**Факультет вычислительной математики и кибернетики**

**Межфакультетский курс**

**Основы криптографии в современном мире: шифрование в сотовых сетях, мессенджерах. Основы работы блокчейнов Bitcoin и Ethereum**

Cryptography fundamentals nowadays: encryption in cellular networks, messengers. Basic operation of Bitcoin and Ethereum blockchains

**Лекции: 26 часов**

**Лектор:** аспирант кафедры информационной безопасности факультета ВМК МГУ

Карнаухов Денис Юрьевич

**Аннотация**.

В современном мире мы ежедневно пользуемся достижениями криптографии: звонок по сотовому телефону, сообщение в мессенджере, загрузка интернет страницы, даже проход через турникет, используя проездную карту студента, не обходятся без применения шифрования.

Основной целью курса является объяснить принципы работы современных методов шифрования студентам, обладающим только школьным уровнем знания математики. Для достижения данной задачи будут использоваться наглядные упрощенные примеры с иллюстрациями.

В самом начале курса будет рассказано про простейшие виды шифрования, которые использовались до появления вычислительной техники. Студенты для наглядности смогут зашифровать любое сообщение, имея при себе только ручку и бумагу.

Следующая лекция будет посвящена симметричному шифрованию, а точнее случаю, когда оба участника переписки заранее договорились о секретном ключе, с помощью которого планируют шифровать сообщения.

Как же быть тем, кто заранее не смог договориться о секретном ключе? Ведь, если не зашифровать секретный ключ, его могут перехватить и расшифровать будущую переписку. Получается замкнутый круг: чтобы переслать секретный ключ нужно заранее договориться о другом секретном ключе. Неужели единственный способ разорвать замкнутый круг – это личная встреча. Для решения данной проблемы было придумано ассиметричное шифрование, которое позволяет передать секретный ключ по незащищенному каналу таким образом, что только отправитель и получатель будут знать его.

Далее будут рассмотрены средства, благодаря которым обеспечивается конфиденциальность передачи информации во время просмотра интернет страниц, методы злоумышленников для компрометации ваших данных, а также продемонстрированы простые способы защиты от этих угроз.

Насколько конфиденциальна и безопасна переписка в мессенджерах? Какой мессенджер самый безопасный? Правда ли, что Telegram не может читать секретные чаты пользователей?

Шифруются ли смс и звонки по телефону? Насколько сложно прослушать звонок или перехватить смс?

На основе уже полученных знаний мы попытаемся ответить на заданные вопросы.

Вторая часть курса будет посвящена блокчейну. Будет буквально на пальцах объяснена основная идея блокчейна, его структура и принцип работы. Также студенты будут ознакомлены с реализацией технологии блокчейн сначала на примере Bitcoin, затем Ethereum.

Основная задача второй части курса – развеять убеждение о сложности принципов работы блокчейна.

**Программа лекций.**

1. Краткая история криптографии.
2. Симметричное шифрование: блочный и поточный шифры, хеш-функция.
3. Ассиметричное шифрование.
4. Электронная подпись.
5. Протокол HTTPS. Сертификаты. Уязвимости HTTPS. Демонстрация MITM.Принцип работы VPN.
6. Принцип работы шифрования в мессенджерах. Секретные чаты Telegram.
7. Шифрование в сотовых сетях. Перехват SMS. SS7.
8. Введение в технологию “блокчейн”.
9. Bitcoin. Архитектура.
10. Изменения в протокол консенсуса Bitcoin на примере Segregated witness.
11. Bitcoin. Возможные векторы атаки.
12. Ethereum. Smart контракты.
13. Ethereum. Уязвимости.

**Вопросы.**

1. Объясните принцип работы одного из видов шифрования, использованного в прошлом.
2. Основные свойства хеш-функции. Для чего необходимы хеш-функции?
3. Приведите пример симметричного шифра.
4. В чём отличие ассиметричного шифрования от симметричного? Приведите пример ассиметричного шифра.
5. В чем отличие протокола HTTP от HTTPS? Объясните принцип работы атаки MITM.
6. Какие виды шифрования используются в мессенджерах?
7. Что такое SS7?
8. Основные составляющие блока в блокчейне.
9. Как вычисляется баланс кошелка в Bitcoin?
10. Какие изменения были внесены в Bitcoin с помощью Segregated Witness?
11. Какие, по вашему мнению, слабые стороны у Bitcoin?
12. Что такое smart контракт?
13. В чём отличия Ethereum от Bitcoin?