Introduction to cryptography (course)

Alexander Buchnev

2023

Introduction

So, the time has come, I finally decided to create an introductory course on cryptography and read it during Fall 2023 semester at Innopolis University. Approximately, course will consist of 10 lectures + corresponding homeworks, and if I can manage it, I'll try to create a some sort of final exam.

Course prerequisites

There are no specific course prerequisites, although it would be great if students know some linear algebra and set theory, as well as can read the mathematical formulas.

Course description

This course is for those who want to become somewhat familiar with cryptography and for those who want to flex their brain muscles with new concepts. It is okay if you don't know much about cryptography and why is it important, at the end of the course you will be able to factor numbers of order 2^{1024} (joke) and hack some of weak implementations of cryptographic primitives (not a joke). The course consists of 10 lectures and homeworks with practical applications to real life. We will also consider some real-life attacks and some silly ones, from CTFs.

Course outcomes

The student is expected to become familiar with basic algebraic notations and definitions, as types of morphisms, semigroups, monoids, groups and rings, as well as obtain some practical experience with cryptanalysis and applied cryptography.

Course structure

1. Introduction + Basic Abstract algebra with SageMath
2. Basic abstract algebra with SageMath (cnt.)
3. Public key cryptography + concept of secure messaging
4. Message integrity: secure hash functions and random numbers
5. Asymmetric cryptography: RSA and Rabin cryptosystems
6. Asymmetric cryptography: DHKE with DLP some other key-exhange protocols
7. Asymmetric cryptography: ECDHKE and TLS/SSL
8. Asymmetric cryptography: digital signatures, GOST and Bitcoin curves
9. Inroduction to symmetric cryptography: block ciphers
10. Inroduction to symmetric cryptography: stream ciphers