

**Гашков СБ.**

**Криптографические методы защиты информации : учеб.  
пособие для студ. вузов / С. Б. Гашков, Э. А. Применко, М.  
А. Черепнев. — М.: Издательский центр «Академия»,  
2010. — 304 с.**

# ОГЛАВЛЕНИЕ

Предисловие

## Глава 1. Основные понятия криптографии

1.1. Исторический экскурс

1.2. Основные объекты криптографии

1.2.1. Формальная модель шифра

1.2.2. Асимметричная криптография

1.2.3. Гибридные схемы

1.2.4. Стойкость симметричных шифров

1.2.5. Имитостойкость симметричных шифров

## Глава 2. Алгебраические основы криптографии

2.1. Группы, кольца, поля

2.1.1. Кольца. Поля. Многочлены над полем

2.1.2. Характеристика поля

2.1.3. Мультипликативная группа конечного поля

2.1.4. Конечные расширения полей

2.1.5. След и норма элементов конечного поля

2.1.6. Полиномиальные и нормальные базисы

2.1.7. Алгебраическое замыкание конечного поля

2.1.8. Поля алгебраических чисел

2.2. Линейные рекуррентные последовательности

2.3. Логарифмические функции

2.3.1. Первообразные корни и индексы

2.3.2. Частное Ферма

2.3.3. Другие логарифмические функции в  
конечных полях

## Глава 3. Эллиптические кривые

3.1. Кривые над произвольным полем

3.1.1. Основные определения

3.1.2. Дискриминант и инвариант эллиптической  
кривой

3.2. Группа точек эллиптической кривой

3.2.1.Строение некоторых классов групп  $\mathcal{E}_p(a, 0)$  и  $\mathcal{E}_p(0, B)$

3.2.2.Верхние и нижние оценки порядка группы  $\mathcal{E}_p(a, B)$

3.3.Эллиптические кривые над полем характеристики 2

3.4.Выбор точки и размещение данных

3.4.1.Решение квадратных уравнений

3.4.2.Выбор точки эллиптической кривой

Размещение данных на эллиптической кривой

3.4.4. Определение порядка точки

эллиптической кривой и

нахождение образующего элемента группы точек

эллиптической кривой

## Глава 4. Базовые протоколы в конечных полях

4.1.Протоколы совместной выработки общего ключа (открытое распределение ключей)

4.1.1.Протокол Асмута — Блюма

4.1.2.Протокол Диффи — Хеллмэна и его модификации

4.1.3.Схема Якоби

4.2.Сравнительная стойкость некоторых криптосхем, построенных на основе задачи дискретного логарифмирования

4.2.1.Схема распределения ключей Окамото

4.2.2.Схема шифрования Шамира — Мэсси — Омуре

4.2.3.Схема Белэйра — Микали (случайный выбор из списка)

4.2.4.Сравнение стойкости задачи Диффи — Хеллмэна

и дискретного логарифмирования

4.3.Вероятностное шифрование

4.4.Протоколы аутентификации

4.4.1.Схема Файге — Фиата — Шамира

4.4.2.Схема Шнорра

4.4.3.Схема Шаума

4.4.4.Протокол аутентификации на основе криптосистемы RSA

4.5.Электронная цифровая подпись

- 4.5.1. Криптосхема RS A
- 4.5.2. Криптосхемы Эль-Гамала
- 4.5.3. Схема Брикелла — Ли — Якоби
- 4.5.4. Схема Шнорра
- 4.5.5. Стандарты электронной подписи РФ и США
- 4.5.6. Схема Фиата - Шамира
- 4.5.7. Схема Рабина
- 4.6. Стираемые подписи
  - 4.6.1. Схема Шаума — Антверпена
  - 4.6.2. Схема Шаума
  - 4.6.3. Стандарт стираемой подписи
  - 3.4.3.
- 4.7. Слепые подписи
  - 4.7.1. Слепая подпись RSA
  - 4.7.2. Слепая подпись Шнорра
  - 4.7.3. Слепая подпись Окамото — Шнорра
  - 4.7.4. Законная слепая подпись
- 4.8. Подпись, в которой подделка может быть доказана
- 4.9. Блобы
- 4.10. Электронные платежи
  - 4.10.1. Схемы Брандса
  - 4.10.2. Переводимая монета
  - 4.10.3. Электронный бумажник

## **Глава 5. Прикладные протоколы в конечных полях**

- 5.1. Протоколы распределения ключей
  - 5.1.1. Протоколы распределения сеансовых секретных ключей
- 5.2. Современные стандарты симметричного шифрования
  - 5.2.1. DES
  - 5.2.2. ГОСТ 28147-89
  - 5.2.3. RND
- 5.3. Протоколы разделения секрета
  - 5.3.1. Интерполяционные пороговые схемы разделения секрета
  - 5.3.2. Матричные пороговые (п,г-)-схемы
  - 5.3.3. Модулярная схема разделения секретов
  - 5.3.4. Групповой протокол разделения секрета
  - 5.3.5. Индивидуально-групповой протокол разделения секрета
- 5.4. Протоколы скрытой передачи секрета

- 5.4.1.Общая схема протокола скрытой передачи  $k$  секретов на основе односторонней функции
- 5.4.2.Теоретико-числовой протокол скрытой передачи секретов
- 5.4.3.Надежный для обладателя секретов протокол скрытой передачи секрета
- 5.4.4.Надежный протокол передачи секретов двум пользователям
- 5.4.5.Протокол скрытой передачи секрета, использующий две криптосистемы
- 5.5.Протоколы доказательств с нулевым разглашением
  - 5.5.1.Протокол доказательства знания факторизации
  - 5.5.2.Протокол доказательства знания дискретного логарифма
  - 5.5.3.Протокол доказательства правильности выбора модуля вычислений для системы RSA
- 5.6.Протоколы голосования
  - 5.6.1.Протокол с одним Доверенным центром
  - 5.6.2.Протоколы голосования с несколькими центрами
- 5.7.Протоколы подбрасывания монеты по телефону
  - 5.7.1.Формальная модель протокола подбрасывания монеты
  - 5.7.2.Экспоненциальный протокол совместной выработки случайного бита
  - 5.7.3.Экспоненциальный протокол подбрасывания монеты
  - 5.7.4.Протокол подбрасывания монеты на основе квадратичнс вычета по модулю числа Блюма
  - 5.7.5.Протокол подбрасывания монеты на основе символа Якоби
  - 5.7.6.Протокол подбрасывания монеты на основе корней сравнения  $x^2 = a(\text{mod}n)$ , являющихся квадратичными вычетами
- 5.8.Игра в покер по телефону
- 5.9.Алгоритмы хэширования
  - 5.9.1.Хэш-алгоритм MD-5
  - 5.9.2.Хэш-алгоритм SHA
  - 5.9.3.ГОСТ Р-34-10-94
  - 5.9.4.Атака на ЭЦП на основе коллизий хэш-функции

## **Глава 6. Протоколы на основе алгебраических**

## **объектов**

- 6.1. Схемы Имаи — Матсумото — Патарина
- 6.2. Распределение ключей с помощью эллиптических кривых
  - 6.2.1. Протокол Диффи — Хеллмэна распределения ключей для классической криптосистемы
  - 6.2.2. Протокол Мэсси — Омура распределения ключей для классической криптосистемы
  - 6.2.3. Протокол распределения ключей Менезеса — Кью — Венстоуна (MQV-протокол)
- 6.3. Криптосистемы Эль-Гамала на эллиптических кривых
- 6.4. Протоколы цифровой подписи на эллиптических кривых
  - 6.4.1. Электронная цифровая подпись
  - 6.4.2. Обобщенная схема электронной подписи Эль-Гамала
  - 6.4.3. Электронная подпись Эль-Гамала с возвратом сообщения (схема Ньюберга — Рюппеля)
- 6.5. Стандарт ЭЦП (ГОСТ Р-34-10-2001)
- 6.6. Стандарты выбора кривых для имплементации криптосистем Билинейная проблема Диффи — Хеллмэна и спаривание
  - 6.7.1. Однораундовый протокол генерации общего секретного ключа между тремя участниками
  - 6.7.2. Короткая цифровая подпись, основанная на спаривании
  - 6.7.3. Криптосистема с публичным индивидуальным ключом

Предметный указатель

Список литературы









5.7.7.