Курс «Принципы Современной Прикладной Криптографии: Симметричные криптосистемы».

Формат – лекции 48 академических часов (1,5 пары в неделю), лабораторные работы + семинары 32 часа (1 пара в неделю).

Курс рассчитан на студентов первого курса Магистратуры.

Курс состоит из четырёх основных разделов – совершенная стойкость и поточные шифры (1-3 неделя), блочные шифры (4-8 неделя), обеспечение целостности сообщений (9-14 неделя), Аутентифицированное шифрование (15-16 неделя). Для сдачи каждого раздела студенту необходимо сдача всех лабораторных работ данного раздела и защита домашней работы.

Особенностью лекционного материала является использование строгих математических моделей при описании криптографических примитивов, а также демонстрация принципов доказательства теоретической стойкости с использованием игровой модели Белларе – Рогавея.

Каждый раздел лекций построен по следующему принципу – математическое описание объекта криптосистемы, математическая модель нарушителя, понятие теоретической и практической стойкости модели, использование модели при построении примитивов, существующие криптографические примитивы, описываемые данной моделью.

Домашние задания представлены в форме теоретических задач. Защита домашних работ происходит во время лабораторных работ.

|  |  |
| --- | --- |
| Номер домашней работы | Тема |
| 1 | Абсолютная и семантическая стойкость. Формальная модель стойкости шифров. |
| 2 | Поточные шифры |
| 3 | Практические аспекты использования программных криптографических средств, Блочные шифры |
| 4 | Блочные шифры, псевдослучайные функции |
| 5 | Стойкость в модели атак по выбранным открытым текстам и соответствующим шифртекстам, уникальные величины и детерминированные шифры на их основе. |
| 6 | Коды аутентичности сообщений, схемы выработки кодов аутентичности сообщений. |
| 7 | Хэш-функции, модели хэш-функций. Использования хэш-функций для построения кодов аутентичности, выработки ключа, шифрования. |
| 8 | Стойкость в модели по выбранным шифртекстам и соответствующим их открытым текстам, аутентифицированное шифрование. |

При выполнении лабораторных работ студенты произведут ряд атак в уязвимых реализациях криптосистем. Для симуляции реальных атак будет развёрнут лабораторный стенд, представляющий собой Rest Web Api службу. Каждой лабораторной работе и каждому студенту будет соответствовать уникальная конечная точка данной службы, предоставляющая доступ к уязвимой криптосистеме с уникальными параметрами. При выполнении лабораторной работы студент должен произвести указанную атаку, взаимодействуя с веб-службой с помощью GET http запросов к службе.

Использование описанного выше подхода позволит получить уникальное задания для каждого студента, а также возможность реализации домашнего задания на произвольном языке программирования.

Темы лабораторных работ:

|  |  |
| --- | --- |
| Неделя | Тема |
| 1-3 | Атака при многократном использовании одноразового блокнота |
| Атака на аутентичность при использовании поточных шифров |
| 4-8 | Реализация режимов блочного шифрования |
| Построения оракула для распознания режимов шифрования |
| Атака на дешифрование ECB |
| Атака на схему с предсказуемым вектором инициализации |
| 9-14 | Атака код аутентичности сообщений на основе SHA-1 |
| Атака по времени на HMAC |
| Атака на подделку CBC MAC |
| Атака на хэш-функцию на основе кода аутентичности с фиксированным ключом |
| 15-16 | Атака c использованием оракула дополнений |