Introduction to Cryptography

Lecture I

Introduction to the course

English

or

Russian?

Slides will be anyway in English

Admin stuff I

Lectures: Tue 15:20 — …

Labs: Tue after the lecture

Lecturer: Elena Kirshanova

Course's webpage:
https://crypto-kantiana.com/elena.kirshanova/teaching/info_sec2020.html

To pass the course: 100% of labs + written test

Questions/complaints to: elenakirshanova@gmail.com

Admin stuff II

In Labs you'll be playing with OpenSSL. Hence, C++

How to submit the labs:

1. On Tue after the lecture
2. Send me an email with a github link

Admin stuff II

In Labs you'll be playing with OpenSSL. Hence, C++

How to submit the labs:

1. On Tue after the lecture
2. Send me an email with a github link

Awesome news: No lecture/labs until 03.03

Syllabus I

This course does not cover

— reverse engineering
— hacking
— blockchain/e-cash/advanced primitives
— quantum or post-quantum crypto

Syllabus II

I

Symmetric crypto

- stream ciphers
- block ciphers (GOST, AES)
- hash functions
- cryptanalysis

II

Assymmetric crypto

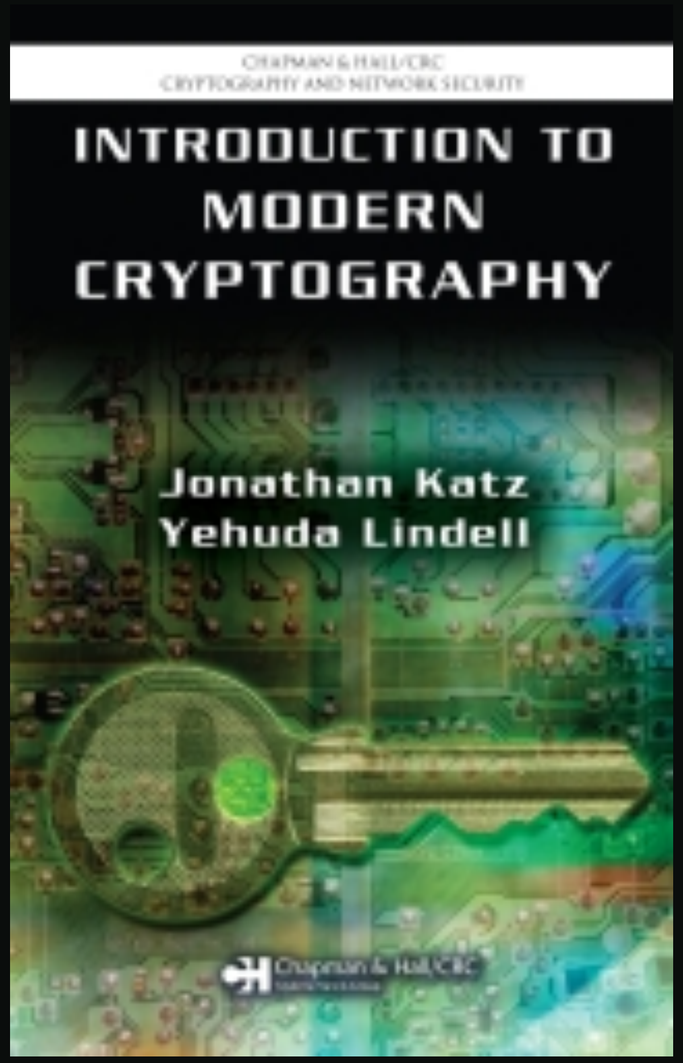
- RSA, factorisation
- Diffie-Hellman key exchange
- Signatures
- Key lengths, attacks

III

Applied crypto

- crypto in networks (SSH, TLS)
- PKI

Literature



A Graduate Course in Applied Cryptography
Dan Boneh and Victor Shoup
https://toc.cryptobook.us/book.pdf

Dan Boneh, Crypto I on Coursera

Prerequisites

Raise you hand if you are familiar with:

$$a \equiv b \bmod p$$

Prerequisites

Raise you hand if you are familiar with:

$$a \equiv b \bmod p$$

$$a^{\varphi(n)} \equiv 1 \bmod n$$

Prerequisites

Raise you hand if you are familiar with:

$$a \equiv b \bmod p$$

$$a^{\varphi(n)} \equiv 1 \bmod n$$

$$\mathbb{F}_p, g \in \mathbb{F}_p, ord(g)$$

Prerequisites

Raise you hand if you are familiar with:

$$a \equiv b \bmod p$$

$$a^{\varphi(n)} \equiv 1 \bmod n$$

$$\mathbb{F}_p, g \in \mathbb{F}_p, ord(g)$$

$$\mathbb{Z}_N^*$$

For the next lecture

1. Install OpenSSL
2. Create a toy project that includes OpenSSL
3. Try to generate an RSA key