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 3 – 4 курса Бакалавриата и 1 – 2 второго 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.

Темы лекций:

|  |  |
| --- | --- |
| Неделя | Тема |
| 1 | Введение, принципы современной криптографии, понятие стойкости  Шифр Шеннона, Абсолютная стойкость;  Вычислимые шифры, Семантическая стойкость |
| 2 | Пренебрежимо малые величины, параметры стойкости и системные параметры, понятие игры, модель эффективного злоумышленника;  Псевдослучайные генераторы – определение и формальная модель, шифрование с использованием псевдослучайных генераторов;  Ограничения псевдослучайных генераторов, композиция псевдослучайных генераторов |
| 3 | Тест на определение следующего бита псевдослучайного генератора, Псевдослучайный генератор Salsa и ChaCha;  Линейные генераторы, псевдослучайный генератор RC4  Способы генерации случайных последовательностей. |
| 4 | Блочные шифры – определение и формальная модель,  Блочные шифры DES и AES |
| 5 | Атаки на блочные шифры – алгоритмические, атаки по побочным каналам, атаки на внесение ошибок, квантовые атаки;  Псевдослучайные функции – определение и формальная модель; |
| 6 | Псевдослучайные функции как модель блочных шифров, построение псевдослучайных функций на основе псевдослучайных генераторов;  Модель идеального шифра |
| 7 | Стойкость при множественном использовании ключа, атаки по произвольному множеству открытых и шифрованных текстов – определение и формальная модель, построение схем стойких к атакам по по произвольному множеству открытых и шифрованных текстов;  режим CTR псевдослучайных функций;  Режим CBC псевдослучайных функций, дополнение в режиме CBC и возможные атаки на него, Nonce based режимы шифрования |
| 8 | Прикладное использование криптопримитивов: анонимная маршрутизация, схемы залога;  Резерв |
| 9 | Коды аутентичности сообщений – определение и формальная модель;  Построение кодов аутентичности на основе псевдослучайных функций |
| 10 | Коды аутентичности CBC MAC, CMAC, PMAC;  Универсальные хэш функции;  Построение кодов аутентичности на основе универсальных хэш функций, композиция универсальных хэш функций |
| 11 | Коды аутентичности Картера – Вагмена; коды аутентичности с использованием Nonce, безусловно стойкие коды аутентичности;  Стойкие к коллизиям хэш функции– определение и формальная модель, построение кодов аутентичности сообщений, парадокс дней рождений;  Парадигма Маеркла-Дамгарда, атака Жо; |
| 12 | Построение функций сжатия, функции сжатия Девиса – Мейера, Хэш функция SHA 256;  Код аутентичности HMAC, Стойкость функции сжатия Девиса – Мейера  Губчатая конструкция, SHA3, SHAKE256, and SHAKE512 |
| 13 | Деревья Меркла, формирование симметричных ключей;  Модель Случайного Оракула, HKDF;  Стойкость при существовании коллизий, вероятностные хэш функции, целевые коллизии |
| 14 | Аутентифицированное шифрование – определение и формальная модель;  Шифрование как абстрактный интерфейс, базовые контракции аутентифицированного шифрования;  Nonce based шифрование с аутентифицированными дополнительными данными |
| 15 | Режим шифрования GCM, Протокол TLS 1.3, атака на протокол SSH;  Атака на протокол WEP, протокол IPSec |
| 16 | Сравнение зашифрованной информации, отзываемое широковещательное шифрование, поиск в зашифрованных данных, атаки по времени, Протокол получения скрытой информации;  Резерв |

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

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 | Атака аутентичность блочного шифра в режиме CBC |
| Реализация атаки с использованием оракула дополнения |
| Построения оракула для распознания режимов шифрования |
| Атака на дешифрование ECB |
| Атака на схему с фиксированным 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 |

Литература курса:

1. Boneh D. A Graduate Course in Applied Cryptography // Dan Boneh, Victor Shoup. − Version 0.4, September 2017. − 832 p.
2. Bellare M. Introduction to Modern Cryptography // Mihir Bellare, Phillip Rogaway. − May 11, 2005 .− 283 p.
3. Goldwasser S. Lecture Notes on Cryptography // Shafi Goldwasser, Mihir Bellare. − July 2008. − 289 p.
4. Katz J. Introduction to Modern Cryptography // Jonathan Katz, Yehuda Lindell. − 2007. − 512 p.
5. Menezes A. HANDBOOK of APPLIED CRYPTOGRAPHY // Alfred J. Menezes Paul C. van Oorschot Scott A. Vanstone . −June 1996 . − 794 p.