Брюс Шнайер

Прикладная криптография

2-е издание

Протоколы, алгоритмы и исходные тексты на языке C

СОДЕРЖАНИЕ

Глава 3
Основные протоколы

3.1 Обмен ключами
3.2 Удостоверение подлинности
3.3 Удостоверение подлинности и обмен ключами
3.4 Формальный анализ протоколов проверки подлинности и обмена ключами
3.5 Криптография с несколькими открытыми ключами
3.6 Разделение секрета
3.7 Совместное использование секрета
3.8 Криптографическая защита баз данных

Глава 4
Промежуточные протоколы

4.1 Службы меток времени
4.2 Подсознательный канал
4.3 Неотрицаемые цифровые подписи
4.4 Подписи уполномоченного свидетеля
4.5 Подписи по доверенности
4.6 Групповые подписи
4.7 Подписи с обнаружением подделки
4.8 Вычисления с зашифрованными данными
4.9 Вручение битов
4.10 Подбрасывание "честной" монеты
4.11 Мысленный покер
4.12 Однонаправленные сумматоры
4.13 Раскрытие секретов "все или ничего"
4.14 Условное вручение ключей

Глава 5
Развитые протоколы

5.1 Доказательства с нулевым знанием
5.2 Использование доказательства с нулевым знанием для идентификации
5.3 Слепые подписи
5.4 Личностная криптография с открытыми ключами
5.5 Рассеянная передача
5.6 Рассеянные подписи
5.7 Одновременная подпись контракта
5.8 Электронная почта с подтверждением
5.9 Одновременный обмен секретами

Глава 6
Эзотерические протоколы

6.1 Безопасные выборы
6.2 Безопасные вычисления с несколькими участниками
6.3 Анонимная широковещательная передача сообщений
6.4 Электронные наличные

Часть II Криптографические методы

Глава 7
Длина ключа

Глава 8
Управление ключами

Глава 9
Типы алгоритмов и криптографические режимы

Глава 10 (Текст главы на английском, sorry. Переводчик, похоже, устал :-)
Использование алгоритмов

Часть III Криптографические алгоритмы

Глава 11
Математические основы

Глава 12
Стандарт шифрования данных DES

Глава 13
Другие блочные шифры

Глава 14
И еще о блочных шифрах

Глава 15
Объединение блочных шифров

Глава 16
Генераторы псевдослучайных последовательностей и потоковые шифры

Глава 17
Другие потоковые шифры и генераторы настоящих случайных последовательностей

Глава 18
Однонаправленные хэш-функции

Глава 19
Алгоритмы с открытыми ключами

Глава 20
Алгоритмы цифровой подписи с открытым ключом

Глава 21
Схемы идентификации

Глава 22
Алгоритмы обмена ключами

Глава 23
Специальные алгоритмы для протоколов

Часть IV Реальный мир

Глава 24
Примеры реализаций

Глава 25
Политика

Мэтт Блейз. Послесловие

Часть V Исходные коды

1. DES
2. LOKI91
3. IDEA
4. GOST
5. BLOWFISH
6. 3-WAY
7. RC5
8. A5
9. SEAL

Библиография