help@otus.ru

Общая стоимость

42 000 руб.

В месяц: 10 500 руб.

Криптографическая защита информации

Баланс “теория vs. практика”, позволяющий глубоко разобраться в криптографических аспектах информационной безопасности

Продолжительность

5 месяцев, 4 часа в неделю

Начало занятий

30 мая

Длительность курса: 96 академических часов

1 Введение в криптографию

1 **Введение в криптографию**

Студенты познакомятся с
1. тем, какие задачами решает современная криптографиия
2. основными понятиями симметричной/ассиметричной криптографии
3. open source библиотеками крипто примитивов

Установят библиотеку OpenSSL, научатся вызывать функции библиотеки

Домашние задания

1 Проектная работа

Студенты разбиваются на группы по 3-5 человек, список предлагаемых тем:

1. Углубленное изучение симметрического криптоанализа ГОСТов Магма, Кузнечик (теоретические алгоритмы + рекомендации по длине ключа)
2. Тестирование псевдослучайных генераторов (алгоритмы тестирования, случай DUAL-ECC)
3. Системы электронного голосования. Система HELIOS. Принцип работы
4. Крипто на эллиптических кривых: реализации, криптоанализ (ГОСТ). Для студентов с уклоном в математику

---

2 **История криптографии. Наивная криптография**

Студенты познакомятся с первыми, известными нам, шифрами и древней криптографией

3	**История криптографии. Формальная криптография**	Студенты познакомятся с 1. частотным анализом как методом криптоанализа исторических шифров 2. важными формальными определениям в крипто 3. понятие One-time pad
4	**История криптографии. Математическая криптография**	Студенты познакомятся с 1. криптографией периода 2ой мировой войны 2. примитивами симметричной критографии

2 Симметричная криптография

1	**Генераторы псевдослучайных чисел (PRNG), Псевдо-случайные функции (PRF)**	
2	**Потоковое шифрование.**	
3	**Блочные шифры I**	
4	**Блочные шифры II**	
5	**Атаки на блочные шифры. Lightweight crypto**	
6	**Режимы шифрования**	
7	**Криптографическое обеспечение целостности данных**	Хэш-функции
8	**Код аутентификации сообщения**	

3 Асимметричная криптография

1	**Предварительные сведения из теории чисел. RSA I**	Слушатели получат необходимые знания из теории числе для понимания алгоритма RSA
2	**RSA на практике. Атаки на RSA**	
3	**Предварительные сведения из теории чисел II. Diffie-Hellman. Атака Man-in-the-middle**	
4	**Diffie-Hellman на эллиптических кривых**	
5	**Цифровые подписи I.**	
6	**Цифровые подписи II.**	
7	**Криптоанализ ассиметричных примитивов**	

4 Прикладные аспекты криптографии

1 **Гибридное шифрование. Инфраструктура открытых ключей**

2 **Инфраструктура открытых ключей II**

3 **Обеспечение безопасности в интернете**

4 **Безопасность TLS**

5 **Обеспечение безопасности в беспроводных сетях**

6 **Продвинутые протоколы I**

7 **Продвинутые протоколы II**

8 **Криптографические аспекты блокчейн-технологии. Часть I**

9 **Криптографические аспекты блокчейн-технологии. Часть II**

10 **Криптографические аспекты блокчейн-технологии. Часть III**

11 **Крипто в повседневной жизни**

12 **Продвинутые протоколы III**

5 Итоговая проектная работа

1 **Консультации и обсуждения проектной работы**

Домашние задания

1 Проектная работа

Студенты разбиваются на группы по 3-5 человек. Преподаватель распределяет задачи по проектной работе внутри каждой группы. Список предлагаемых тем:

1.Симметрический криптоанализ (AES, GOST).
Проектная работа включает в себя:
- реализацию на C++ одной из предложенных атак (дифференциальные или линейные атаки) на схемы AES и Ghost. К примеру, реализация результатов из работы https://eprint.iacr.org/2011/312.pdf (в выборе конкретных атак будут учтены пожелания студентов)
- демонстрация работы алгоритма на малых параметрах
- сделать сравнительный анализ атак, сделать вывод о битовой стойкости шифров
2. Статистический анализ псевдослучайных генераторов.
Проектная работа включает в себя:
- изучение методов статистического анализа псевдослучайных генераторов
- практическая реализация методов для генератора RC4 (источник https://infoscience.epfl.ch/record/165984/files/wpa-e11proc2.pdf)
- демонстрацию реализации
3. Open-sourse схема голосования e-voting HELIOS.
Проектная работа включает в себя:
- описание схемы работы электронного голосования (основные примитивы и модель

безопасности, используемые в системах голосования)
- развертывание схемы HELIOS (документация и код доступны по ссылке https://heliosvoting.org/).
- разработку демо-версии голосования (подсчет собранных голосов)
4. Эллиптическая криптография в протоколе обмена ключами.
Проектная работа включает в себя:
- изучение стандарта обмена ключом https://tools.ietf.org/html/rfc7836.html (используемые примитивы и их спецификации)
- реализацию алгоритма на языке C++
- демонстрацию реализации