

Брюс Шнайер
Прикладная криптография
2-е издание
Протоколы, алгоритмы и исходные тексты на языке C

СОДЕРЖАНИЕ

Уитфилд Диффи. Предисловие

Введение

Глава 1

Основные понятия

- 1.1 Терминология
- 1.2 Стеганография
- 1.3 Подстановочные и перестановочные шифры
- 1.4 Простое XOR
- 1.5 Одноразовые блокноты
- 1.6 Компьютерные алгоритмы
- 1.7 Большие числа

Часть I Криптографические протоколы

Глава 2

Элементы протоколов

- 2.1 Введение в протоколы
- 2.2 Передача информации с использованием симметричной криптографии
- 2.3 Однонаправленные функции
- 2.4 Однонаправленные хэш-функции
- 2.5 Передача информации с использованием криптографии с открытыми ключами
- 2.6 Цифровые подписи
- 2.7 Цифровые подписи и шифрование
- 2.8. Генерация случайных и псевдослучайных последовательностей

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

- 7.1 Длина симметричного ключа
- 7.2 Длина открытого ключа
- 7.3 Сравнение длин симметричных и открытых ключей
- 7.4 Вскрытие в день рождения против однонаправленных хэш-функций
- 7.5 Каков должны быть длина ключа?
- 7.6 Caveat emptor

Глава 8

Управление ключами

- 8.1 Генерация ключей
- 8.2 Нелинейные пространства ключей
- 8.3 Передача ключей
- 8.4 Проверка ключей
- 8.5 Использование ключей
- 8.6 Обновление ключей
- 8.7 Хранение ключей
- 8.8 Резервные ключи
- 8.9 Скомпрометированные ключи
- 8.10 Время жизни ключей
- 8.11 Разрушение ключей
- 8.12 Управление открытыми ключами

Глава 9

Типы алгоритмов и криптографические режимы

- 9.1 Режим электронной шифровальной книги
- 9.2 Повтор блока
- 9.3 Режим сцепления блоков шифра
- 9.4 Поточковые шифры
- 9.5 Самосинхронизирующиеся потоковые шифры
- 9.6 Режим обратной связи по шифру
- 9.7 Синхронные потоковые шифры
- 9.8 Режим выходной обратной связи
- 9.9 Режим счетчика
- 9.10 Другие режимы блочных шифров
- 9.11 Выбор режима шифра
- 9.12 Прослаивание
- 9.13 Блочные шифры против потоковых шифров

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

Использование алгоритмов

- 10.1 Выбор алгоритма
- 10.2 Криптография с открытым ключом против симметричной криптографии

- 10.3 Шифрование коммуникационных каналов
- 10.4 Шифрование хранимых данных
- 10.5 Аппаратное шифрование против программного шифрования
- 10.6 Компрессия, кодирование и шифрование
- 10.7 Выявление шифрования
- 10.8 Скрытие шифртекста в шифртексте
- 10.9 Разрушение информации

Часть III Криптографические алгоритмы

Глава 11

Математические основы

- 11.1 Теория информации
- 11.2 Теория сложности
- 11.3 Теория чисел
- 11.4 Разложение на множители
- 11.5 Генерация простого числа
- 11.6 Дискретные логарифмы в конечном поле

Глава 12

Стандарт шифрования данных DES

- 12.1 Введение
- 12.2 Описание DES
- 12.3 Безопасность DES
- 12.4 Дифференциальный и линейный криптоанализ
- 12.5 Реальные критерии проектирования
- 12.6 Варианты DES
- 12.7 Насколько безопасен сегодня DES?

Глава 13

Другие блочные шифры

- 13.1 LUCIFER
- 13.2 MADRYGA
- 13.3 NewDES
- 13.4 FEAL
- 13.5 REDOC
- 13.6 LOKI
- 13.7 KHUFU и KHAFRE
- 13.8 RC2
- 13.9 IDEA
- 13.10 MMB
- 13.11 CA-1.1
- 13.12 SKIPJACK

Глава 14

И еще о блочных шифрах

- 14.1 ГОСТ
- 14.2 CAST
- 14.3 BLOWFISH
- 14.4 SAFER
- 14.5 3-WAY
- 14.6 CRAB
- 14.7 SXAL8/MBAL
- 14.8 RC5
- 14.9 Другие блочные алгоритмы
- 14.10 Теория проектирования блочного шифра
- 14.11 Использование однонаправленных хэш-функций
- 14.12 Выбор блочного алгоритма

Глава 15

Объединение блочных шифров

- 15.1 Двойное шифрование
- 15.2 Тройное шифрование
- 15.3 Удвоение длины блока
- 15.4 Другие схемы многократного шифрования
- 15.5 Уменьшение длины ключа в CDMF
- 15.6 Отбеливание
- 15.7 Многократное последовательное использование блочных алгоритмов
- 15.8 Объединение нескольких блочных алгоритмов

Глава 16

Генераторы псевдослучайных последовательностей и потоковые шифры

- 16.1 Линейные конгруэнтные генераторы
- 16.2 Сдвиговые регистры с линейной обратной связью
- 16.3 Проектирование и анализ потоковых шифров
- 16.4 Потоковые шифры на базе LFSR
- 16.5 A5
- 16.6 Hughes XPD/KPD
- 16.7 Nanoteq
- 16.8 Rambutan
- 16.9 Аддитивные генераторы
- 16.10 Gifford
- 16.11 Алгоритм M
- 16.12 PKZIP

Глава 17

Другие потоковые шифры и генераторы настоящих случайных последовательностей

- 17.1 RC4
- 17.2 SEAL

- 17.3 WAKE
- 17.4 Сдвиговые регистры с обратной связью по переносу
- 17.5 Поточковые шифры, использующие FCSR
- 17.6 Сдвиговые регистры с нелинейной обратной связью
- 17.7 Другие поточковые шифры
- 17.8 Системно-теоретический подход к проектированию поточковых шифров
- 17.9 Сложностно-теоретический подход к проектированию поточковых шифров
- 17.10 Другие подходы к проектированию поточковых шифров
- 17.11 Шифры с каскадом нескольких потоков
- 17.12 Выбор поточкового шифра
- 17.13 Генерация нескольких потоков из одного генератора псевдослучайной последовательности
- 17.14 Генераторы реальных случайных последовательностей

Глава 18

Однонаправленные хэш-функции

- 18.1 Основы
- 18.2 Snefru
- 18.3 *N*-хэш
- 18.4 MD4
- 18.5 MD5
- 18.6 MD2
- 18.7 Алгоритм безопасного хэширования (Secure Hash Algorithm, SHA)
- 18.8 RIPE-MD
- 18.9 HAVAL
- 18.10 Другие однонаправленные хэш-функции
- 18.11 Однонаправленные хэш-функции, использующие симметричные блочные алгоритмы
- 18.12 Использование алгоритмов с открытым ключом
- 18.13 Выбор однонаправленной хэш-функции
- 18.14 Коды проверки подлинности сообщения

Глава 19

Алгоритмы с открытыми ключами

- 19.1 Основы
- 19.2 Алгоритмы рюкзака
- 19.3 RSA
- 19.4 Pohlig-Hellman
- 19.5 Rabin
- 19.6 ElGamal
- 19.7 McEliece
- 19.8 Криптосистемы с эллиптическими кривыми
- 19.9 LUC
- 19.10 Криптосистемы с открытым ключом на базе конечных автоматов

Глава 20

Алгоритмы цифровой подписи с открытым ключом

- 20.1 Алгоритм цифровой подписи (DIGITAL SIGNATURE ALGORITHM, DSA)
- 20.2 Варианты DSA
- 20.3 Алгоритм цифровой подписи ГОСТ
- 20.4 Схемы цифровой подписи с использованием дискретных логарифмов

- 20.5 ONG-SCHNORR-SHAMIR
- 20.6 ESIGN
- 20.7 Клеточные автоматы
- 20.8 Другие алгоритмы с открытым ключом

Глава 21

Схемы идентификации

- 21.1 FEIGE-FIAT-SHAMIR
- 21.2 GUILLOU-QUISQUATER
- 21.3 SCHNORR
- 21.4 Преобразование схем идентификации в схемы подписи

Глава 22

Алгоритмы обмена ключами

- 22.1 DIFFIE-HELLMAN
- 22.2 Протокол "точка-точка"
- 22.3 Трехпроходный протокол Шамира
- 22.4 COMSET
- 22.5 Обмен зашифрованными ключами
- 22.6 Защищенные переговоры о ключе
- 22.7 Распределение ключа для конференции и секретная ширококвещательная передача

Глава 23

Специальные алгоритмы для протоколов

- 23.1 Криптография с несколькими открытыми ключами
- 23.2 Алгоритмы разделения секрета
- 23.3 Подсознательный канал
- 23.4 Неотрицаемые цифровые подписи
- 23.5 Подписи, подтверждаемые доверенным лицом
- 23.6 Вычисления с зашифрованными данными
- 23.7 Бросание "честной" монеты
- 23.8 Однонаправленные сумматоры
- 23.9 Раскрытие секретов "все или ничего"
- 23.10 Честные и отказоустойчивые криптосистемы
- 23.11 ZERO-KNOWLEDGE PROOFS OF KNOWLEDGE
- 23.12 Слепые подписи
- 23.13 Передача с забыванием
- 23.14 Безопасные вычисления с несколькими участниками
- 23.15 Вероятностное шифрование
- 23.16 Квантовая криптография

Часть IV Реальный мир

Глава 24

Примеры реализаций

- 24.1 Протокол управления секретными ключами компании IBM
- 24.2 MITRENET
- 24.3 ISDN
- 24.4 STU-III
- 24.5 KERBEROS
- 24.6 KRYPTOKNIGHT
- 24.7 SESAME
- 24.8 Общая криптографическая архитектура IBM
- 24.9 Схема проверки подлинности ISO
- 24.10 Почта с повышенной секретностью PRIVACY-ENHANCED MAIL (PEM)
- 24.11 Протокол безопасности сообщений
- 24.12 PRETTY GOOD PRIVACY (PGP)
- 24.13 Интеллектуальные карточки
- 24.14 Стандарты криптографии с открытыми ключами
- 24.15 Универсальная система электронных платежей
- 24.16 CLIPPER
- 24.17 CAPSTONE
- 24.18 Безопасный телефон AT&T MODEL 3600 TELEPHONE SECURITY DEVICE (TSD)

Глава 25

Политика

- 25.1 Агентство национальной безопасности (NSA)
- 25.2 Национальный центр компьютерной безопасности (NCSC)
- 25.3 Национальный институт стандартов и техники
- 25.4 RSA Data Security, Inc.
- 25.5 PUBLIC KEY PARTNERS
- 25.6 Международная ассоциация криптологических исследований
- 25.7 Оценка примитивов целостности RACE (RIPE)
- 25.8 Условный доступ для Европы (SAFE)
- 25.9 ISO/IEC 9979
- 25.10 Профессиональные и промышленные группы, а также группы защитников гражданских свобод
- 25.11 Sci.crypt
- 25.12 Шифропанки
- 25.13 Патенты
- 25.14 Экспортное законодательство США
- 25.15 Экспорт и импорт криптографии за рубежом
- 25.16 Правовые вопросы

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