

ЮБИЛЕЙНЫЙ ВЫПУСК К 20-летию КНИГИ

ПРИКЛАДНАЯ КРИПТОГРАФИЯ



Протоколы, алгоритмы
и исходные коды на языке C

БРЮС ШНАЙЕР



WILEY

Оглавление

| | |
|----------------------------|----|
| Предисловие | 29 |
| Предисловие Уитфилда Диффи | 33 |
| Введение | 39 |
| Об авторе | 45 |
| Глава 1. Основные понятия | 47 |

Часть I

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ 71

| | |
|--|-----|
| Глава 2. Структурные элементы протоколов | 73 |
| Глава 3. Основные протоколы | 107 |
| Глава 4. Промежуточные протоколы | 143 |
| Глава 5. Усовершенствованные протоколы | 177 |
| Глава 6. Эзотерические протоколы | 209 |

Часть II

МЕТОДЫ КРИПТОГРАФИИ 241

| | |
|--|-----|
| Глава 7. Длина ключа | 243 |
| Глава 8. Управление ключами | 267 |
| Глава 9. Типы алгоритмов и криптографических режимов | 293 |
| Глава 10. Использование алгоритмов | 325 |

Часть III

КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ 347

| | |
|--|-----|
| Глава 11. Математические основы | 349 |
| Глава 12. Стандарт шифрования данных DES | 389 |
| Глава 13. Другие блочные шифры | 437 |
| Глава 14. Другие блочные шифры | 473 |
| Глава 15. Комбинирование блочных шифров | 505 |
| Глава 16. Генераторы псевдослучайных последовательностей и потоковые шифры | 521 |
| Глава 17. Другие потоковые шифры и генераторы истинно случайных последовательностей | 555 |
| Глава 18. Односторонние хеш-функции | 595 |

| | |
|--|-----|
| Глава 19. Алгоритмы с открытыми ключами | 633 |
| Глава 20. Алгоритмы цифровой подписи с открытым ключом | 663 |
| Глава 21. Схемы идентификации | 687 |
| Глава 22. Алгоритмы обмена ключами | 699 |
| Глава 23. Специальные алгоритмы для протоколов | 715 |

Часть IV
РЕАЛЬНЫЙ МИР 753

| | |
|--------------------------------|-----|
| Глава 24. Примеры реализаций | 755 |
| Глава 25. Политические вопросы | 801 |
| Послесловие Мэтта Блейза | 829 |

Часть V
ПРИЛОЖЕНИЕ 833

| | |
|----------------------|------|
| Исходные коды | 835 |
| Список литературы | 897 |
| Предметный указатель | 1021 |

Содержание

| | |
|---|----|
| Предисловие | 29 |
| Предисловие Уитфилда Диффи | 33 |
| Введение | 39 |
| Как читать эту книгу | 40 |
| Благодарности | 43 |
| Об авторе | 45 |
| Глава 1. Основные понятия | 47 |
| 1.1. Терминология | 47 |
| Отправитель и получатель | 47 |
| Сообщения и шифрование | 47 |
| Аутентификация, целостность и неотрицание авторства | 48 |
| Алгоритмы и ключи | 49 |
| Симметричные алгоритмы | 50 |
| Алгоритмы с открытым ключом | 51 |
| Криптоанализ | 52 |
| Безопасность алгоритмов | 56 |
| Исторические термины | 57 |
| 1.2. Стеганография | 58 |
| 1.3. Подстановочные и перестановочные шифры | 58 |
| Подстановочные шифры | 59 |
| Перестановочные шифры | 61 |
| Роторные машины | 62 |
| Для дальнейшего чтения | 63 |
| 1.4. Простая операция XOR | 63 |
| 1.5. Одноразовые блокноты | 65 |
| 1.6. Компьютерные алгоритмы | 68 |
| 1.7. Большие числа | 69 |

Часть I

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ 71

| | |
|--|----|
| Глава 2. Структурные элементы протоколов | 73 |
| 2.1. Введение в протоколы | 73 |
| Предназначение протоколов | 75 |
| Действующие лица | 75 |
| Протоколы с посредником | 76 |
| Арбитражные протоколы | 79 |
| Самодостаточные протоколы | 80 |
| Атаки на протоколы | 80 |

| | |
|--|------------|
| 2.2. Обмен сообщениями с помощью симметричной криптографии | 81 |
| 2.3. Односторонние функции | 83 |
| 2.4. Односторонние хеш-функции | 84 |
| Коды проверки подлинности сообщения | 86 |
| 2.5. Обмен сообщениями с помощью криптографии с открытым ключом | 86 |
| Гибридные криптосистемы | 88 |
| Головоломки Меркла | 90 |
| 2.6. Цифровые подписи | 91 |
| Подпись документа с помощью симметричных криптосистем и посредника | 92 |
| Деревья цифровых подписей | 94 |
| Подпись документа с помощью криптографии с открытым ключом | 94 |
| Подпись документа и метки времени | 95 |
| Подписание документов с помощью криптографии с открытым ключом и односторонних хеш-функций | 96 |
| Алгоритмы и терминология | 97 |
| Многократные подписи | 97 |
| Невозможность отказа от авторства и цифровые подписи | 98 |
| Применение цифровых подписей | 99 |
| 2.7. Цифровые подписи и шифрование | 99 |
| Возвращение полученного сообщения | 101 |
| Отражение атаки, основанной на повторной пересылке сообщений | 102 |
| Атаки криптосистем с открытыми ключами | 103 |
| 2.8. Генерация случайных и псевдослучайных последовательностей | 103 |
| Псевдослучайные последовательности | 104 |
| Криптографически стойкие псевдослучайные последовательности | 105 |
| Истинно случайные последовательности | 106 |
| Глава 3. Основные протоколы | 107 |
| 3.1. Обмен ключами | 107 |
| Обмен ключами с помощью симметричной криптографии | 107 |
| Обмен ключами с помощью криптографии с открытым ключом | 108 |
| Атака “человек посередине” | 108 |
| Протокол взаимоблокировки | 109 |
| Обмен ключами с помощью цифровых подписей | 110 |
| Одновременная передача ключей и сообщений | 111 |
| Широковещательная рассылка ключей и сообщений | 112 |

| | |
|--|------------|
| 3.2. Аутентификация | 113 |
| Аутентификация с помощью односторонних функций | 113 |
| Атака по словарю и “соль” | 113 |
| Программа SKEY | 114 |
| Аутентификация с помощью криптографии с открытым ключом | 115 |
| Взаимная аутентификация с помощью протокола взаимоблокировки | 116 |
| Протоколы SKID | 117 |
| Аутентификация сообщений | 118 |
| 3.3. Аутентификация и обмен ключами | 119 |
| Протокол Wide-Mouth Frog | 119 |
| Протокол Yahalom | 120 |
| Протокол Нидхем—Шредера | 121 |
| Протокол Отвей—Рииса | 123 |
| Протокол Kerberos | 123 |
| Протокол Ньюмана—Стаблбайна | 124 |
| Протокол DASS | 126 |
| Протокол Деннинга—Сакко | 127 |
| Протокол Ву—Лама | 128 |
| Другие протоколы | 129 |
| Выводы | 129 |
| 3.4. ФОРМАЛЬНЫЙ АНАЛИЗ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ И ОБМЕНА КЛЮЧАМИ | 130 |
| 3.5. КРИПТОГРАФИЯ С НЕСКОЛЬКИМИ ОТКРЫТЫМИ КЛЮЧАМИ | 134 |
| Широковещательная передача сообщения | 135 |
| 3.6. РАЗБИЕНИЕ СЕКРЕТА | 136 |
| 3.7. РАЗДЕЛЕНИЕ СЕКРЕТА | 138 |
| Разделение секрета с мошенниками | 139 |
| Разделение секрета без помощи Трента | 140 |
| Разделение секрета без раскрытия долей | 140 |
| Верифицированное разделение секрета | 140 |
| Схемы разделения секрета с предохранительными мерами | 141 |
| Разделение секрета с вычеркиванием из списка | 141 |
| 3.8. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА БАЗ ДАННЫХ | 141 |
| ГЛАВА 4. ПРОМЕЖУТОЧНЫЕ ПРОТОКОЛЫ | 143 |
| 4.1. СЛУЖБЫ МЕТОК ВРЕМЕНИ | 143 |
| Решение с посредником | 143 |
| Улучшенный протокол с посредником | 144 |
| Протокол связывания | 145 |
| Распределенный протокол | 146 |

| | |
|---|-----|
| Дальнейшая работа | 147 |
| 4.2. СКРЫТЫЙ КАНАЛ | 147 |
| Применения скрытого канала | 149 |
| Подписи, свободные от скрытого канала | 150 |
| 4.3. НЕОСПОРИМЫЕ ЦИФРОВЫЕ ПОДПИСИ | 150 |
| 4.4. ПОДПИСИ, ПОДТВЕРЖДАЕМЫЕ ДОВЕРЕННЫМИ ЛИЦАМИ | 152 |
| 4.5. ПОДПИСИ ПО ДОВЕРЕННОСТИ | 153 |
| 4.6. ГРУППОВЫЕ ПОДПИСИ | 154 |
| Групповые подписи с доверенным посредником | 155 |
| 4.7. ПОДПИСИ С ОБНАРУЖЕНИЕМ ПОДДЕЛКИ | 155 |
| 4.8. ВЫЧИСЛЕНИЯ НАД ЗАШИФРОВАННЫМИ ДАННЫМИ | 157 |
| 4.9. ПЕРЕДАЧА БИТОВ | 157 |
| Передача битов с помощью симметричной криптографии | 158 |
| Передача бита с помощью односторонних функций | 159 |
| Передача бита с помощью генератора псевдослучайной последовательности | 159 |
| Двоичные объекты | 160 |
| 4.10. ЖЕРЕБЬЕВКА С ПОМОЩЬЮ ИДЕАЛЬНОЙ МОНЕТЫ | 161 |
| Жеребьевка с помощью односторонних функций | 162 |
| Жеребьевка с помощью криптографии с открытым ключом | 162 |
| Бросок монеты в колодез | 164 |
| Генерация ключей с помощью жеребьевки | 164 |
| 4.11. МЫСЛЕННЫЙ ПОКЕР | 164 |
| Мысленный покер с тремя игроками | 165 |
| Атаки на протоколы мысленного покера | 167 |
| Анонимное распределение ключей | 167 |
| 4.12. ОДНОСТОРОННИЕ СУММАТОРЫ | 169 |
| 4.13. РАСКРЫТИЕ СЕКРЕТОВ ПО ПРИНЦИПУ “ВСЕ ИЛИ НИЧЕГО” | 170 |
| 4.14. ДЕПОНИРОВАНИЕ КЛЮЧЕЙ | 171 |
| Стратегии депонирования | 173 |
| Глава 5. Усовершенствованные протоколы | 177 |
| 5.1. ДОКАЗАТЕЛЬСТВА С НУЛЕВЫМ ЗНАНИЕМ | 177 |
| Базовый протокол с нулевым разглашением | 178 |
| Изоморфизм графа | 181 |
| Гамильтоновы циклы | 182 |
| Параллельные доказательства с нулевым разглашением | 183 |
| Неинтерактивные доказательства с нулевым разглашением | 184 |

| | |
|---|-----|
| Общие замечания | 186 |
| 5.2. ИСПОЛЬЗОВАНИЕ ДОКАЗАТЕЛЬСТВА С НУЛЕВЫМ РАЗГЛАШЕНИЕМ для идентификации | 187 |
| Проблема гроттмейстера | 188 |
| Мошенничество мафии | 188 |
| Обман, осуществленный террористами | 189 |
| Предлагаемые решения | 189 |
| Обман с несколькими лицами | 190 |
| Прокат паспортов | 190 |
| Доказательство членства | 191 |
| 5.3. Слепые подписи | 191 |
| Полностью слепые подписи | 191 |
| Слепые подписи | 192 |
| Патенты | 195 |
| 5.4. Личностная криптография с открытым ключом | 195 |
| 5.5. Забычивая передача | 196 |
| 5.6. Забычивые подписи | 198 |
| 5.7. Одновременное подписание контракта | 199 |
| Подпись контракта с помощью посредника | 199 |
| Одновременная подпись контракта без посредника (при личной встрече) | 200 |
| Одновременная подпись контракта без посредника (без личной встречи) | 200 |
| Одновременная подпись контракта без посредника (с помощью криптографии) | 202 |
| 5.8. Заказная электронная почта | 204 |
| 5.9. Одновременный обмен секретами | 207 |
| Глава 6. Эзотерические протоколы | 209 |
| 6.1. Тайное голосование | 209 |
| Упрощенный протокол голосования №1 | 209 |
| Упрощенный протокол голосования №2 | 210 |
| Голосование со слепыми подписями | 210 |
| Голосование с двумя центральными комиссиями | 212 |
| Голосование с одной центральной комиссией | 213 |
| Улучшенное голосование с одной центральной комиссией | 214 |
| Голосование без центральной избирательной комиссии | 216 |
| Другие схемы голосования | 220 |
| 6.2. Секретные многосторонние вычисления | 221 |
| Протокол №1 | 221 |
| Протокол №2 | 222 |

| | |
|---|-----|
| Протокол №3 | 223 |
| Протокол №4 | 224 |
| Безусловно тайные многосторонние протоколы | 225 |
| Тайное вычисление схемы | 225 |
| 6.3. ШИРОКОВЕЩАТЕЛЬНАЯ ПЕРЕДАЧА АНОНИМНЫХ СООБЩЕНИЙ | 225 |
| 6.4. ЭЛЕКТРОННЫЕ ДЕНЬГИ | 228 |
| Протокол №1 | 229 |
| Протокол №2 | 230 |
| Протокол №3 | 231 |
| Протокол №4 | 232 |
| Электронные деньги и идеальное преступление | 236 |
| Реальные электронные наличные | 236 |
| Другие протоколы электронных денег | 236 |
| Анонимные кредитные карточки | 238 |

Часть II

МЕТОДЫ КРИПТОГРАФИИ 241

| | |
|---|------------|
| Глава 7. Длина ключа | 243 |
| 7.1. Длина симметричного ключа | 243 |
| Оценка продолжительности и стоимости лобовой атаки | 244 |
| Программы для взлома | 247 |
| Нейронные сети | 248 |
| Вирусы | 248 |
| Китайская лотерея | 249 |
| Биотехнология | 250 |
| Термодинамические ограничения | 251 |
| 7.2. Длина открытого ключа | 252 |
| Вычисление с помощью ДНК | 259 |
| Квантовые вычисления | 261 |
| 7.3. Сравнение длин симметричных и открытых ключей | 262 |
| 7.4. АТАКА НА ОСНОВЕ ПАРАДОКСА ДНЕЙ РОЖДЕНИЯ И ОДНОСТОРОННИЕ ХЕШ-ФУНКЦИИ | 263 |
| 7.5. КАКОЙ ДОЛЖНА БЫТЬ ДЛИНА КЛЮЧА? | 263 |
| 7.6. ПРЕДОСТЕРЕЖЕНИЕ | 265 |
| Глава 8. УПРАВЛЕНИЕ КЛЮЧАМИ | 267 |
| 8.1. Генерация ключей | 268 |
| Уменьшенные пространства ключей | 268 |
| Неправильный выбор ключей | 270 |
| Случайные ключи | 272 |

| | |
|---|------------|
| Ключевые фразы | 273 |
| Стандарт генерации ключей X9.17 | 274 |
| Генерация ключей в Министерстве обороны США | 275 |
| 8.2. НЕЛИНЕЙНЫЕ ПРОСТРАНСТВА КЛЮЧЕЙ | 275 |
| 8.3. ПЕРЕСЫЛКА КЛЮЧЕЙ | 276 |
| Распределение ключей в крупных сетях | 278 |
| 8.4. ПРОВЕРКА КЛЮЧЕЙ | 278 |
| Обнаружение ошибок при пересылке ключей | 280 |
| Обнаружение ошибок при расшифровке | 280 |
| 8.5. ИСПОЛЬЗОВАНИЕ КЛЮЧЕЙ | 281 |
| Контроль использования ключей | 282 |
| 8.6. ОБНОВЛЕНИЕ КЛЮЧЕЙ | 282 |
| 8.7. ХРАНЕНИЕ КЛЮЧЕЙ | 283 |
| 8.8. РЕЗЕРВНЫЕ КЛЮЧИ | 284 |
| 8.9. СКОМПРОМЕТИРОВАННЫЕ КЛЮЧИ | 285 |
| 8.10. СРОК ДЕЙСТВИЯ КЛЮЧЕЙ | 286 |
| 8.11. РАЗРУШЕНИЕ КЛЮЧЕЙ | 288 |
| 8.12. УПРАВЛЕНИЕ КЛЮЧАМИ В СИСТЕМАХ С ОТКРЫТЫМ КЛЮЧОМ | 289 |
| Сертификаты открытых ключей | 290 |
| Распределенное управление ключами | 291 |
| ГЛАВА 9. ТИПЫ АЛГОРИТМОВ И КРИПТОГРАФИЧЕСКИХ РЕЖИМОВ | 293 |
| 9.1. РЕЖИМ ЭЛЕКТРОННОЙ КОДОВОЙ КНИГИ | 294 |
| Заполнение блоков | 295 |
| 9.2. ПОВТОР БЛОКА | 296 |
| 9.3. РЕЖИМ СЦЕПЛЕНИЯ БЛОКОВ ШИФРОТЕКСТА | 298 |
| Вектор инициализации | 299 |
| Дополнение | 300 |
| Распространение ошибки | 302 |
| Вопросы безопасности | 302 |
| 9.4. ПОТОКОВЫЕ ШИФРЫ | 303 |
| 9.5. САМОСИНХРОНИЗИРУЮЩИЕСЯ ПОТОКОВЫЕ ШИФРЫ | 305 |
| Вопросы безопасности | 306 |
| 9.6. РЕЖИМ ГАММИРОВАНИЯ С ОБРАТНОЙ СВЯЗЬЮ | 306 |
| Вектор инициализации | 308 |
| Распространение ошибки | 309 |
| 9.7. СИНХРОННЫЕ ПОТОКОВЫЕ ШИФРЫ | 309 |
| Атака вставкой | 311 |
| 9.8. РЕЖИМ ОБРАТНОЙ СВЯЗИ ПО ВЫХОДУ | 311 |
| Вектор инициализации | 312 |

| | |
|---|------------|
| Распространение ошибки | 312 |
| Режим OFB и проблемы безопасности | 313 |
| Потоковые шифры в режиме OFB | 313 |
| 9.9. РЕЖИМ СЧЕТЧИКА | 314 |
| Потоковые шифры в режиме счетчика | 314 |
| 9.10. ДРУГИЕ РЕЖИМЫ БЛОЧНЫХ ШИФРОВ | 315 |
| Режим сцепления блоков | 315 |
| Режим сцепления блоков шифра с распространением ошибки | 316 |
| Сцепление блоков шифротекста с контрольной суммой | 317 |
| Нелинейная обратная связь по выходу | 317 |
| Прочие режимы | 317 |
| 9.11. ВЫБОР РЕЖИМА ШИФРОВАНИЯ | 318 |
| 9.12. ЧЕРЕДОВАНИЕ | 321 |
| 9.13. СРАВНЕНИЕ БЛОЧНЫХ И ПОТОКОВЫХ ШИФРОВ | 322 |
| ГЛАВА 10. ИСПОЛЬЗОВАНИЕ АЛГОРИТМОВ | 325 |
| 10.1. ВЫБОР АЛГОРИТМА | 326 |
| Экспорт алгоритмов | 328 |
| 10.2. СРАВНЕНИЕ КРИПТОГРАФИИ С ОТКРЫТЫМ КЛЮЧОМ И СИММЕТРИЧНОЙ КРИПТОГРАФИИ | 328 |
| 10.3. ШИФРОВАНИЕ КАНАЛОВ СВЯЗИ | 330 |
| Канальное шифрование | 330 |
| Сквозное шифрование | 332 |
| Объединение двух подходов | 333 |
| 10.4. ШИФРОВАНИЕ ДАННЫХ ДЛЯ ХРАНЕНИЯ | 335 |
| Разыменование ключей | 336 |
| Шифрование на файловом уровне и на уровне драйверов | 336 |
| Обеспечение произвольного доступа к зашифрованному диску | 338 |
| 10.5. СРАВНЕНИЕ АППАРАТНОГО И ПРОГРАММНОГО СПОСОБОВ ШИФРОВАНИЯ | 339 |
| Аппаратное шифрование | 339 |
| Программное шифрование | 341 |
| 10.6. СЖАТИЕ, КОДИРОВАНИЕ И ШИФРОВАНИЕ | 342 |
| 10.7. ОБНАРУЖЕНИЕ ЗАШИФРОВАННЫХ ДАННЫХ | 342 |
| 10.8. СОКРЫТИЕ ШИФРОТЕКСТА В ШИФРОТЕКСТЕ | 343 |
| 10.9. РАЗРУШЕНИЕ ИНФОРМАЦИИ | 345 |

Часть III

КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ 347

| | |
|--|------------|
| Глава 11. МАТЕМАТИЧЕСКИЕ ОСНОВЫ | 349 |
| 11.1. ТЕОРИЯ ИНФОРМАЦИИ | 349 |
| Энтропия и неопределенность | 349 |
| Энтропия языка | 350 |
| Стойкость криптосистем | 351 |
| Расстояние единственности | 352 |
| Практическое использование теории информации | 354 |
| Перемешивание и рассеивание | 354 |
| 11.2. ТЕОРИЯ СЛОЖНОСТИ | 355 |
| Сложность алгоритмов | 355 |
| Сложность задач | 357 |
| NP-полные задачи | 360 |
| 11.3. ТЕОРИЯ ЧИСЕЛ | 361 |
| Модулярная арифметика | 361 |
| Простые числа | 364 |
| Наибольший общий делитель | 365 |
| Обратные значения по модулю | 366 |
| Вычисление коэффициентов | 368 |
| Малая теорема Ферма | 368 |
| Функция Эйлера | 369 |
| Китайская теорема об остатках | 370 |
| Квадратичные вычеты | 371 |
| Символ Лежандра | 372 |
| Символ Якоби | 373 |
| Целые числа Блюма | 374 |
| Образующие | 375 |
| Вычисление в поле Галуа | 376 |
| 11.4. ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ | 378 |
| Квадратные корни по модулю n | 381 |
| 11.5. ГЕНЕРАЦИЯ ПРОСТЫХ ЧИСЕЛ | 381 |
| Тест Соловея—Штрассена | 382 |
| Тест Леманна | 383 |
| Тест Рабина—Миллера | 383 |
| Практические соображения | 384 |
| Сильные простые числа | 385 |
| 11.6. ДИСКРЕТНЫЕ ЛОГАРИФМЫ В КОНЕЧНОМ ПОЛЕ | 386 |
| Вычисление дискретных логарифмов в конечной группе | 386 |

| | |
|---|------------|
| ГЛАВА 12. СТАНДАРТ ШИФРОВАНИЯ ДАННЫХ DES | 389 |
| 12.1. Основы | 389 |
| Разработка стандарта | 389 |
| Принятие стандарта | 392 |
| Аттестация и сертификация оборудования DES | 393 |
| События 1987 года | 394 |
| События 1993 года | 395 |
| 12.2. ОПИСАНИЕ СТАНДАРТА DES | 396 |
| Схема алгоритма | 396 |
| Начальная перестановка | 398 |
| Преобразования ключа | 399 |
| Расширяющая перестановка | 400 |
| Подстановка с помощью S-блоков | 401 |
| Перестановка с помощью P-блоков | 404 |
| Заключительная перестановка | 404 |
| Расшифровка в алгоритме DES | 405 |
| Режимы алгоритма DES | 405 |
| Аппаратные и программные реализации DES | 405 |
| 12.3. СТОЙКОСТЬ АЛГОРИТМА DES | 407 |
| Слабые ключи | 408 |
| Комплементарные ключи | 411 |
| Алгебраическая структура | 411 |
| Длина ключа | 412 |
| Количество раундов | 413 |
| Проектирование S-блоков | 414 |
| Дополнительные результаты | 415 |
| 12.4. ДИФФЕРЕНЦИАЛЬНЫЙ И ЛИНЕЙНЫЙ КРИПТОАНАЛИЗ | 415 |
| Дифференциальный криптоанализ | 415 |
| Криптоанализ на основе связанных ключей | 421 |
| Линейный криптоанализ | 422 |
| Дальнейшие направления | 425 |
| 12.5. ПРАКТИЧЕСКИЕ КРИТЕРИИ ПРОЕКТИРОВАНИЯ | 426 |
| 12.6. ВАРИАНТЫ АЛГОРИТМА DES | 427 |
| Множественный алгоритм DES | 427 |
| Алгоритм DES с независимыми подключками | 427 |
| Алгоритм DESX | 428 |
| Алгоритм CRYPT(3) | 428 |
| Обобщенный алгоритм DES | 428 |
| Алгоритм DES с измененными S-блоками | 430 |
| Алгоритм RDES | 430 |

| | |
|---|-----|
| Алгоритм s^n DES | 431 |
| Алгоритм DES с S-блоками, зависящими от ключа | 432 |
| 12.7. Насколько стоек алгоритм DES в настоящее время? | 434 |
| Глава 13. Другие блочные шифры | 437 |
| 13.1. Алгоритм LUCIFER | 437 |
| 13.2. Алгоритм MADRYGA | 438 |
| Описание алгоритма Madryga | 439 |
| Криптоанализ алгоритма Madryga | 441 |
| 13.3. Алгоритм NewDES | 441 |
| 13.4. Алгоритм FEAL | 443 |
| Описание алгоритма FEAL | 443 |
| Криптоанализ алгоритма FEAL | 446 |
| Патенты | 448 |
| 13.5. Алгоритм REDOC | 448 |
| Алгоритм REDOC III | 449 |
| Патенты и лицензии | 450 |
| 13.6. Алгоритм LOKI | 450 |
| Алгоритм LOKI91 | 451 |
| Описание алгоритма LOKI91 | 451 |
| Криптоанализ алгоритма LOKI91 | 453 |
| Патенты и лицензии | 453 |
| 13.7. Алгоритмы KHUFU и KHAFRE | 454 |
| Алгоритм Khufu | 455 |
| Алгоритм Khafre | 455 |
| Патенты | 456 |
| 13.8. Алгоритм RC2 | 456 |
| 13.9. Алгоритм IDEA | 458 |
| Обзор алгоритма IDEA | 459 |
| Описание алгоритма IDEA | 459 |
| Скорость IDEA | 462 |
| Криптоанализ алгоритма IDEA | 462 |
| Режимы работы и варианты IDEA | 465 |
| Предостережение | 466 |
| Патенты и лицензии | 466 |
| 13.10. Алгоритм MMB | 466 |
| Безопасность алгоритма MMB | 468 |
| 13.11. Алгоритм CA-1.1 | 468 |
| 13.12. Алгоритм SKIPJACK | 469 |

| | |
|---|------------|
| Глава 14. Другие блочные шифры | 473 |
| 14.1. Алгоритм ГОСТ | 473 |
| Описание алгоритма ГОСТ | 473 |
| Криптоанализ алгоритма ГОСТ | 476 |
| 14.2. Алгоритм CAST | 477 |
| 14.3. Алгоритм BLOWFISH | 479 |
| Описание алгоритма Blowfish | 479 |
| Стойкость алгоритма Blowfish | 482 |
| 14.4. Алгоритм SAFER | 483 |
| Описание алгоритма SAFER K-64 | 483 |
| Алгоритм SAFER K-128 | 485 |
| Стойкость алгоритма SAFER K-64 | 485 |
| 14.5. Алгоритм 3-Way | 486 |
| Описание алгоритма 3-Way | 486 |
| 14.6. Алгоритм CRAB | 487 |
| 14.7. Алгоритм SXAL8/MBAL | 489 |
| 14.8. Алгоритм RC5 | 489 |
| 14.9. Другие блочные алгоритмы | 491 |
| 14.10. ТЕОРИЯ ПРОЕКТИРОВАНИЯ БЛОЧНЫХ ШИФРОВ | 492 |
| Сети Фейстеля | 493 |
| Простые соотношения | 493 |
| Групповая структура | 494 |
| Слабые ключи | 494 |
| Устойчивость к дифференциальному и линейному криптоанализу | 495 |
| Проектирование S-блоков | 495 |
| Проектирование блочного шифра | 498 |
| 14.11. ИСПОЛЬЗОВАНИЕ ОДНОСТОРОННИХ ХЕШ-ФУНКЦИЙ | 499 |
| Алгоритм Карна | 499 |
| Алгоритм Любы–Ракоффа | 500 |
| Шифр MDC | 501 |
| Безопасность шифров, основанных на односторонних хеш-функциях | 502 |
| 14.12. ВЫБОР БЛОЧНОГО АЛГОРИТМА | 503 |
| Глава 15. КОМБИНИРОВАНИЕ БЛОЧНЫХ ШИФРОВ | 505 |
| 15.1. ДВОЙНОЕ ШИФРОВАНИЕ | 505 |
| 15.2. ТРОЙНОЕ ШИФРОВАНИЕ | 507 |
| Тройное шифрование с двумя ключами | 507 |
| Тройное шифрование с тремя ключами | 509 |
| Тройное шифрование с минимальным ключом (ТЕМК) | 509 |

| | |
|---|------------|
| Режимы тройного шифрования | 509 |
| Варианты тройного шифрования | 511 |
| 15.3. Удвоение длины блока | 513 |
| 15.4. ДРУГИЕ СХЕМЫ МНОГОКРАТНОГО ШИФРОВАНИЯ | 513 |
| Двойной OFB/счетчик | 514 |
| Метод ECB + OFB | 514 |
| Схема xDES ⁱ | 515 |
| Пятикратное шифрование | 517 |
| 15.5. УМЕНЬШЕНИЕ ДЛИНЫ КЛЮЧА В АЛГОРИТМЕ CDMF | 517 |
| 15.6. ОТБЕЛИВАНИЕ | 517 |
| 15.7. КАСКАДНОЕ ПРИМЕНЕНИЕ БЛОЧНЫХ АЛГОРИТМОВ | 518 |
| 15.8. КОМБИНАЦИЯ НЕСКОЛЬКИХ БЛОЧНЫХ АЛГОРИТМОВ | 519 |
| ГЛАВА 16. ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ И ПОТОКОВЫЕ ШИФРЫ | 521 |
| 16.1. ЛИНЕЙНЫЕ КОНГРУЭНТНЫЕ ГЕНЕРАТОРЫ | 521 |
| Комбинирование линейных конгруэнтных генераторов | 523 |
| 16.2. РЕГИСТРЫ СДВИГА С ЛИНЕЙНОЙ ОБРАТНОЙ СВЯЗЬЮ | 526 |
| Программные реализации регистров LFSR | 532 |
| 16.3. ПРОЕКТИРОВАНИЕ И АНАЛИЗ ПОТОКОВЫХ ШИФРОВ | 534 |
| Линейная сложность | 534 |
| Корреляционная стойкость | 535 |
| Другие атаки | 536 |
| 16.4. ПОТОКОВЫЕ ШИФРЫ НА ОСНОВЕ РЕГИСТРОВ LFSR | 536 |
| Генератор Геффе | 537 |
| Обобщенный генератор Геффе | 538 |
| Генератор Дженнингса | 538 |
| Генератор “старт–стоп” Бета–Пайпера | 539 |
| Чередующийся генератор “старт–стоп” | 540 |
| Двусторонний генератор “старт–стоп” | 541 |
| Пороговый генератор | 541 |
| Самопрореживающие генераторы | 542 |
| Многоскоростной генератор скалярного произведения | 542 |
| Суммирующий генератор | 544 |
| Генератор DNRSG | 544 |
| Каскад Голлманна | 544 |
| Сжимающий генератор | 545 |
| Самосжимающий генератор | 545 |
| 16.5. ШИФР A5 | 546 |
| 16.6. АЛГОРИТМ HUGHES XPD/KPD | 547 |

| | |
|--|------------|
| 16.7. АЛГОРИТМ NANOTEQ | 548 |
| 16.8. АЛГОРИТМ RAMBUTAN | 548 |
| 16.9. АДДИТИВНЫЕ ГЕНЕРАТОРЫ | 549 |
| Генератор Fish | 549 |
| Алгоритм Pike | 550 |
| Алгоритм Mush | 550 |
| 16.10. АЛГОРИТМ ДЖИФФОРДА | 551 |
| 16.11. АЛГОРИТМ M | 552 |
| 16.12. АЛГОРИТМ PKZIP | 553 |
| Надежность алгоритма PKZIP | 554 |
| Глава 17. ДРУГИЕ ПОТОКОВЫЕ ШИФРЫ И ГЕНЕРАТОРЫ ИСТИННО СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ | 555 |
| 17.1. АЛГОРИТМ RC4 | 555 |
| 17.2. АЛГОРИТМ SEAL | 557 |
| Семейство псевдослучайных функций | 557 |
| Описание алгоритма SEAL | 558 |
| Надежность алгоритма SEAL | 559 |
| Патенты и лицензии | 560 |
| 17.3. АЛГОРИТМ WAKE | 560 |
| 17.4. РЕГИСТРЫ СДВИГА С ОБРАТНОЙ СВЯЗЬЮ ПО ПЕРЕНОСУ | 561 |
| 17.5. ПОТОКОВЫЕ ШИФРЫ НА ОСНОВЕ РЕГИСТРОВ FCSR | 570 |
| Каскадные генераторы | 570 |
| Комбинированные генераторы FCSR | 570 |
| Каскад LFSR/FCSR с суммированием/четностью | 571 |
| Чередующиеся генераторы “старт–стоп” | 572 |
| Сжимающие генераторы | 573 |
| 17.6. РЕГИСТРЫ СДВИГА С НЕЛИНЕЙНОЙ ОБРАТНОЙ СВЯЗЬЮ | 573 |
| 17.7. ДРУГИЕ ПОТОКОВЫЕ ШИФРЫ | 575 |
| Генератор Плесса | 575 |
| Генератор на основе клеточного автомата | 576 |
| Генератор 1/p | 576 |
| Алгоритм crypt(1) | 576 |
| Другие схемы | 577 |
| 17.8. ПРОЕКТИРОВАНИЕ ПОТОКОВЫХ ШИФРОВ НА ОСНОВЕ ТЕОРИИ СИСТЕМ | 577 |
| 17.9. ПРОЕКТИРОВАНИЕ ПОТОКОВЫХ ШИФРОВ НА ОСНОВЕ ТЕОРИИ СЛОЖНОСТИ | 579 |
| Генератор псевдослучайных чисел Шамира | 579 |
| Генератор Блюма–Микали | 579 |

| | |
|--|------------|
| Генератор RSA | 579 |
| Генератор Блюма—Блюма—Шуба | 580 |
| 17.10. Другие подходы к проектированию потоковых шифров | 581 |
| Шифр “Рип ван Винкль” | 582 |
| Рандомизированный потоковый шифр Диффи | 582 |
| Рандомизированный потоковый шифр Маурера | 583 |
| 17.11. Каскад из нескольких потоковых шифров | 583 |
| 17.12. Выбор потокового шифра | 584 |
| 17.13. Генерирование нескольких потоков с помощью одного генератора псевдослучайных последовательностей | 584 |
| 17.14. Генераторы истинно случайных последовательностей | 586 |
| Таблицы случайных чисел | 586 |
| Использование случайного шума | 587 |
| Использование таймера компьютера | 589 |
| Измерение задержек клавиатуры | 590 |
| Смещения и корреляции | 590 |
| Извлеченная случайность | 591 |
| Глава 18. Односторонние хеш-функции | 595 |
| 18.1. Основы | 595 |
| Длины односторонних хеш-функций | 596 |
| Обзор односторонних хеш-функций | 597 |
| 18.2. Алгоритм SNEFRU | 598 |
| Криптоанализ алгоритма Snefru | 599 |
| 18.3. Алгоритм N-хеш | 599 |
| Криптоанализ алгоритма N-хеш | 602 |
| 18.4. Алгоритм MD4 | 602 |
| 18.5. Алгоритм MD5 | 603 |
| Описание алгоритма MD5 | 603 |
| Стойкость MD5 | 608 |
| 18.6. Алгоритм MD2 | 608 |
| 18.7. Алгоритм SHA | 609 |
| Описание алгоритма SHA | 610 |
| Стойкость алгоритма SHA | 613 |
| 18.8. Алгоритм RIPE-MD | 614 |
| 18.9. Алгоритм HAVAL | 614 |
| 18.10. Другие односторонние хеш-функции | 615 |
| 18.11. Односторонние хеш-функции на основе симметричных блочных алгоритмов | 616 |
| Схемы, в которых длина хеш-значения равна длине блока | 617 |

| | |
|---|------------|
| Модификация схемы Дэвиса—Майера | 619 |
| Схема Пренеля—Босселаерса—Говарца—Вандевалле | 620 |
| Алгоритм Кискатера—Жиро | 620 |
| Алгоритм LOKI с удвоенным блоком | 621 |
| Параллельная схема Дэвиса—Майера | 621 |
| Тандемная и синхронная схемы Дэвиса—Майера | 621 |
| Алгоритмы MDC-2 и MDC-4 | 623 |
| Хеш-функция AR | 624 |
| Хеш-функция ГОСТ | 625 |
| Другие схемы | 625 |
| 18.12. ИСПОЛЬЗОВАНИЕ АЛГОРИТМОВ С ОТКРЫТЫМ КЛЮЧОМ | 626 |
| 18.13. ВЫБОР ОДНОСТОРОННЕЙ ХЕШ-ФУНКЦИИ | 626 |
| 18.14. КОДЫ АУТЕНТИФИКАЦИИ СООБЩЕНИЙ | 627 |
| Алгоритм CBC-MAC | 628 |
| Алгоритм МАА | 628 |
| Двунаправленный алгоритм MAC | 628 |
| Методы Джунемана | 629 |
| Алгоритм RIPE-MAC | 629 |
| Алгоритм IBC-хеш | 630 |
| Односторонняя хеш-функция MAC | 630 |
| Алгоритм MAC с использованием потокового шифра | 631 |
| Глава 19. АЛГОРИТМЫ С ОТКРЫТЫМИ КЛЮЧАМИ | 633 |
| 19.1. Основы | 633 |
| Стойкость алгоритмов с открытым ключом | 634 |
| 19.2. АЛГОРИТМЫ НА ОСНОВЕ ЗАДАЧИ ОБ УКЛАДКЕ РАНЦА | 634 |
| Сверхвозрастающие ранцы | 636 |
| Создание открытого ключа из закрытого | 637 |
| Шифрование | 637 |
| Расшифровка | 638 |
| Практические реализации | 638 |
| Стойкость ранцевого метода | 638 |
| Варианты ранцевых алгоритмов | 639 |
| Патенты | 639 |
| 19.3. АЛГОРИТМ RSA | 640 |
| Аппаратные реализации RSA | 643 |
| Скорость работы RSA | 644 |
| Программные ускорители | 644 |
| Стойкость алгоритма RSA | 645 |
| Атака с подобранным шифротекстом на RSA | 646 |
| Атака на RSA с использованием общего модуля RSA | 647 |

| | |
|---|------------|
| Атака на RSA с использованием малого показателя шифрования | 648 |
| Атака на RSA с использованием малого показателя расшифровки | 648 |
| Выводы | 649 |
| Атака на шифрование и цифровую подпись с использованием алгоритма RSA | 649 |
| Стандарты | 650 |
| Патенты | 650 |
| 19.4. СХЕМА ПОЛИГА—ХЕЛЛМАНА | 650 |
| Патенты | 651 |
| 19.5. СХЕМА РАБИНА | 651 |
| Схема Уильямса | 652 |
| 19.6. СХЕМА ЭЛЬ-ГАМАЛЯ | 653 |
| Подписи по схеме Эль-Гамала | 653 |
| Шифрование по схеме Эль-Гамала | 655 |
| Быстродействие | 656 |
| Патенты | 656 |
| 19.7. СХЕМА МАКЭЛИСА | 656 |
| Другие алгоритмы, основанные на линейных кодах, исправляющих ошибки | 657 |
| 19.8. КРИПТОСИСТЕМЫ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ | 658 |
| 19.9. КРИПТОСИСТЕМА LUC | 659 |
| 19.10. КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ НА ОСНОВЕ КОНЕЧНЫХ АВТОМАТОВ | 660 |
| ГЛАВА 20. АЛГОРИТМЫ ЦИФРОВОЙ ПОДПИСИ С ОТКРЫТЫМ КЛЮЧОМ | 663 |
| 20.1. АЛГОРИТМ ЦИФРОВОЙ ПОДПИСИ DSA | 663 |
| Реакция на заявление | 664 |
| Описание DSA | 667 |
| Ускоряющие предварительные вычисления | 669 |
| Генерация простых чисел DSA | 670 |
| Шифрование по схеме Эль-Гамала с алгоритмом DSA | 671 |
| Шифрование по алгоритму RSA с помощью алгоритма DSA | 672 |
| Стойкость алгоритма DSA | 673 |
| Атаки, направленные на параметр k | 674 |
| Опасности общего модуля | 674 |
| Скрытый канал в алгоритме DSA | 675 |
| Патенты | 675 |
| 20.2. ВАРИАНТЫ АЛГОРИТМА DSA | 676 |
| 20.3. АЛГОРИТМ ЦИФРОВОЙ ПОДПИСИ ГОСТ | 678 |
| 20.4. СХЕМЫ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ДИСКРЕТНЫХ ЛОГАРИФМОВ | 679 |

| | |
|--|------------|
| 20.5. СХЕМА ОНГА—ШНОРРА—ШАМИРА | 681 |
| 20.6. СХЕМА ESIGN | 682 |
| Стойкость схемы ESIGN | 683 |
| Патенты | 684 |
| 20.7. КЛЕТОЧНЫЕ АВТОМАТЫ | 684 |
| 20.8. ДРУГИЕ АЛГОРИТМЫ С ОТКРЫТЫМ КЛЮЧОМ | 684 |
| Глава 21. СХЕМЫ ИДЕНТИФИКАЦИИ | 687 |
| 21.1. СХЕМА ФЕЙГЕ—ФИАТА—ШАМИРА | 687 |
| Упрощенная схема идентификации Фейге—Фиата—Шамира | 687 |
| Схема идентификации Фейге—Фиата—Шамира | 689 |
| Пример | 689 |
| Улучшения протокола | 691 |
| Схема подписи Фиата—Шамира | 691 |
| Улучшенная схема подписи Фиата—Шамира | 693 |
| Другие улучшения | 693 |
| Схема идентификации Ота—Окамото | 693 |
| Патенты | 693 |
| 21.2. СХЕМА ГИЛЛУ—КИСКАТЕ | 693 |
| Схема идентификации Гиллу—Кискате | 694 |
| Схема подписи Гиллу—Кискате | 695 |
| Несколько подписей | 695 |
| 21.3. СХЕМА ШНОРРА | 696 |
| Протокол проверки подлинности | 696 |
| Протокол цифровой подписи | 697 |
| Патенты | 698 |
| 21.4. ПРЕОБРАЗОВАНИЕ СХЕМ ИДЕНТИФИКАЦИИ в СХЕМЫ ПОДПИСИ | 698 |
| Глава 22. АЛГОРИТМЫ ОБМЕНА КЛЮЧАМИ | 699 |
| 22.1. АЛГОРИТМ ДИФФИ—ХЕЛЛМАНА | 699 |
| Алгоритм Диффи—Хеллмана с тремя и более участниками | 700 |
| Расширенный алгоритм Диффи—Хеллмана | 701 |
| Алгоритм Хьюза | 701 |
| Обмен ключом без предварительного обмена данными | 702 |
| Патенты | 702 |
| 22.2. ПРОТОКОЛ “СТАНЦИЯ—СТАНЦИЯ” | 702 |
| 22.3. ТРЕХПРОХОДНЫЙ ПРОТОКОЛ ШАМИРА | 703 |
| 22.4. ПРОТОКОЛ COMSET | 705 |
| 22.5. ПРОТОКОЛ ОБМЕНА ЗАШИФРОВАННЫМИ КЛЮЧАМИ | 705 |
| Базовый протокол ЕКЕ | 705 |

| | |
|---|-----|
| Реализация протокола ЕКЕ с помощью алгоритма RSA | 706 |
| Реализация протокола ЕКЕ с помощью схемы Эль-Гамала | 707 |
| Реализация протокола ЕКЕ с помощью алгоритма Диффи–Хеллмана | 707 |
| Усовершенствование протокола ЕКЕ | 708 |
| Расширенный протокол ЕКЕ | 708 |
| Применение протокола ЕКЕ | 709 |
| 22.6. ЗАЩИЩЕННЫЕ ПЕРЕГОВОРЫ О СОГЛАСОВАНИИ КЛЮЧА | 710 |
| 22.7. РАСПРЕДЕЛЕНИЕ КЛЮЧА ДЛЯ КОНФЕРЕНЦ-СВЯЗИ И СЕКРЕТНОЙ широковещательной передачи | 711 |
| Распределение ключей для конференции | 713 |
| Протокол Татебаяши–Мацузаки–Ньюмена | 713 |
| Глава 23. СПЕЦИАЛЬНЫЕ АЛГОРИТМЫ ДЛЯ ПРОТОКОЛОВ | 715 |
| 23.1. Криптография с несколькими открытыми ключами | 715 |
| 23.2. АЛГОРИТМЫ РАЗДЕЛЕНИЯ СЕКРЕТА | 716 |
| Схема интерполяционных многочленов Лагранжа | 716 |
| Векторная схема | 717 |
| Схема Асмута–Блума | 718 |
| Схема Карнина–Грини–Хеллмана | 718 |
| Более сложные пороговые схемы | 718 |
| Разделение секрета с мошенниками | 719 |
| 23.3. СКРЫТЫЙ КАНАЛ | 720 |
| Скрытый канал на основе схемы Онга–Шнорра–Шамира | 720 |
| Скрытый канал на основе схемы Эль-Гамала | 721 |
| Скрытый канал на основе схемы ESIGN | 722 |
| Скрытый канал на основе схемы DSA | 724 |
| Уничтожение скрытого канала в схеме DSA | 726 |
| Другие схемы | 727 |
| 23.4. НЕОСПОРИМЫЕ ЦИФРОВЫЕ ПОДПИСИ | 727 |
| Преобразуемые неоспоримые подписи | 729 |
| 23.5. Подписи, подтверждаемые доверенным лицом | 730 |
| 23.6. Вычисления с зашифрованными данными | 732 |
| Задача дискретного логарифмирования | 732 |
| 23.7. ЖЕРЕБЬЕВКА С ПОМОЩЬЮ ИДЕАЛЬНОЙ МОНЕТЫ | 732 |
| Жеребьевка с помощью идеальной монеты и квадратных корней | 732 |
| Жеребьевка с помощью идеальной монеты и возведения в степень по модулю p | 733 |
| Жеребьевка с помощью идеальной монеты и целых чисел Блюма | 734 |

| | |
|---|-----|
| 23.8. Односторонние сумматоры | 735 |
| 23.9. РАСКРЫТИЕ СЕКРЕТОВ ПО ПРИНЦИПУ “ВСЕ ИЛИ НИЧЕГО” | 735 |
| 23.10. Законные и отказоустойчивые криптосистемы | 739 |
| Законная схема Диффи–Хеллмана | 739 |
| Отказоустойчивая схема Диффи–Хеллмана | 740 |
| 23.11. Доказательство знания с нулевым разглашением | 740 |
| Доказательство знания дискретного логарифма с нулевым разглашением | 740 |
| Доказательство способности взломать алгоритм RSA с нулевым разглашением | 741 |
| Доказательство с нулевым разглашением того, что p является числом Блума | 742 |
| 23.12. Слепые подписи | 743 |
| 23.13. Забывчивая передача | 743 |
| 23.14. Тайные многосторонние вычисления | 744 |
| Пример протокола | 745 |
| 23.15. Вероятностное шифрование | 746 |
| 23.16. Квантовая криптография | 749 |

Часть IV

РЕАЛЬНЫЙ МИР 753

| | |
|---|------------|
| Глава 24. ПРИМЕРЫ РЕАЛИЗАЦИЙ | 755 |
| 24.1. Протокол компании IBM для управления секретными ключами | 755 |
| Модификация схемы | 756 |
| 24.2. Система MITRENET | 757 |
| 24.3. Телефонный терминал ISDN | 758 |
| Ключи | 758 |
| Вызов | 759 |
| 24.4. STU-III | 760 |
| 24.5. Протокол KERBEROS | 761 |
| Модель Kerberos | 761 |
| Как работает Kerberos | 762 |
| Удостоверения | 763 |
| Сообщения Kerberos версии 5 | 764 |
| Получение первоначального мандата | 764 |
| Получение серверных мандатов | 765 |
| Запрос к службе | 766 |
| Версия 4 протокола Kerberos | 766 |
| Стойкость протокола Kerberos | 767 |

| | |
|--|------------|
| Лицензии | 768 |
| 24.6. СИСТЕМА KRYPTOKNIGHT | 768 |
| 24.7. СИСТЕМА SESAME | 769 |
| 24.8. ОБЩАЯ КРИПТОГРАФИЧЕСКАЯ АРХИТЕКТУРА IBM | 770 |
| 24.9. СХЕМА ПРОВЕРКИ ПОДЛИННОСТИ ISO | 771 |
| Сертификаты | 772 |
| Протоколы аутентификации | 774 |
| 24.10. СТАНДАРТ PEM | 776 |
| Документы PEM | 777 |
| Сертификаты | 778 |
| Сообщения PEM | 778 |
| Безопасность стандарта PEM | 781 |
| Стандарт TIS/PEM | 783 |
| Программа RIPEM | 783 |
| 24.11. ПРОТОКОЛ БЕЗОПАСНОСТИ СООБЩЕНИЙ MSP | 784 |
| 24.12. ПРОГРАММА PRETTY GOOD PRIVACY (PGP) | 785 |
| 24.13. ИНТЕЛЛЕКТУАЛЬНЫЕ КАРТОЧКИ | 788 |
| 24.14. СТАНДАРТЫ КРИПТОГРАФИИ С ОТКРЫТЫМ КЛЮЧОМ | 789 |
| 24.15. УНИВЕРСАЛЬНАЯ СИСТЕМА ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ UEPS | 792 |
| 24.16. МИКРОСХЕМА CLIPPER | 794 |
| 24.17. МИКРОСХЕМА CAPSTONE | 797 |
| 24.18. БЕЗОПАСНЫЙ ТЕЛЕФОН AT&T MODEL 3600 TELEPHONE SECURITY DEVICE (TSD) | 798 |
| ГЛАВА 25. ПОЛИТИЧЕСКИЕ ВОПРОСЫ | 801 |
| 25.1. АГЕНТСТВО НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ | 801 |
| Коммерческая программа CSEP | 803 |
| 25.2. НАЦИОНАЛЬНЫЙ ЦЕНТР КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ (NCSC) | 804 |
| 25.3. НАЦИОНАЛЬНЫЙ ИНСТИТУТ СТАНДАРТОВ И ТЕХНИКИ NIST | 805 |
| 25.4. КОРПОРАЦИЯ RSA DATA SECURITY, INC. | 809 |
| 25.5. КОРПОРАЦИЯ PUBLIC KEY PARTNERS | 809 |
| 25.6. АССОЦИАЦИЯ IACR | 811 |
| 25.7. КОНСОРЦИУМ RIPE | 812 |
| 25.8. ПРОЕКТ CAFE | 812 |
| 25.9. СТАНДАРТ ISO/IEC 9979 | 813 |
| 25.10. ПРОФЕССИОНАЛЬНЫЕ, ПРОМЫШЛЕННЫЕ И ПРАВООЗАЩИТНЫЕ ГРУППЫ | 814 |
| Центр EPIC | 814 |
| Фонд EFF | 815 |
| Ассоциация ACM | 815 |

| | |
|--|-----|
| Институт IEEE | 815 |
| Ассоциация SPA | 815 |
| 25.11. КОМПЬЮТЕРНАЯ СЕТЬ SCI.CRYPT | 816 |
| 25.12. ШИФРОПАНКИ | 816 |
| 25.13. ПАТЕНТЫ | 817 |
| 25.14. ЭКСПОРТНОЕ ЗАКОНОДАТЕЛЬСТВО США | 817 |
| 25.15. ЭКСПОРТ И ИМПОРТ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗА РУБЕЖОМ | 826 |
| 25.16. ПРАВОВЫЕ ВОПРОСЫ | 827 |
| ПОСЛЕСЛОВИЕ МЭТТА БЛЕЙЗА | 829 |

Часть V
ПРИЛОЖЕНИЕ 833

| | |
|----------------------|------|
| Исходные коды | 835 |
| DES | 835 |
| LOKI91 | 846 |
| IDEA | 853 |
| ГОСТ | 859 |
| BLOWFISH | 864 |
| 3-WAY | 873 |
| RC5 | 879 |
| A5 | 883 |
| SEAL | 888 |
| СПИСОК ЛИТЕРАТУРЫ | 897 |
| ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ | 1021 |