# Теория информационной безопасности и методология защиты информации

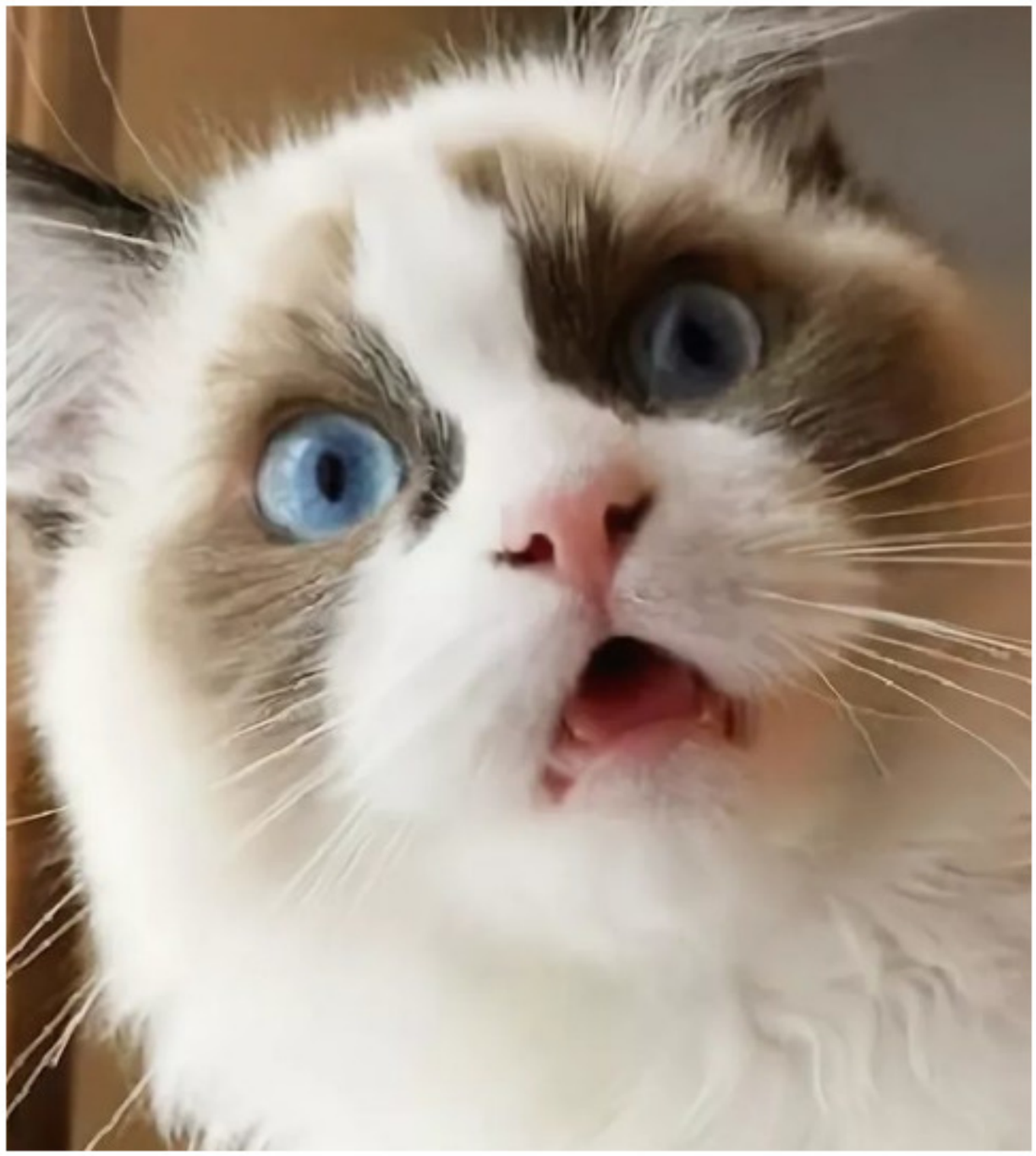
Лекция 7

Идентификация, аутентификация.
Электронная подпись

к.т.н., доцент ФБИТ
Коржук Виктория Михайловна

весна, 2023

# Предыдущая лекция



1. Модели БЛМ, ХРУ, Хартсона, MMS..
2. Модели Биба, Кларка-Вилсона...
3. Модель Миллена
4. ...

# Poll

Лучше всего на данный момент я знаю, что такое...

- симметричное и асимметричное шифрование
- потоковое и блочное шифрование
- электронная подпись
- идентификация и аутентификация
- чайный гриб

# Идентификация и аутентификация

Сопровождающие процессы:

1. Регистрация - внесение данных об идентификаторе и пароле в систему.
2. Редактрирование учетной записи
3. Удаление учетной записи

Основные процессы:

1. Идентификация - проверка идентификатора (логина)
2. Аутентификация - предоставление подтверждающей информцаии (секрета)
3. Авторизация - предоставление прав на действия в системе

# Виды аутентификации

1. Парольная (классическая)
2. Беспарольная (одноразовая ссылка для входа)
3. Биометрические
4. Многофакторные - любая совокупность, в основном пароль + дополнительный метод
5. По привязке к устройству
6. ...

| | | | |
|---|---|---|---|
| Биометрическая | Ваша ссылка для входа в уютную запись | По электронному ключу (флеш/ смарт-карты) | по привязке к устройству |
| | | | Хотите добавить данное |

# Matching Pairs

RUTUBE

Войти

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. «Cookie Policy».

**https://rutube.ru/video/05e19c094cf320dd167cf9fb76b75abc/**

Ok

12+ 4 года и 3 недели назад

В топ Сохранить Поделиться •••

# Шифрование

Симметричное - один и тот же ключ (код) за шифрования и расшифрования.

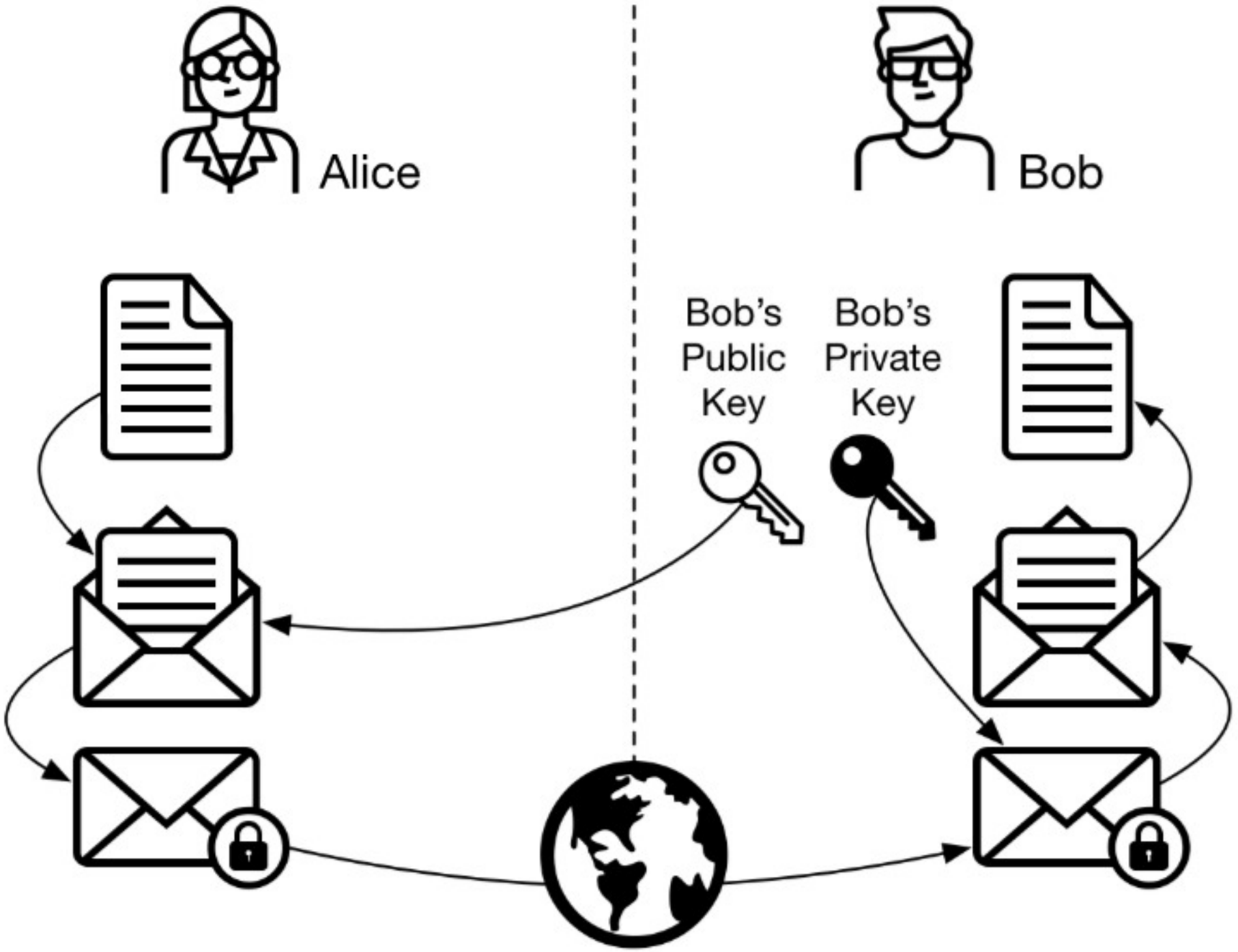
Например, для простого шифра сдвига "Цезарь" ключ - сам сдвиг по алфавиту.

Асимметричное - разные ключи для зашифрования и расшифрования.

Открытый и закрытый
или
Public и private

А еще блочное и поточное...

# Алиса и Боб



# Электронная подпись

1. Простая
2. Усиленная
    - 2.1. неквалифицированная
    - 2.2. квалифицированная

Как вы считаете, что такое простая электронная подпись?

Где может использоваться?

Instructions

Collaborate Board

Как вы считаете, что такое простая электронная подпись?

# Простая ЭП

Простая ЭП - совокупность логина и пароля.

Используется в корпоративных ИС, в которых для регистрации нужны паспортные данные или документы, удостоверяющие личность.

Содержит информацию об авторе, времени создания сообщения и, периодически, подтверждает целостность.

Instructions

Collaborate Board

Что же тогда усиленная ЭП? Чем она усилена?

# Хэш-функция

В идеале - необратима

Результат (хэш-сумма) - определенной длинны (зависит только от самой функции)

Коллизии 1 и 2 рода

# Схема ЭП

## Подписание документов усиленной квалифицированной электронной подписью


* В соответствии с пунктом 1 статьи 6 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

Instructions

Collaborate Board

# В чем разница между квалифицированной и неквалифицированной ЭП?

# Quiz

Если Алиса отправляет Бобу открытый ключ и подписанный закрытым ключом документ, то это...

- симметричное шифрование
- аутентификация по закрытому ключу
- проверка электронной подписи

Алгоритм, шифрующий символы в зависимости от их положения в последовательности - ...

- симметричный блочный
- симметричный поточный
- ассиметричный блочный
- ассиметричный потоковый

Если в процессе аутентификации пользователю приходит одноразовая ссылка для входа, то такой метод аутентификации называетя...

- многофакторная
- по специальному коду
- беспарольная
- по привязке к устройству

Может ли неквалифицированная усиленная ЭП иметь юридическую силу?

- всегда имеет
- имеет, если есть договор
- имеет, если не используется в роуминге
- никогда не имеет

В каком случае простая ЭП имеет юридическую силу?

- не имеет
- если есть договор
- если используется в закрытых корпоративных системах
- если используется в социальных сетях

Авторизация - это...

- присвоение прав
- совокупность идентификации и аутентификации
- подтверждение личности субъекта
- вход в систему

Какой сдвиг у фразы "Юфмфшуффкчягдфрпьяузк", зашифрованной шифром Цезаря?

- 7
- 12
- 3
- 17

# Exit ticket

Есть ли вопросы? Комментарии?

Instructions

Collaborate Board

## Exit ticket