

**Фороузан Б.А.**

Криптография и безопасность сетей: Учебное пособие / Фороузан Б.А.; пер. с англ. под ред. А.Н. Берлина. — М.: Интернет-Университет Информационных Технологий : БИНОМ. Лаборатория знаний, 2010. — 784 с: ил., табл. — (Основы информационных технологий).

# Оглавление

Предисловие к русскому переводу

Предисловие

## Лекция 1. Введение

- 1.1. Цели поддержки безопасности
- 1.2. Атаки
- 1.3. Услуги и механизмы
- 1.4. Методы
- 1.5. Остальные части книги
- 1.6. Рекомендованное чтение
- 1.7. Итоги
- 1.8. Набор для практики

## Часть 1. Шифрование симметричными ключами

### Лекция 2. Математика криптографии.

Часть I. Модульная арифметика, сравнения и матрицы

- 2.1. Арифметика целых чисел
- 2.2. Модульная арифметика
- 2.3. Матрицы
- 2.4. Линейное сравнение
- 2.5. Рекомендованная литература
- 2.6. Итоги
- 2.7. Набор для практики

### Лекция 3. Традиционные шифры с симметричным ключом

- 3.1. Введение
- 3.2. Шифры подстановки
- 3.3. Шифры перестановки
- 3.4. Шифры потока и блочные шифры
- 3.5. Рекомендованная литература
- 3.6. Итоги
- 3.7. Набор для практики

### Лекция 4. Математика криптографии.

Часть II. Алгебраические структуры

- 4.1. Алгебраические структуры
- 4.2. Поля  $GF(2^n)$

4.3. Рекомендованная литература

4.4. Итоги

4.5. Вопросы и упражнения

Лекция 5. Введение в основы современных шифров  
с симметричным ключом

5.1. Современные блочные шифры

5.2. Современные шифры потока

5.3. Рекомендованная литература

5.4. Итоги

5.5. Вопросы и упражнения

Лекция 6. Стандарт шифрования данных (DES)

6.1. Введение

6.2. Структура DES

6.3. Анализ DES

6.4. Многократное применение DES

6.5. Безопасность DES

6.6. Рекомендованная литература

6.7. Итоги

6.8. Набор для практики

Лекция 7. Усовершенствованный стандарт шифрования  
(AES — Advanced encryption standard)

7.1. Введение

7.2. Преобразования

7.3. Расширение ключей

7.4. Шифры

7.5. Примеры

7.6. Анализ AES

7.7. Рекомендованная литература

7.8. Итоги

7.9. Набор для практики

Лекция 8. Шифрование, использующее современные шифры  
с симметричным ключом

8.1. Применение современных блочных шифров

8.2. Использование шифров потока

8.3. Другие проблемы

8.4. Рекомендованная литература

8.5. Итоги

## 8.6. Набор для практики

### **Часть 2. Шифрование с асимметричными ключами**

#### **Лекция 9. Математика криптографии. Часть III.**

Простые числа и уравнения сравнения

- 9.1. Простые числа
- 9.2. Испытание простоты чисел
- 9.3. Разложение на множители
- 9.4. Китайская теорема об остатках
- 9.5. Квадратичное сравнение
- 9.6. Возведение в степень и логарифмы
- 9.7. Рекомендованная литература
- 9.8. Итоги
- 9.9. Набор для практики

#### **Лекция 10. Криптография с ассимметричным ключом**

- 10.1. Введение
- 10.2. Криптографическая система RSA
- 10.3. Криптосистема Рабина
- 10.4. Криптографическая система Эль-Гамал
- 10.5. Криптосистемы на основе метода эллиптических кривых
- 10.6. Рекомендованная литература
- 10.7. Итоги
- 10.8. Набор для практики

### **Часть 3. Целостность, установление подлинности и управление ключами**

#### **Лекция 11. Целостность сообщения и установление**

- 11.1. Целостность сообщения
- 11.2. Случайная модель Oracle
- 11.3. Установление подлинности сообщения
- 11.4. Рекомендованная литература
- 11.5. Итоги
- 11.6. Набор для практики

#### **Лекция 12. Криптографические хэш-функции**

- 12.1. Введение
- 12.2. SHA-512
- 12.3. Whirlpool

12.4. Рекомендованная литература

12.5. Итоги

12.6. Набор для практики

**Лекция 13. Цифровая подпись**

13.1. Сравнение

13.2. Процесс

13.3. Услуги

13.4. Атаки цифровой подписи

13.5. Схемы цифровой подписи

13.6. Варианты и приложения

13.7. Рекомендованная литература

13.8. Итоги

13.9. Набор для практики

**Лекция 14. Установление подлинности объекта**

14.1. Введение

14.2. Пароли

14.3. Запрос-ответ

14.4. Подтверждение с нулевым разглашением

14.5. Биометрия

14.6. Рекомендованная литература

14.7. Итоги

14.8. Набор для практики

**Лекция 15. Управление ключами**

15.1. Распределение с симметричными ключами

15.2. Цербер

15.3. Соглашение с симметричными ключами

15.4. Распределение открытого ключа

15.5. Рекомендованная литература

15.6. Итоги

15.7. Набор для практики

**Часть 4. Безопасность сети**

**Лекция 16. Безопасность на прикладном уровне: PGP И S/MIME**

16.1. Электронная почта

16.2. PGP

16.3. S/MIME

16.4. " Рекомендованная литература

16.5. Итоги

16.6. Набор для практики

**Лекция 17.** Безопасность на транспортном уровне: SSL И TLS

17.1. SSL-архитектура

17.2. Четыре протокола

17.3. Форматы сообщения SSL

17.4. Безопасность транспортного уровня

17.4. Рекомендованная литература

17.8. Итоги

17.7. Набор для практики

**Лекция 18.** Безопасность на сетевом уровне: IP SEC

18.1. Два режима

18.2. Два протокола безопасности

18.3. Услуги обеспечения безопасности трафика

18.4. Стратегия безопасности

18.5. Протокол интернет-обмена ключами (IKE)

18.6. ISAKMP

18.7. Рекомендованная литература

18.8. Итоги

18.9. Набор для практики

**Приложение А.** ASCII

**Приложение В.** Стандарты и организации по стандартизации

**Приложение С.** Набор протоколов TCP/IP

**Приложение D.** Элементарная теория вероятностей

**Приложение Е.** Проблемы дня рождения

**Приложение F.** Теория информации

**Приложение G.** Список неприводимых и примитивных полиномов

**Приложение H.** Простые числа, меньшие чем 10 000

**Приложение I.** Простые множители целых чисел, меньшие чем 1000

**Приложение J.** Список первых первообразных корней *для* простых чисел, меньших чем 1000

**Приложение K.** Генератор случайных чисел

**Приложение L.** Сложность

**Приложение М. ZIP**

**Приложение N.** Дифференциальный и линейный криптоанализ DES

**Приложение O.** Упрощенный DES (S-DES)

**Приложение P.** Упрощенный AES (S-AES)

**Приложение Q.** Некоторые доказательства

Глоссарий

Список литературы

Предметный указатель

Сокращения