Министерство образования и науки РФ

Государственное образовательное учреждение высшего профессионального образования

**«Санкт-Петербургский государственный электротехнический университет “ЛЭТИ” им.В.И. Ульянова (Ленина)» (СПбГЭТУ)**

РАБОЧАЯ ПРОГРАММА

дисциплины

*«Криптографические протоколы»*

Для подготовки дипломированных специалистов по специальности 090301.65

*«Компьютерная безопасность»*

Санкт-Петербург

2011

Санкт-Петербургский государственный электротехнический

университет “ЛЭТИ”

"УТВЕРЖДАЮ"

проректор по учебной работе

Лысенко Н.В.

"\_\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_\_2011 г.

Рабочая программа

дисциплины

*«Криптографические протоколы»*

Для подготовки дипломированных специалистов по специальности 090301.65

*«Компьютерная безопасность»*

Уч.план № 836

Факультет компьютерных технологий и информатики

Кафедра автоматизированных систем обработки информации и управления

Курс – 5

Семестр – 9

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Лекции | 54 ч. |  | Экзамен | 9 семестр |
| Лабораторные занятия | 36 ч. |  | Зачет | 9 семестр |
| Практические занятия | 18 ч. |  |  |  |
| Курсовая работа | ч. |  | Курсовая работа | 9семестр |

|  |  |
| --- | --- |
| Аудиторные занятия | 108 ч. |
| Самостоятельные занятия | 96 ч. |
| Всего часов | 204 ч. |

2011 г.

Рабочая программа обсуждена на заседании кафедры автоматизированных систем обработки информации и управления «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2011 г., протокол № \_\_\_\_.

Рабочая программа составлена в соответствии с государственным образовательным стандартом для дипломированных специалистов по специальности

090301.65 — «Компьютерная безопасность»

Дисциплина «Криптографические протоколы» преподается на основе изученных ранее дисциплин:

* Алгебра и геометрия;
* Математический анализ;
* Вычислительная математика;
* Теория вероятностей и математическая статистика;
* Теоретические основы компьютерной безопасности;
* Теоретико-числовые методы в криптографии;
* Криптографические методы защиты информации;

и может являться фундаментом для изучения следующих дисциплин:

* Защита операционных систем и систем управления базами данных;
* Защита компьютерных сетей и телекоммуникаций;
* Технология разработки ИС в ЗИ.

Рабочая программа одобрена методической комиссией факультета компьютерных технологий и информатики «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2011 г.

Аннотация дисциплины

«Криптографические протоколы» является одной из основных дисциплин цикла «Методы и средства обеспечения информационной безопасности» и обеспечивает приобретение знаний, умений и навыков в области криптографической защиты информации в соответствии с государственным образовательным стандартом.

**Цели и задачи дисциплины**

1. Освоение теоретических основ решения задач аутентификации пользователей и информации, распределения ключей, обеспечения неотрекаемости и анонимности в современных информационных технологиях электронного документооборота и управления
2. Формирование практических навыков использования криптографических протоколов для решения задач обеспечения информационной безопасности компьютерных и телекоммуникационных систем.

**Требования к уровню освоения дисциплины**

Изучение дисциплины направлено на формирование вклада в следующие компетенции:

*ПК-2* – способность применять мат.аппарат, в т.ч. с использование ВТ, для решения проф.задач;

*ПК-12* – способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах;

*ПК-15* – способность применять современные методы и средства исследования для обеспечения ИБ КС;

*ПК-16* – способность проводить анализ безопасности КС с использованием отечественных и зарубежных стандартов в области КБ;

*ПК-18* – способность разрабатывать математические модели безопасности защищаемых КС;

*ПСК-8.4* – способность разрабатывать проектные решения по системам обеспечения ИБ ОИ на базе КС в защищенном исполнении;

*ПСК-8.5* – способность проводить анализ систем обеспечения ИБ ОИ на базе КС в защ.исполнении на предмет их соответствия требованиям по обеспечению ИБ.

В результате изучения дисциплины студент должен:

***знать и уметь использовать:***

* основные понятия и термины современных криптографических протоколов;
* математические модели описания криптографических протоколов;
* основные задачи информационной безопасности решаемые криптографическими протоколами;
* основные трудные задачи, лежащие в основе криптографических протоколов;
* пороговые схемы разделения секрета;
* методы строгой аутентификации пользователей;
* способы установки времени создания файлов;
* типовые криптографические протоколы и их криптографические качества;
* средства обеспечения анонимности пользователей;
* методы обеспечения неотрекаемости от электронных сообщений;
* основные стандарты электронной цифровой подписи;
* основные требования к выбору криптографических протоколов;

***иметь представление:***

* об основных типах криптографических протоколов;
* о современных тенденциях развития криптографических средств обеспечения компьютерной безопасности;
* о принципах разработки и применения криптографических протоколов для защиты и аутентификации электронной информации;
* о методах и критериях оценки надежности криптографических протоколов;
* об основных методах и средствах стойкости криптографических протоколов;
* об основных моделях нападений на криптографические протоколы;
* о требованиях к функциональным качествам криптографических протоколов;
* о протоколах открытого согласования и открытого распределения ключей;
* о национальных и международных криптографических стандартов;

***владеть навыками:***

* решения задач обеспечения информационной безопасности информационных и телекоммуникационных технологий криптографическими методами и средствами.
* применения криптографических протоколов и стандартов.

Содержание рабочей программы

**Вводная лекция**

Предмет, задачи и содержание дисциплины. Терминология и проблематика криптографических протоколов. Цели и задачи криптографической защиты и аутентификации электронной информации. Рекомендуемая литература.

**Тема 1. Сетевое взаимодействие абонентов**

Основные понятия, определения и объекты. Представления основных объектов. Модель взаимодействия. Криптографические протоколы и основные требования к ним. Протоколы "рукопожатия", протоколы установления подлинности. Протоколы идентификации и аутентификации. Парольные системы разграничения доступа. Условная и доказуемая стойкость криптографических протоколов. Теоретическая и практическая стойкость. Проблема распределения секретных ключей. Модели шифров. Проблема аутентификации ключей.

**Тема 2. Протоколы распределения ключей**

Типы и назначение ключей Основные, временные и сеансовые ключи. Открытые и закрытые ключи. Протоколы формирования защищаемых туннелей Протоколы распределения ключей. Задача согласования параметров канала по характеристикам его защищенности. Методы решения задачи генерации ключей. Математическая модель протокола. Протоколы открытого распределения и открытого согласования секретных ключей. Трудные задачи, лежащие в основе протоколов открытого распределения и согласования ключей.

**Тема 3. Пороговые схемы разделения секрета**

Задачи депонирования и хранения ключей. Пороговая схема разделения секрета на основе китайской теоремы об остатках. Пороговая схема разделения секрета на основе многочленов над конечными полями. Идеальные (оптимальные) пороговые схемы разделения секрета.

**Тема 4. Протоколы аутентификации**

Задача аутентификации информации и пользователей. Простая и строгая аутентификация. Достоинства и недостатки процедур простой и строгой аутентификации. Протоколы "рукопожатия", протоколы установления подлинности. Парольные системы разграничения доступа. Протоколы "рукопожатия" с использованием симметричных и асимметричных криптографических алгоритмов.

**Тема 5. Протоколы с нулевым разглашением**

Протоколы с нулевым разглашением. Понятие и доказательство нулевого разглашения. Итеративный протокол Фиата-Шамира на основе трудности задачи извлечения квадратных корней по составному модулю. Итеративные протоколы с нулевым разглашением над задачей дискретного логарифмирования. Трехпроходный протокол с нулевым разглашением. Вывод схем ЭЦП из протоколов с нулевым разглашением.

**Тема 6. Протоколы индивидуальной и коллективной цифровой подписи**

Протоколы электронной цифровой подписи (ЭЦП). Система RSA. Секретный и открытый ключ в системе RSA. Сложность проблемы разложения чисел на два простых множителя - основа стойкости системы RSA. Генерация секретного ключа. Генерация простых чисел. Генерация открытого ключа. Шифрование и формирование цифровой подписи. Стандарты электронной цифровой подписи ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001. Стандарты ЭЦП других стран. Протоколы мультиподписи. Коллективная м композиционная подпись. Упорядоченные мультиподписи. Целостность коллективной подписи. Требование контроля корректности формирования открытого ключа. Атаки на протоколы коллективной подписи. Редукционное доказательство стойкости коллективной подписи. Протоколы коллективной подписи над стандартами ЭЦП.

**Тема 7. Протоколы слепой подписи**

Задача обеспечения анонимности. Требования к протоколам слепой подписи. Протокол Чаума. Протоколы слепой ЭЦП над задачей дискретного логарифмирования. Протоколы слепой подписи над стандартами ЭЦП. Доказательство корректности и решение задачи обеспечения анонимности.

**Тема 8. Специальные криптографические протоколы**

Системы электронной жеребьевки, тайного электронного голосования. Системы электронных денег. Протоколы открытого и коммутативного шифрования. Игра в покер по телефону. Протокол послания в будущее. Установка метки времени создания файла. Особенности системы RSA: мультипликативность и коммутативность. Открытое шифрование методом Эль-Гамаля. Протоколы распределения ключей по каналам с помехами. Виртуальные частные сети. Метод туннелирования. Криптографические методы в защищенных виртуальных частных сетях. Криптографические протоколы, взлом которых требует одновременного решения двух трудных задач.

**Тема 9. Протоколы эллиптической криптографии**

Эллиптические кривые над конечными полями. Групповая операции сложения (суперпозиции) точек эллиптической кривой (ЭК). Геометрическая интерпретация операции сложения точек. Формулы вычисления суммы двух точек. Алгоритм быстрого умножения точки ЭК на число. Принцип использования эллиптической кривой для построения криптографических алгоритмов. Криптографические протоколы над задачей дискретного логарифмирования на эллиптической кривой. Специальные проколы эллиптической криптографии.

**Заключительная лекция**

Краткий обзор дисциплины. Перспективы развития криптографических протоколов. Рекомендации по самостоятельному углублению знаний в области криптографических протоколов.

#### **Перечень лабораторных работ**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Наименование темы занятия | Номер темы | Трудоемкость |
| 1 | Синтез протокола рукопожатия над криптосхемой с открытым ключом. | 7 | 8 |
| 2 | Реализация и исследование протоколов коллективной ЭЦП над эллиптическими кривыми. | 9 | 10 |
| 3 | Синтез протокола открытого распределения ключей с использованием криптосистемы RSA. | 2, 6 | 8 |
| 4 | Синтез схемы ЭЦП, взлом которой требует одновременного решения задачи дискретного логарифмирования и факторизации. | 8 | 10 |

#### **Перечень практических занятий**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Наименование темы занятия | Номер темы | Трудоемкость |
| 1 | Протокол рукопожатия над криптосхемой с открытым ключом. | 7 | 4 |
| 2 | Протоколы коллективной ЭЦП над эллиптическими кривыми. | 9 | 5 |
| 3 | Протокол открытого распределения ключей | 2, 6 | 4 |
| 4 | Схемы ЭЦП, взлом которых требует одновременного решения задачи дискретного логарифмирования и факторизации. | 8 | 5 |

**Цели и содержание курсовой работы**

Выполнение работ по курсовому проектированию является важным этапом подготовки специалистов. Представляется целесообразным выдавать задания по таким темам, которые развивают умение пользоваться математическим аппаратом и одновременно углубляют понимание идей, на основе которых обеспечивается требуемая функциональность криптографических протоколов. Темы заданий для курсового проектирования могут быть выбраны из основных разделов курса по криптографическим протоколам, включенных в программу вузовской подготовки специалистов. Например, темы могут быть сформулированы в соответствии со следующими разделами:

1. Разработка и/или анализ протоколов индивидуальной электронной цифровой подписи на основе сложности задачи дискретного логарифмирования или сложности задачи факторизации.
2. Разработка и/или анализ протоколов коллективной электронной цифровой подписи на основе сложности задачи дискретного логарифмирования.
3. Разработка и/или анализ протоколов слепой электронной цифровой подписи на основе сложности задачи дискретного логарифмирования.
4. Разработка и/или анализ протоколов коллективной электронной цифровой подписи на основе сложности задачи факторизации чисел специального вида.
5. Разработка и/или анализ протоколов слепой электронной цифровой подписи, основанных на сложности задачи факторизации больших чисел специального вида.
6. Разработка и программная реализация (*n*, *k*)-пороговых схем разделения секрета на основе многочленов над конечными полями.
7. Разработка и программная реализация (*n*, *k*)-пороговых схем разделения секрета на основе китайской теоремы об остатках.
8. Разработка и/или анализ протоколов с нулевым разглашением секрета на основе трудности одной из следующих задач: а) извлечения квадратных корней по трудно разложимому модулю, б) дискретного логарифмирования, в) факторизации чисел специального вида.
9. Разработка и/или анализ протоколов электронной цифровой подписи с восстановлением сообщения, основанных на основе сложности задачи дискретного логарифмирования.

Задачей курсового проектирования является проработка схемы ЭЦП, заданной проверочным уравнением.

Задание для курсового проектирования включает:

* общую характеристику и обоснование схемы ЭЦП, построенной на основе заданного проверочного уравнения;
* описание процедуры генерации подписи и формулирование требований к ней;
* оценку стойкости и безопасных размеров параметров криптосхемы;
* вывод формул для вычисления параметров *k* и *g*;
* анализ схемы на наличие слабостей и поиск вариантов усиления с минимальным модифицированием;
* рассмотрение возможности экзистенциальной подделки подписи;
* рассмотрение возможности сокращения размера подписи;
* рассмотрение необходимости дополнительных требований к выбору параметров схемы ЭЦП;
* рассмотрение необходимости дополнительных требований к генерации ключей;
* рассмотрение возможности преобразования в схему ЭЦП с восстановлением сообщения;
* критический анализ на 1) наличие избыточных операций в процедурах генерации и проверки подписи, 2) несоответствие длины открытого ключа и подписи достигаемому уровню стойкости;
* программную реализацию схемы и генерацию примера работы схемы с искусственно уменьшенным размером значений ее параметров (с учетом программной реализации дополнительные варианты могут быть сформированы путем задания 1) разных размеров для основных параметров схемы, 2) различных способов их генерации, 3) различной структуры чисел, используемых как модули и т. д.).

**Распределение учебных часов по темам, видам занятий**

**и видам самостоятельной работы**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№**  **темы** | **Название разделов и тем** | Объем учебных часов | | | | | | | **Семестр** | **Литература по темам** |
| **Лекции** | **Лабор.**  **занят.** | **Практ.занят.** | **Аудит.**  **занят.** | | **Сам.**  **работа** | **Всего** |
| **Всего** | **в т.ч. инт.формы** |
|  | Вводная лекция | 2 |  |  | 2 |  |  | 2 | 9 |  |
| 1 | Сетевое взаимодействие абонентов | 4 |  |  | 4 |  |  | 4 | 9 | Л5, Л8 |
| 2 | Протоколы распределения ключей | 6 | 4 | 2 | 12 | 4 | 2 | 14 | 9 | Л5, Л8 |
| 3 | Пороговые схемы разделения секрета | 8 |  |  | 8 |  |  | 8 | 9 | Л2, Л5 |
| 4 | Протоколы аутентификации | 8 |  |  | 8 |  |  | 8 | 9 | Л1, Л3, Л4 |
| 5 | Протоколы с нулевым разглашением | 4 |  |  | 4 |  |  | 4 | 9 | Л1, Л5, Л9 |
| 6 | Протоколы индивидуальной и коллективной цифровой подписи | 4 | 4 | 2 | 10 | 4 | 3 | 13 | 9 | Л2, Л5 |
| 7 | Протоколы слепой подписи | 6 | 8 | 4 | 18 | 8 | 5 | 23 | 9 | Л1, Л2, Л9 |
| 8 | Специальные криптографические протоколы | 6 | 10 | 5 | 21 | 10 | 7 | 28 | 9 | Л1, Л4, Л5 |
| 9 | Протоколы эллиптической криптографии | 4 | 10 | 5 | 19 | 10 | 7 | 26 | 9 | Л1, Л3, Л6, Л7 |
|  | Заключительная лекция | 2 |  |  | 2 |  |  | 2 | 9 |  |
| Курсовая работа | |  |  |  |  |  | 36 | 36 | 9 |
| Подготовка к экзамену | |  |  |  |  |  | 36 | 36 | 9 |
| ИТОГО: | | 54 | 36 | 18 | 108 | 36 | 96 | 204 |  |















# Учебно-методическое обеспечение дисциплины

# Основная литература

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Название, библиографическое описание | Л | Лр | Пз (С) | Кп | Кр | К-во экз. в библ. (на каф.) | Гриф |
| **Л1** | Дернова Е.С., Молдовян Д.Н., Молдовян Н.А. Криптографические протоколы. - СПб., Изд. СПбГЭТУ, 2010. - 100 с. | 9 | 9 | 9 |  | 9 | У(21) |  |
| **Л2** | Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. – СПб.: БХВ – Петербург, 2010. – 304 с. | 9 | 9 | 9 |  | 9 | нет |  |
| **Л3** | Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. – СПб.: БХВ – Петербург, 2005. – 286 с. | 9 | 9 | 9 |  | 9 | нет |  |
| **Л4** | Молдовян Н.А. Практикум по криптосистемам с открытым ключом. – СПб.: БХВ – Петербург, 2010. – 298 с. | 9 | 9 | 9 |  | 9 | нет |  |
| **Л5** | Дернова Е.С., Молдовян Н.А., Молдовяну П.А. Элементы теоретических основ криптографии. - СПб., Изд. СПбГЭТУ, 2009. – 92 с. | 9 |  |  |  | 9 | У(13)  Ф(2) |  |
| **Л6** | Еремеев М.А.., Молдовян Н.А., Молдовян А.А. Криптография. От примитивов к синтезу алгоритмов. – Спб.: БХВ – Петербург, 2004г. - 448с. | 9 | 9 | 9 |  | 9 | нет |  |
| **Л7** | Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптография. Скоростные шифры. – СПб.: БХВ – Петербург, 2002. – 496 с. | 9 | 9 | 9 |  | 9 | нет |  |
| **Л8** | Столлингс В. Криптография и защита сетей: принципы и практика., 2-е изд. : Пер. с англ. – Изд. Дом «Вильямс», 2001. – 672с. | 9 |  |  |  | 9 | У(12)  ЧЗ1(2) |  |

##### Дополнительная литература

|  |  |  |
| --- | --- | --- |
| № | Название, библиографическое описание | К-во экз. в библ. (на каф.) |
| **Д1** | Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2003. - 480с. | нет |
| **Д2** | Иванов М.А. Криптографические методы защиты информации. – М.: Кудиц-Образ. 2001г. - 368с. | нет |
| **Д3** | Шнайер Б. Прикладная криптогргафия. Протоколы, алгоритмы, исходные тексты на языке СИ. – М.: Триумф, 2002, -816с. | нет |
| **Д4** | Грушо А.А., Тимонина Е.Е., Применко Э.А. Анализ и синтез криптоалгоритмов. Курс лекций. Йошкар-Ола, 2000г. – 112с. | нет |
| **Д5** | Харин Ю.С., Агиевич С.В. Компьютерный практикум по математическим методам защиты информации: Учебное пособие. – Мн.: БГУ, 2001г. - 190с. | нет |
| **Д6** | Осипян В.О., Осипян К.В. Криптография в задачах и упражнениях. –М.: Гелиос АРВ., 2004г. – 144с. | нет |
| **Д7** | Бабаш А.В., Шанкин Г.П. Криптография – М. – Солон-Р, 2002, -512с. | Ф(1)  ЧЗ1(1) |
| **Д8** | Ростовцев А.Г. Алгебраические основы криптографии. – СПб.: НПО «Мир и семья», 2000г. | нет |
| **Д9** | Айерленд Р. Классическое введение в современную теорию чисел. – М.: Мир, 1987г. | Ф(4) |
| **Д10** | Степанов С.А. Арифметика алгебраических кривых. \_ М.: Наука, 1991г. – 368 с. | нет |
| **Д11** | Лидр Р., Нидеррайтер Г. Конечные поля: В 2-х т. Пер. с англ. \_ М.:, 1988г. – 430 с. | нет |
| **Д12** | Журналы: Безопасность информационных технологий (МИФИ), Вопросы защиты информации (ВИМИ), "Конфидент", Дискретная математика. | нет |
| **Д13** | Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. СПб., Лань, 2001. – 218 с. | У(9) |

|  |  |
| --- | --- |
| Зав. отделом учебной литературы *(для технических дисциплин)* | Киселева Т.В |

|  |  |
| --- | --- |
| Автор: |  |
| д.т.н., профессор | Молдовян Н.А. |
|  |  |
| Рецензент |  |
| д.т.н., профессор | Водяхо А.И. |
|  |  |
| Зав. кафедрой автоматизированных систем обработки информации управленияи и управления |  |
| д.т.н., профессор | Советов Б.Я. |
| Декан факультета КТИ,  д.т.н., профессор | Куприянов М.С. |
|  |  |
| Программа согласована: |  |
|  |  |
| Председатель методической комиссии факультета *компьютерных*  *технологий и информатики* |  |
| к.т.н., доц. | Михалков В.А. |
|  |  |
| Руководитель методического отдела |  |
| к.т.н., доцент | Марасина Л.А. |
|  |  |