

Запечников С. В.

Криптографические протоколы и их применение в финансовой и коммерческой деятельности: Учебное пособие для вузов. -М.: Горячая линия-Телеком, 2007. - 320 с.

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Глава 1. БАЗОВЫЕ КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

- 1.1. Закономерности организации сложных криптосистем
 - 1.2. Основы теории криптографических протоколов
 - 1.3. Вероятностные доказательства
 - 1.3.1. Интерактивные системы доказательства
 - 1.3.2. Доказательства с нулевым разглашением знания
 - 1.4. Протоколы аутентификации
 - 1.4.1. Парольная аутентификация
 - 1.4.2. Аутентификация методом «запрос - ответ»
 - 1.4.3. Аутентификация, основанная на доказательствах с нулевым разглашением знания
 - 1.5. Проблемы обеспечения конфиденциальности и аутентичности информации
 - 1.6. Специальные схемы цифровой подписи
 - 1.6.1. Схема цифровой подписи с восстановлением сообщения
 - 1.6.2. Схема цифровой подписи с опережающей безопасностью
 - 1.7. Схемы разделения секрета
 - 1.8. Технические средства поддержки криптографических протоколов
- Контрольные вопросы и задачи к гл. 1

Глава 2. ИНФРАСТРУКТУРА КРИПТОСИСТЕМ

- 2.1. Управление ключами
 - 2.1.1. Основные понятия и определения
 - 2.1.2. Жизненный цикл криптографических ключей
 - 2.1.3. Модели управления ключами
 - 2.1.4. Структура ключевой системы симметричных криптосхем

- 2.1.5. Методы распространения открытых ключей
- 2.1.6. Метод сертификации открытых ключей.
Инфраструктура открытых ключей
- 2.1.7. Особенности управления ключами в сложных (многодоменных) информационных системах
- 2.2. Протоколы распределения ключей
 - 2.2.1. Основные понятия и определения
 - 2.2.2. Свойства протоколов распределения ключей
 - 2.2.3. Протоколы распределения ключей, основанные на симметричных криптосхемах
 - 2.2.4. Протоколы распределения ключей, основанные на асимметричных криптосхемах
 - 2.2.5. Конференц-связь
 - 2.2.6. Методы анализа протоколов распределения ключей
- Контрольные вопросы и задачи к гл. 2

Глава 3. СИСТЕМЫ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ

- 3.1. Классификация и структура СЭП
 - 3.1.1. Модельное представление СЭП
 - 3.1.2. Обобщенный интерфейс прикладного программирования СЭП
 - 3.1.3. Потребительские качества СЭП
 - 3.1.4. Цели обеспечения безопасности информации в СЭП
- 3.2. Неанонимные СЭП, работающие в реальном масштабе времени
 - 3.2.1. Системы без криптографической защиты
 - 3.2.2. Системы с защищенными симметричными каналами
 - 3.2.3. Системы с симметричной аутентификацией
 - 3.2.4. Системы с аутентификацией посредством цифровой подписи
 - 3.2.5. Микроплатежи
- 3.3. Неанонимные автономные СЭП
 - 3.3.1. Системы на основе цифровой подписи

- 3.3.2. Системы с симметричной аутентификацией
 - 3.4. Анонимные СЭП, работающие в реальном масштабе времени
 - 3.4.1. Анонимные счета
 - 3.4.2. Анонимно переводимые «стандартные величины»
 - 3.4.3. СЭП на базе затемненной подписи
 - 3.5. Анонимные автономные СЭП
 - 3.5.1. СЭП, основанные на взломозащищенных устройствах
 - 3.5.2. СЭП с идентификацией повторной траты монеты
 - 3.5.3. СЭП Брандса
- Контрольные вопросы и задачи к гл. 3

Глава. 4 КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ В ЭЛЕКТРОННОЙ КОММЕРЦИИ И В ЭЛЕКТРОННОМ ДОКУМЕНТООБОРОТЕ

- 4.1. Основные задачи защиты информации в электронной коммерции
 - 4.1.1. Классификация задач электронной коммерции
 - 4.1.2. Пример: архитектура SEMPER
- 4.2. Защищенные каналы передачи информации
- 4.3. Честный обмен цифровыми подписями и его приложения
 - 4.3.1. Постановка задачи
 - 4.3.2. Схема Asokan - Shoup - Waidner
 - 4.3.3. Честный обмен цифровыми данными. Сертифицированная электронная почта
 - 4.3.4. Честный обмен в СЭП Брандса
 - 4.3.5. Одновременное подписание контракта
- 4.4. Многосторонние транзакции, коммерческие сделки, правовые отношения
 - 4.4.1. Электронные аукционы
 - 4.4.2. Криптографическая поддержка государственно-правовых отношений. Электронные выборы

Контрольные вопросы и задачи к гл. 4

ЗАКЛЮЧЕНИЕ

ЛИТЕРАТУРА

ПРИЛОЖЕНИЯ

А. Источники информации в сети Интернет

1. Международные, правительственные и профессиональные организации
2. Ведущие фирмы, занимающиеся проблемами криптологии
3. Собрания ссылок на ресурсы по криптологии
4. Личные страницы ученых-криптографов

Б. Учебные курсы по криптологическим дисциплинам, представленные в сети Интернет

КОММЕНТАРИИ И ССЫЛКИ

