

Содержание

Предисловие	16
Как читать эту книгу	18
Глава 1. Наша философия проектирования	20
1.1 Обратная сторона производительности	21
1.2 Обратная сторона оснащённости	24
Глава 2. Криптография в контексте окружающего мира	25
2.1 Роль криптографии	26
2.2 Правило слабого звена	27
2.3 Противоборствующее окружение	29
2.4 Практическая паранойя	30
2.4.1 Критика	31
2.5 Модель угроз	33
2.6 Криптография — это не решение	35
2.7 Криптография очень сложна	36
2.8 Криптография — это самая простая часть	37
2.9 Рекомендуемая литература	38
Глава 3. Введение в криптографию	39
3.1 Шифрование	39
3.1.1 Принцип Кирхгофа	41
3.2 Аутентификация	42
3.3 Шифрование с открытым ключом	44
3.4 Цифровые подписи	46
3.5 Инфраструктура открытого ключа	47
3.6 Типы атак	49
3.6.1 Только шифрованный текст	49
3.6.2 Известный открытый текст	49
3.6.3 Избранный открытый текст	50
3.6.4 Избранный шифрованный текст	51
3.6.5 Различающие атаки	51
3.6.6 Атаки, в основе которых лежит парадокс задачи о днях рождения	52

3.6.7	Двусторонняя атака	53
3.6.8	Другие типы атак	55
3.7	Уровень безопасности	55
3.8	Производительность	56
3.9	Сложность	58
Часть I Безопасность сообщений		61
Глава 4. Блочные шифры		62
4.1	Что такое блочный шифр?	62
4.2	Типы атак	63
4.3	Идеальный блочный шифр	65
4.4	Определение безопасности блочного шифра	65
4.4.1	Четность перестановки	68
4.5	Современные блочные шифры	70
4.5.1	DES	71
4.5.2	AES	74
4.5.3	Serpent	78
4.5.4	Twofish	79
4.5.5	Другие финалисты AES	82
4.5.6	Атаки с помощью решения уравнений	82
4.5.7	Какой блочный шифр выбрать	83
4.5.8	Каким должен быть размер ключа	85
Глава 5. Режимы работы блочных шифров		87
5.1	Дополнение	88
5.2	Электронная шифровальная книга (ECB)	89
5.3	Сцепление шифрованных блоков (CBC)	90
5.3.1	Фиксированный вектор инициализации	90
5.3.2	Счетчик	90
5.3.3	Случайный вектор инициализации	91
5.3.4	Оказия	92
5.4	Обратная связь по выходу (OFB)	93
5.5	Счетчик (CTR)	95
5.6	Новые режимы	97
5.7	Какой режим выбрать	98
5.8	Утечка информации	99
5.8.1	Вероятность коллизии	101
5.8.2	Как бороться с утечкой информации	102
5.8.3	О наших вычислениях	103

Глава 6. Функции хэширования	104
6.1 Безопасность функций хэширования	105
6.2 Современные функции хэширования	107
6.2.1 MD5	108
6.2.2 SHA-1	109
6.2.3 SHA-256, SHA-384 и SHA-512	110
6.3 Недостатки функций хэширования	111
6.3.1 Удлинение сообщения	111
6.3.2 Коллизия при частичном хэшировании сообщений	112
6.4 Исправление недостатков	113
6.4.1 Полное исправление	114
6.4.2 Более эффективное исправление	115
6.5 Какую функцию хэширования выбрать	116
6.6 Работа на будущее	117
Глава 7. Коды аутентичности сообщений	118
7.1 Что такое MAC	118
7.2 Идеальная функция вычисления MAC	119
7.3 Безопасность MAC	119
7.4 CBC-MAC	120
7.5 HMAC	122
7.5.1 HMAC или SHA_d ?	124
7.6 UMAC	125
7.6.1 Размер значения	125
7.6.2 Выбор функции	126
7.6.3 Платформенная гибкость	127
7.6.4 Нехватка анализа	128
7.6.5 Зачем тогда нужен UMAC?	128
7.7 Какую функцию вычисления MAC выбрать	129
7.8 Использование MAC	129
Глава 8. Безопасный канал общения	132
8.1 Формулировка проблемы	132
8.1.1 Роли	132
8.1.2 Ключ	133
8.1.3 Сообщения или поток	134
8.1.4 Свойства безопасности	134
8.2 Порядок аутентификации и шифрования	136
8.3 Структура решения	139
8.3.1 Номера сообщений	139
8.3.2 Аутентификация	140
8.3.3 Шифрование	141

8.3.4	Формат пакета	141
8.4	Детали реализации	142
8.4.1	Инициализация	142
8.4.2	Отправка сообщения	143
8.4.3	Получение сообщения	145
8.4.4	Порядок сообщений	146
8.5	Альтернативы	147
8.6	Заключение	149
Глава 9.	Проблемы реализации. Часть I	150
9.1	Создание правильных программ	152
9.1.1	Спецификации	152
9.1.2	Тестирование и исправление	153
9.1.3	Халатное отношение	154
9.1.4	Так что же нам делать?	155
9.2	Создание безопасного программного обеспечения	156
9.3	Как сохранить секреты	157
9.3.1	Уничтожение состояния	157
9.3.2	Файл подкачки	160
9.3.3	Кэш	161
9.3.4	Удерживание данных в памяти	163
9.3.5	Доступ других программ	165
9.3.6	Целостность данных	166
9.3.7	Что делать	167
9.4	Качество кода	168
9.4.1	Простота	168
9.4.2	Модуляризация	169
9.4.3	Утверждения	170
9.4.4	Переполнение буфера	171
9.4.5	Тестирование	172
9.5	Атаки с использованием побочных каналов	173
9.6	Заключение	174
Часть II	Согласование ключей	175
Глава 10.	Генерация случайных чисел	176
10.1	Истинно случайные числа	177
10.1.1	Проблемы использования истинно случайных чисел	178
10.1.2	Псевдослучайные числа	179
10.1.3	Истинно случайные числа и генераторы псевдослучайных чисел	180
10.2	Модели атак на генератор псевдослучайных чисел	181

10.3	Проект Fortuna	183
10.4	Генератор	183
10.4.1	Инициализация	186
10.4.2	Изменение начального числа	186
10.4.3	Генерация блоков	187
10.4.4	Генерация случайных данных	188
10.4.5	Скорость работы генератора	189
10.5	Аккумулятор	189
10.5.1	Источники энтропии	190
10.5.2	Пулы	191
10.5.3	Вопросы реализации	194
10.5.4	Инициализация	197
10.5.5	Получение случайных данных	197
10.5.6	Добавление события	199
10.6	Управление файлом начального числа	200
10.6.1	Запись в файл начального числа	201
10.6.2	Обновление файла начального числа	201
10.6.3	Когда нужно считывать и перезаписывать файл начального числа?	202
10.6.4	Архивирование	202
10.6.5	Атомарность операций обновления файловой системы	203
10.6.6	Первая загрузка	204
10.7	Так что же делать?	205
10.8	Выбор случайных элементов	206
Глава 11. Простые числа		208
11.1	Делимость и простые числа	208
11.2	Генерация малых простых чисел	211
11.3	Арифметика по модулю простого числа	213
11.3.1	Сложение и вычитание	214
11.3.2	Умножение	215
11.3.3	Группы и конечные поля	215
11.3.4	Алгоритм поиска НОД	217
11.3.5	Расширенный алгоритм Евклида	218
11.3.6	Вычисления по модулю 2	219
11.4	Большие простые числа	220
11.4.1	Проверка того, является ли число простым	223
11.4.2	Оценивание степеней	227

Глава 12. Алгоритм Диффи–Хеллмана	229
12.1 Группы	230
12.2 Базовый алгоритм Диффи–Хеллмана	231
12.3 Атака посредника	233
12.4 “Подводные камни” реализации	235
12.5 Надежные простые числа	236
12.6 Использование подгрупп меньшего размера	237
12.7 Размер p	238
12.8 Практические правила	241
12.9 Что может пойти не так	242
Глава 13. Алгоритм RSA	245
13.1 Введение	245
13.2 Китайская теорема об остатках	246
13.2.1 Формула Гарнера	247
13.2.2 Обобщение	248
13.2.3 Использование	248
13.2.4 Заключение	250
13.3 Умножение по модулю n	250
13.4 Определение RSA	251
13.4.1 Создание цифровой подписи с помощью RSA	252
13.4.2 Открытые показатели степеней	252
13.4.3 Закрытый ключ	253
13.4.4 Размер n	255
13.4.5 Генерация ключей RSA	255
13.5 “Подводные камни” использования RSA	257
13.6 Шифрование	259
13.7 Подписи	262
Глава 14. Введение в криптографические протоколы	266
14.1 Роли	266
14.2 Доверие	267
14.2.1 Риск	269
14.3 Стимул	269
14.4 Доверие в криптографических протоколах	272
14.5 Сообщения и действия	273
14.5.1 Транспортный уровень	273
14.5.2 Идентификация протоколов и сообщений	274
14.5.3 Кодирование и анализ сообщений	275
14.5.4 Состояние выполнения протокола	276
14.5.5 Ошибки	277
14.5.6 Воспроизведение и повторение	279

Глава 15. Протокол согласования ключей	282
15.1 Окружение	282
15.2 Первая попытка	283
15.3 Пусть всегда будут протоколы!	285
15.4 Соглашение об аутентификации	286
15.5 Вторая попытка	287
15.6 Третья попытка	288
15.7 Окончательная версия протокола	290
15.8 Анализ протокола с различных точек зрения	292
15.8.1 Точка зрения пользователя А	292
15.8.2 Точка зрения пользователя Б	293
15.8.3 Точка зрения злоумышленника	293
15.8.4 Взлом ключа	295
15.9 Вычислительная сложность протокола	296
15.9.1 Методы оптимизации	297
15.10 Сложность протокола	297
15.11 Небольшое предупреждение	299
15.12 Согласование ключей с помощью пароля	299
Глава 16. Проблемы реализации. Часть II	301
16.1 Арифметика больших чисел	301
16.1.1 Вупинг	303
16.1.2 Проверка вычислений алгоритма ДН	307
16.1.3 Проверка шифрования RSA	308
16.1.4 Проверка цифровых подписей RSA	308
16.1.5 Заключение	309
16.2 Быстрое умножение	309
16.3 Атаки с использованием побочных каналов	311
16.3.1 Меры предосторожности	312
16.4 Протоколы	314
16.4.1 Выполнение протоколов поверх безопасного канала общения	314
16.4.2 Получение сообщения	315
16.4.3 Время ожидания	317
Часть III Управление ключами	319
Глава 17. Часы	320
17.1 Зачем нужны часы	320
17.1.1 Срок действия	320
17.1.2 Уникальные значения	320
17.1.3 Монотонность	321

17.1.4	Выполнение транзакций в режиме реального времени	322
17.2	Использование микросхемы датчика времени	322
17.3	Виды угроз	323
17.3.1	Перевод часов назад	323
17.3.2	Остановка часов	324
17.3.3	Перевод часов вперед	325
17.4	Создание надежных часов	326
17.5	Проблема одного и того же состояния	327
17.6	Время	329
17.7	Заключение	330
Глава 18.	Серверы ключей	331
18.1	Основная идея	332
18.2	Kerberos	332
18.3	Решения попроще	333
18.3.1	Безопасное соединение	334
18.3.2	Создание ключа	335
18.3.3	Обновление ключа	335
18.3.4	Другие свойства	336
18.4	Что выбрать	336
Глава 19.	PKI: красивая мечта	337
19.1	Краткий обзор инфраструктуры открытого ключа	337
19.2	Примеры инфраструктуры открытого ключа	338
19.2.1	Всеобщая инфраструктура открытого ключа	338
19.2.2	Доступ к виртуальным частным сетям	339
19.2.3	Электронные платежи	339
19.2.4	Нефтеперегонный завод	339
19.2.5	Ассоциация кредитных карт	340
19.3	Дополнительные детали	340
19.3.1	Многоуровневые сертификаты	340
19.3.2	Срок действия	342
19.3.3	Отдельный центр регистрации	342
19.4	Заключение	343
Глава 20.	PKI: жестокая реальность	345
20.1	Имена	345
20.2	Полномочный орган	348
20.3	Доверие	349
20.4	Непрямая авторизация	350
20.5	Прямая авторизация	351
20.6	Системы мандатов	352

20.7	Измененная мечта	355
20.8	Отзыв	356
20.8.1	Список отзыва	356
20.8.2	Быстрое устаревание	358
20.8.3	Отзыв обязателен	358
20.9	Где может пригодиться инфраструктура открытого ключа	359
20.10	Что выбрать	361
Глава 21. Практические аспекты PKI		362
21.1	Формат сертификата	362
21.1.1	Язык разрешений	362
21.1.2	Ключ корневого ЦС	363
21.2	Жизненный цикл ключа	364
21.3	Почему ключи изнашиваются	367
21.4	Так что же нам делать?	368
Глава 22. Хранение секретов		369
22.1	Диск	369
22.2	Человеческая память	370
22.2.1	Солим и растягиваем	372
22.3	Портативное хранилище	375
22.4	Идентификатор безопасности	376
22.5	Безопасный пользовательский интерфейс	377
22.6	Биометрика	379
22.7	Однократная регистрация	380
22.8	Риск утраты	381
22.9	Совместное владение секретом	382
22.10	Уничтожение секретов	383
22.10.1	Бумага	383
22.10.2	Магнитное хранилище	384
22.10.3	Полупроводниковые записывающие устройства	386
Часть IV Разное		387
Глава 23. Стандарты		388
23.1	Процесс стандартизации	388
23.1.1	Стандарт	390
23.1.2	Функциональность	390
23.1.3	Безопасность	391
23.2	SSL	392
23.3	AES: стандартизация на конкурсной основе	393

Глава 24. Патенты	395
24.1 Прототип	395
24.2 Расширения	396
24.3 Расплывчатость описаний	397
24.4 Чтение патентов	397
24.5 Лицензирование	398
24.6 Защищающие патенты	400
24.7 Как исправить систему патентования	400
24.8 Отречение	401
Глава 25. Привлечение экспертов	402
Благодарности	407
Список основных источников информации	408
Предметный указатель	416