**ПРОГРАММА ДИСЦИПЛИНЫ**

СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Семестр** | **Лекции,**  **часов** | **Практические занятия,**  **часов** | **Лабораторные работы,**  **часов** | **Формы контроля**  **(зачет, экзамен, курсовая работа, курсовой проект)** |
| Осень | 32 | 0 | 32 | Экзамен |

АННОТАЦИЯ

Цель дисциплины – изучение современных подходов доказательной криптографии при анализе и построении криптографических схем.

Курс охватывает следующие темы – совершенная стойкость и поточные шифры, блочные шифры, обеспечение целостности сообщений, аутентифицированное шифрование. 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.

ТРЕБОВАНИЯ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

От студентов требуется владение навыками программирования на произвольном языке, поддерживающем работу с HTTP запросами, и навыки работы с ПК (ОС Windows или Linux) на уровне начинающего пользователя.

формируемые знания и умения

Студент, освоивший дисциплину, будет

знать:

- принципы построения и доказательства стойкости современных схем обеспечения конфиденциальности и целостности информации;

уметь:

- эффективно использовать средства криптографической защиты информации, уметь анализировать существующие реализации криптографических схем.

СТРУКТУРА ДИСЦИПЛИНЫ

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Наименование раздела** | **Недели** | **Лекции,**  **часов** | **Практические занятия, часов** | **Лабораторные работы, часов** | **Текущий контроль**  **(форма- неделя)** | **Аттестация раздела**  **(форма- неделя)** | **Максимальный балл** |
| *Осень* |  |  |  |  |  |  |  |
| Раздел 1  Совершенная стойкость и поточные шифры, блочные шифры | 1-8 | 16 | 0 | 0 | ДЗ-1,  ДЗ-2,  ДЗ-4,  ДЗ-5,  ДЗ-6 | ЛР-8,  КИ-8 | 25 |
| Раздел 2  Обеспечение целостности сообщений, аутентифицированное шифрование | 9-16 | 16 | 0 | 32 | ДЗ-10, ДЗ-11, ДЗ-12 | ЛР-16,  КИ-16 | 25 |
| **Аттестация** |  |  |  |  |  | Экзамен | 50 |

Сокращение наименований форм текущего контроля и аттестации разделов:

|  |  |
| --- | --- |
| **Обозначение** | **Полное наименование** |
| КИ | Аттестация по итогам текущего контроля |
| Т | Тестирование |
| ЛР | Лабораторные работы |
| КР | Контрольная работа |
| ДЗ | Домашнее задание |
| Сем | Работа на практическом занятии (семинаре) |
| Реф | Реферат |
| Д | Доклад |
| Кол | Коллоквиум |
| Отч | Отчет |

содержание дисциплины

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Недели** | **Темы занятий / Содержание** | **Лек., час.** | **Пр., час.** | **Лаб., час.** |
|  | *Осень* |  |  |  |
|  | **Раздел 1** Совершенная стойкость и поточные шифры, блочные шифры |  |  |  |
| 1 - 2 | **Основные понятия доказательной криптографии**  Введение, принципы современной криптографии, понятие стойкости, Шифр Шеннона, абсолютная стойкость, вычислимые шифры, семантическая стойкость, пренебрежимо малые величины, параметры стойкости и системные параметры, понятие игры, модель эффективного противника. | 4 | 0 | 4 |
| 2 - 4 | **Псевдослучайные генераторы**  Псевдослучайные генераторы – определение и формальная модель, шифрование с использованием псевдослучайных генераторов, ограничения псевдослучайных генераторов, композиция псевдослучайных генераторов. | 4 | 0 | 4 |
| 4 - 6 | **Поточные шифры**  Тест на определение следующего бита псевдослучайного генератора, псевдослучайный генератор Salsa и ChaCha,  линейные генераторы, псевдослучайный генератор CSS,  Способы генерации случайных последовательностей. | 4 | 0 | 4 |
| 7 - 8 | **Блочные шифры**  Блочные шифры – определение и формальная модель, блочные шифры DES, AES, Магма, Кузнечик, псевдослучайные функции – определение и формальная модель, псевдослучайные функции как модель блочных шифров, построение псевдослучайных функций на основе псевдослучайных генераторов, стойкость при множественном использовании ключа, атаки по произвольному множеству открытых и шифрованных текстов – определение и формальная модель, построение схем стойких к атакам по произвольному множеству открытых и шифрованных текстов, режим CTR, режим CBC, дополнение в режиме CBC и возможные атаки на него. | 4 | 0 | 4 |
|  | **Раздел 2** Обеспечение целостности сообщений, аутентифицированное шифрование |  |  |  |
| 9 - 12 | **Коды аутентичности сообщений** Коды аутентичности сообщений – определение и формальная модель;  Построение кодов аутентичности на основе псевдослучайных функций  Коды аутентичности CBC MAC, CMAC, PMAC. | 4 | 0 | 4 |
| 13 - 14 | **Хэш-функции** Коды аутентичности Картера – Вагмена, стойкие к коллизиям хэш-функции – определение и формальная модель, построение кодов аутентичности сообщений на основе хэш-функций, парадокс дней рождений, построение функций сжатия, функции сжатия Девиса – Мейера, хэш-функция SHA 256, стойкость функции сжатия Девиса – Мейера, губчатая конструкция, SHA3,  деревья Меркла, формирование симметричных ключей,  модель Случайного Оракула, стойкость при существовании коллизий. | 8 | 0 | 8 |
| 15 - 16 | **Аутентифицированное шифрование** Аутентифицированное шифрование – определение и формальная модель, шифрование как абстрактный интерфейс, базовые конструкции аутентифицированного шифрования, режим шифрования GCM, Протокол TLS 1.3, атака на протокол SSH, атака на протокол WEP, протокол IPSec, оракулы дополнений и атаки по времени. | 4 | 0 | 4 |
|  | ИТОГО | 32 | 0 | 32 |

вопросы к экзамену

1. Принципы доказательной криптографии, понятие модели и игры.
2. Пренебрежимо малые, суперполиномиальные и полиномиально ограниченные величины. Ограничения на противников и параметры схемы при рассмотрении стойкости.
3. Псевдослучайные генераторы.
4. Модель стойкого блочного шифры, PRF и PRP.
5. Семантическая стойкость
6. Стойкость при множественном использовании ключа
7. Режимы блочного шифрования.
8. Коды аутентичности сообщений, обеспечение целостности сообщений.
9. Построение кодов аутентичности сообщений на основе блочных шифров.
10. Стойкие к коллизиям и односторонние хэш-функции.
11. Принципы построения хэш-функций.
12. Построение кодов аутентичности сообщений с использование хэш-функций.
13. Выработка симметричных ключей с использованием хэш-функций и источника энтропии.
14. Аутентифицированное шифрование.
15. Построение стойких схем аутентифицированного шифрования.

рекомендуемые источники

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. − 2005.− 283 p.

3. Goldwasser S. Lecture Notes on Cryptography // Shafi Goldwasser, Mihir Bellare. − 2008. − 289 p.

4. Aumasson J. Serious Cryptography: A Practical Introduction to Modern Encryption. − 2017. − 313p.

5. Katz J. Introduction to Modern Cryptography // Jonathan Katz, Yehuda Lindell. − 2007. − 512 p.

6. Menezes A. HANDBOOK of APPLIED CRYPTOGRAPHY // Alfred J. Menezes Paul C. van Oorschot Scott A. Vanstone. − 1996. − 794 p.

7. Смарт Н. Криптография [Текст] / Н. Смарт. − М.: Техносфера, 2005. − 528 с.

требуемое оборудование и программное обеспечение

Компьютерный класс.