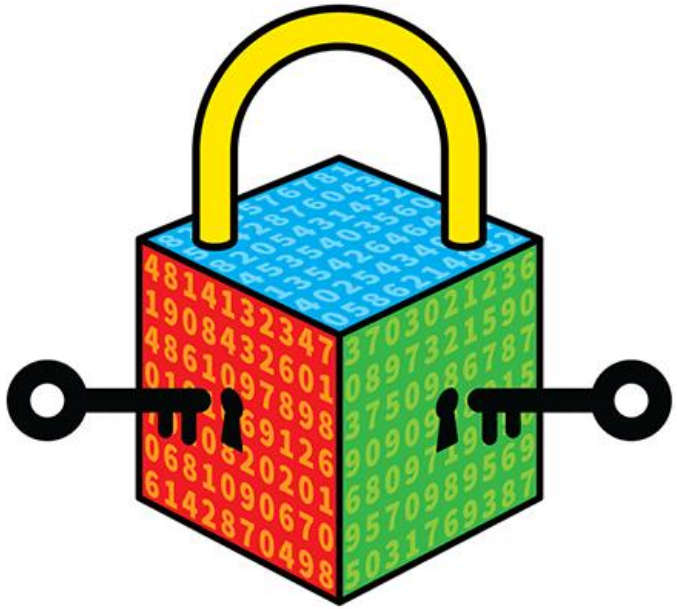
Перехват данных лишается всякого смысла – **без ключа посторонний не сможет их расшифровать.**



Какую роль играет криптография в современной жизни?

Криптография служит разным целям:

- Сохранение **конфиденциальности**.
- Сохранение **целостности данных**.
- **Аутентификация**
- **Подтверждение обязательств**.



Как криптография применяется в кибербезопасности?

Несколько примеров применения **криптографии** в повседневной жизни:

- Защита передаваемой по сети информации с помощью **сквозного шифрования**
- **Защита от кибератак**
- Создание и **проверка учетных данных**, в частности **паролей**
- **Защита** операций с **криптовалютами**
- **Защита** электронных документов **цифровой подписью**
- **Идентификация** пользователя *при входе в учетные записи*

Потребность в криптографии

Зная, что такое **криптография,** пользователь **сможет**:

- **ответственно** подойти к использованию цифровых сервисов *в повседневной жизни*
- **повысить уровень безопасности**

Криптография используется **для защиты** многих операций в интернете.

Роль криптографии в образовании

Защита учебных данных - одна из основных задач **криптографии** в образовании: **личная информация** *студентов и преподавателей*.

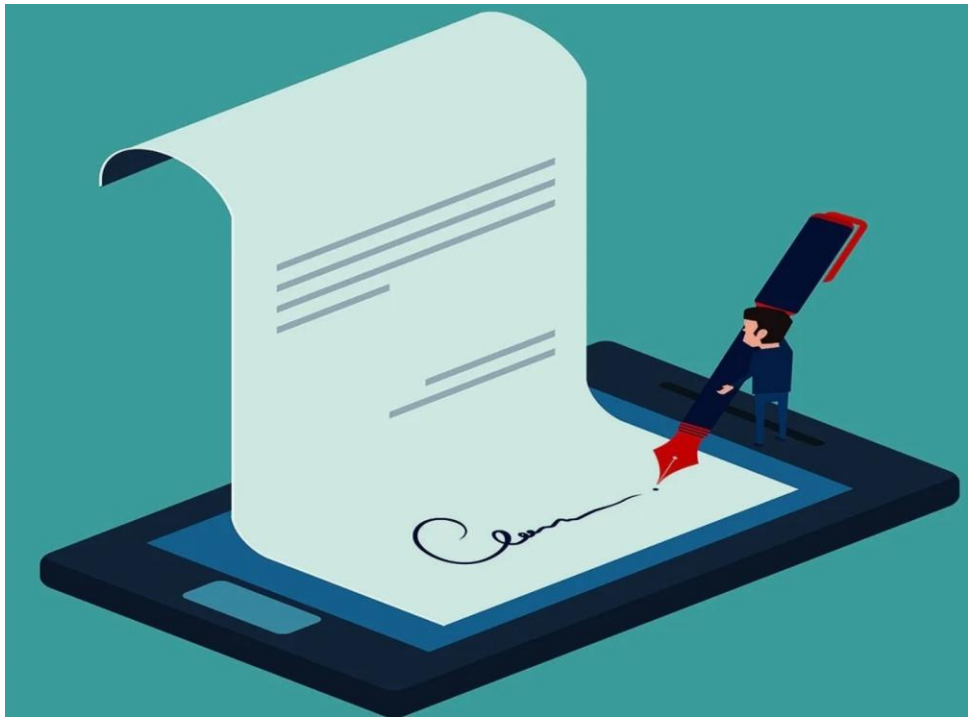
Криптография позволяет **зашифровать** эти данные, **чтобы предотвратить** несанкционированный доступ к ним.

Криптография играет важную роль в **защите** *интеллектуальной собственности в образовании*.

Методы криптографии в образовании

Основные методы **криптографии**:

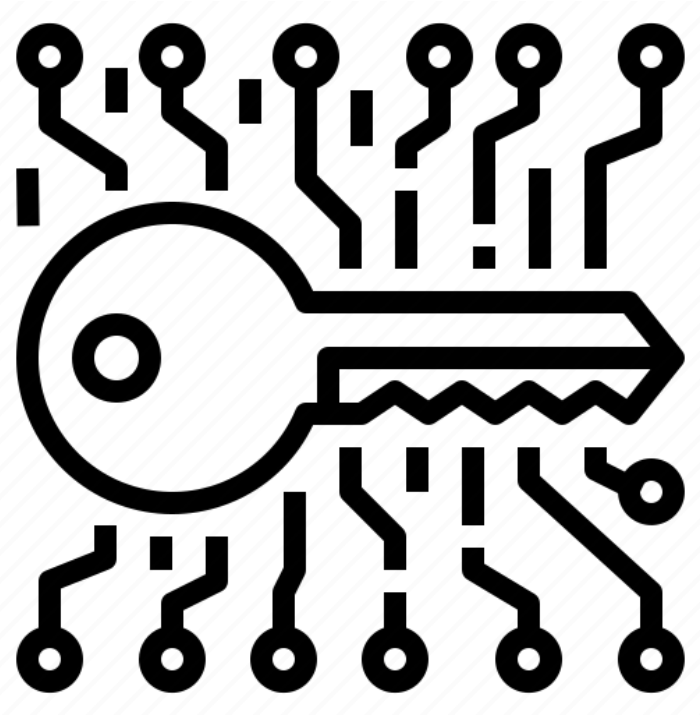
- *Симметричное* **шифрование**
- *асимметричное* **шифрование**
- **хэширование**
- **цифровые подписи**



Польза от криптографии в образовании

Использование **криптографии** в образовании имеет ряд **преимуществ**:

- **обеспечивает безопасность** данных и защиту *личной* информации студентов и преподавателей
- способствует сохранению конфиденциальности и целостности учебных материалов и исследований
- криптография помогает предотвратить *плагиат* и **несанкционированное использование** учебных материалов.



Примеры применения криптографии в образовании: защита учебных материалов

Польза:

- **Предотвращение** утечки *конфиденциальной* информации
- **Защита авторских прав**
- Улучшение **безопасности** данных

Проблемы:

- Необходимость ввода пароля для доступа к материалам
- Возможность потери пароля

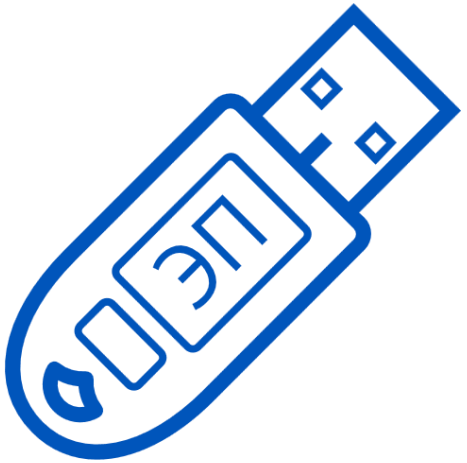
Примеры применения криптографии в образовании: электронная подпись

Польза:

- Гарантия **подлинности** документов
- **Улучшение** *доверия* к электронным документам
- **Упрощение** процесса подписания и *проверки* документов

Проблемы:

- Необходимость в использовании *специального* программного обеспечения
- Возможность **подделки электронной подписи**



Примеры применения криптографии в образовании: защита онлайн-тестов

Польза:

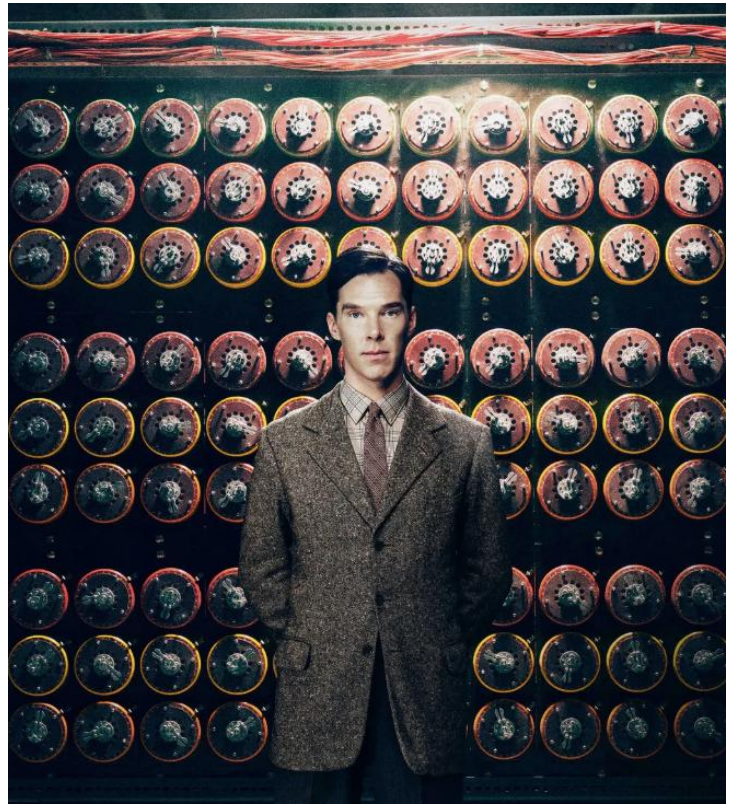
- Предотвращение **мошенничества** и **плагиата**
- **Улучшение** *достоверности* результатов тестирования
- **Защита конфиденциальности** ответов студентов

Проблемы:

- Возможность утечки тестовых вопросов и ответов
- Требуется **надежная** система управления доступом

Примеры применения криптографии в образовании: задачи и игры

- Обучение студентов основам **криптографии** и развития логического мышления
- Проведение **криптографических игр, задач** для **практического** применения знаний, исследовательских проектов в области криптографии для углубления знаний, развития навыков **анализа** и **проектирования**



Интернет вещей (IoT)

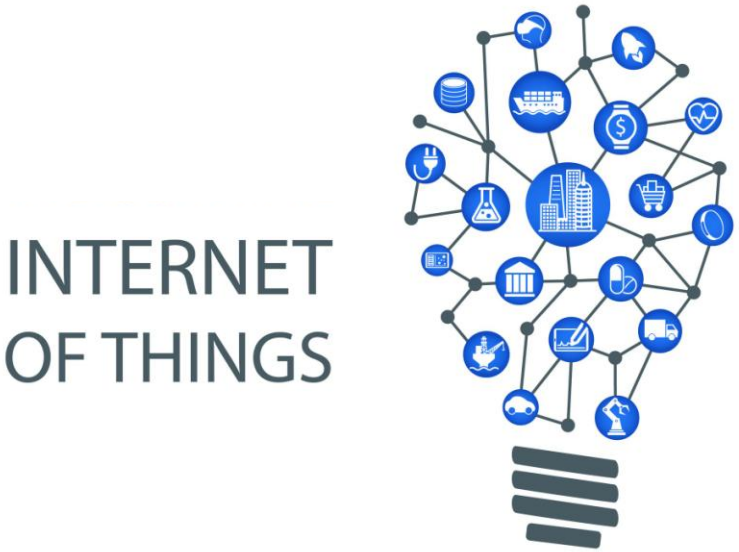
Интернет вещей (*IoT – Internet of Things*) – процесс обмена данными между различными устройствами на основе использования сетевых технологий.

Наглядным примером является технология *«умный дом».*

Сегодня интернет вещей применяется практически во всех отраслях и сферах, в том числе и **в образовании**.

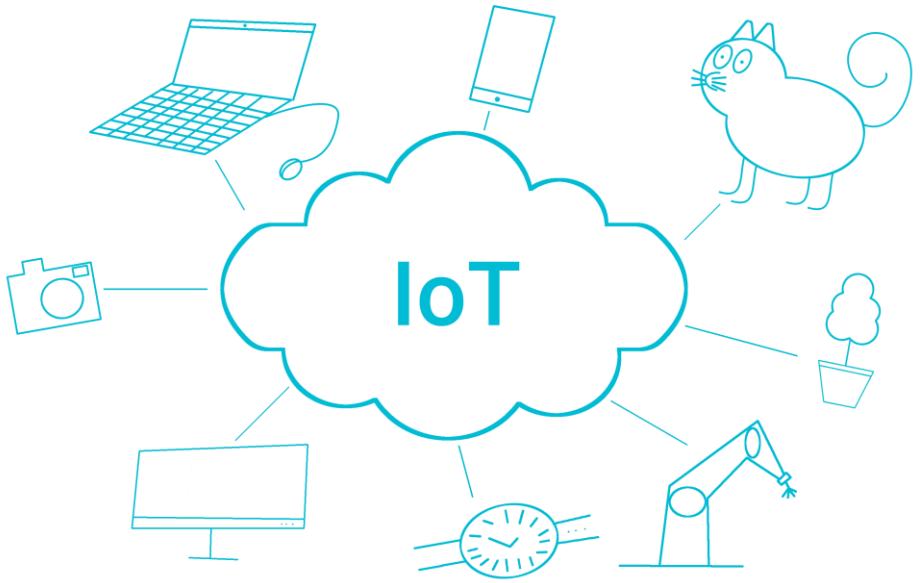
Каким образом такие технологии влияют на учебный процесс?

- Внедрение **современных технологий** в образовательные программы **положительно** влияет на обучение.
- Учащиеся хорошо относятся к использованию новых систем, таких как **интернет вещей**, что позволяет создать интерактивное обучение и адаптировать процесс под **каждого студента**.
- Такие системы обеспечивают постоянную связь **педагогов с учениками**.



Каким образом такие технологии влияют на учебный процесс?

- Использование **интернета вещей** в образовании повышает **качество** обучения, включая **безопасность**, учет знаний и посещаемость через RFID-метки и мобильные устройства.
- **Улучшает** проведение занятий и позволяют педагогам **эффективно отслеживать активность учащихся**.



Каковы перспективы этих технологий в сфере образования?

- **Новые перспективы** для **создания** *индивидуального* **образовательного процесса**
- Значительные **финансовые** затраты

Низкоресурсная криптография

1. **Безопасность** устройств IoT.
2. Защита данных и конфиденциальность.
3. Повышение производительность и безопасности обучения.
4. **Безопасное** пространство для **обучения**.

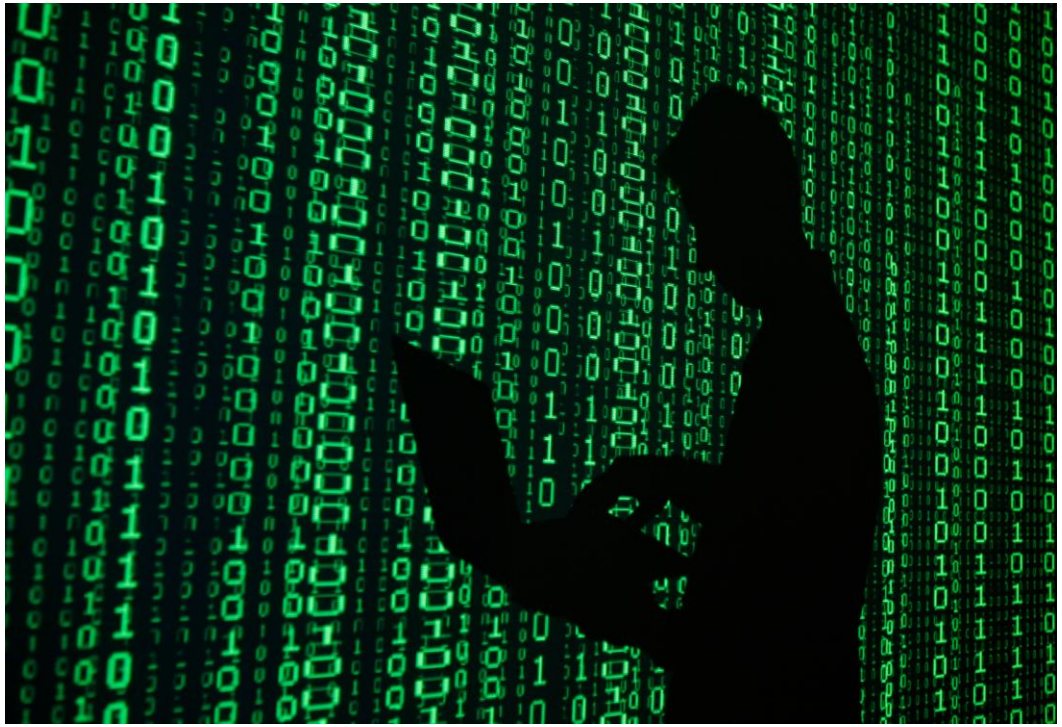
Ограничения и вызовы

- **сложность** реализации
- **обучение** персонала и студентов
- возможность возникновения **ошибок** при использовании

Криптография играет **важную роль** в образовании:

- обеспечивая **безопасность** и **конфиденциальность данных**
- **защиту интеллектуальной собственности**
- **предотвращение несанкционированного доступа**

Криптография - **важная часть** современного информационного общества, **инструмент для обеспечения безопасности** в образовании.



Список литературы

1. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО,2003. 328 с.
2. Нестеренко А.Ю. Теоретико-числовые алгоритмы в криптографии. М.: МГИЭиМ,2012. 224 с
3. Ниссенбаум О. В., Поляков Н.В. Криптографические протоколы: лабораторный практикум: учебно-методическое пособие для студентов специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем». Тюмень: ТюмГУ. 2012. 40 с.
4. Коблиц Н. Курс теории чисел и криптографии. М.: Научное изд-во ТВП, 2001. 260 с.
5. Панасенко Сергей Петрович НИЗКОРЕСУРСНАЯ СИММЕТРИЧНАЯ КРИПТОГРАФИЯ: ПРИНЦИПЫ, ПОДХОДЫ И КОМПРОМИССЫ // ПДМ. Приложение. 2023. №16.
6. Рябко Б. Я., Фионов А.Н. Основы современной криптографии и стеганографии. М.: Горячая линия-Телеком, 2011. 232 с.
7. NISTIR 8114. Report on Lightweight Cryptography. URL: https://doi.org/10.6028/NIST.IR. 8114. 2017.