Лекция №1

Часть 1. О курсе

Елена Киршанова

Курс “Основы криптографии”

Структура курса

I. Симметрическая криптография

- Псевдослучайные генераторы
- Блок-шифры
- Коды аутентификации сообщений
- Хэш-функции
- Шифрование с аутентификацией

II. Асимметрическая криптография

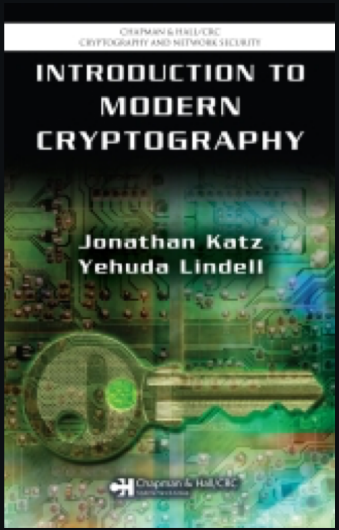
- Обмен ключами
- Цифровые подписи
- Асимметрическое шифрование
- Протоколы

Чего не будет

Мы не будем говорить о

- блокчейнах
- программировании / реверс инжиниринге
- хакерстве
- квантовой и пост-квантовой криптографии

Литература



A Graduate Course in Applied Cryptography

Dan Boneh, Victor Shoup

`https://toc.cryptobook.us/book.pdf`

Комментарии

- Подразумеваем знания элементарных алгоритмов, тер. вера, линейной алгебры
- Теоремы и доказательства в курсе будут строгими
- Будет много англоязычных слов!
- Опечатки неизбежны
- Комментарии/замечания/пожелания/недовольства можно отправить по почте

elenakirshanova [at] gmail [dot] com