УДК 004.382
ББК 32.973-018
Р82

Рубин Ф.
Р82 Криптография с секретным ключом / пер. с англ. А. А. Слинкина. – М.: ДМК Пресс, 2023. – 386 с.: ил.

ISBN 978-5-97060-748-0

В книге объясняется, как создавать шифры с секретным ключом – от простых, для которых хватает карандаша и бумаги, до очень сложных, применяемых в современной компьютерной криптографии. Вы научитесь конструировать 30 невскрываемых шифров, измерять стойкость шифров и гарантированно обеспечивать их безопасность, противостоять гипотетическим ультракомпьютерам будущего. А для развлечения предлагается вскрыть несколько несложных мини-шифров.

Издание предназначено для профессиональных инженеров, специалистов по информатике и криптографов-любителей.

УДК 004.382
ББК 32.973-018

ISBN 978-1-6334-3979-5 (англ.)
ISBN 978-5-97060-748-0 (рус.)

Содержание

Оглавление 5
Вступительное слово 13
Предисловие 16
Благодарности 18
Об этой книге 19
Об авторе 22
Об иллюстрации на обложке 23

1 ***Введение*** 24

2 ***Что такое криптография?*** 27
2.1 Невскрываемые шифры 28
2.2 Виды криптографии 30
2.3 Симметричная и асимметричная криптография 32
2.4 Блочные и потоковые шифры 33
2.5 Механические и цифровые шифры 33
2.6 Зачем выбирать шифр с секретным ключом? 37
2.7 Зачем создавать собственный шифр? 38

3 ***Предварительные сведения*** 41
3.1 Биты и байты 41
3.2 Функции и операторы 42
3.3 Булевы операторы 43
3.4 Системы счисления 44
3.5 Простые числа 46
3.6 Модульная арифметика 46

4 ***Инструментарий криптографа*** 48
4.1 Система оценивания 49

4.2 Подстановка ... 50
4.2.1 Коды Хаффмана ... 51
4.3 Перестановка ... 52
4.4 Фракционирование ... 53
4.5 Генераторы случайных чисел ... 54
4.5.1 Цепной генератор цифр ... 56
4.6 Полезные комбинации, бесполезные комбинации ... 58
4.6.1 Шифр Базери типа 4 ... 59

5 Подстановочные шифры ... 61
5.1 Простая подстановка ... 62
5.2 Перемешивание алфавита ... 67
5.3 Номенклаторы ... 70
5.4 Многоалфавитная подстановка ... 70
5.5 Шифр Беласо ... 71
5.6 Метод Касиски ... 72
5.7 Индекс совпадения ... 76
5.8 И снова об индексе совпадения ... 77
5.9 Вскрытие многоалфавитного шифра ... 78
5.9.1 Вскрытие шифра Беласо ... 78
5.9.2 Вскрытие шифра Виженера ... 81
5.9.3 Вскрытие общего многоалфавитного шифра ... 83
5.10 Автоключ ... 85
5.11 Бегущий ключ ... 86
*5.12 Моделирование роторных машин ... 88
5.12.1 Одноротorная машина ... 90
5.12.2 Трехроторная машина ... 91
5.12.3 Восьмироторная машина ... 92

6 Контрмеры ... 94
6.1 Двойное шифрование ... 95
6.2 Null-символы ... 96
6.3 Прерванный ключ ... 96
6.4 Омофоническая подстановка ... 99
6.4.1 Шифр 5858 ... 100
6.5 Подстановка биграмм и триграмм ... 100
*6.6 Сокрытие сообщений в изображениях ... 101
6.7 Добавление null-битов ... 103
6.8 Объединение нескольких сообщений ... 105
6.9 Внедрение сообщения в файл ... 107

7 Перестановка ... 109
7.1 Маршрутная перестановка ... 109
7.2 Столбцовая перестановка ... 111
7.2.1 Cysquare ... 115
7.2.2 Перестановка слов ... 116

7.3 Двойная столбцовая перестановка 117
7.4 Столбцовая перестановка с циклическим сдвигом 118
7.5 Перестановка со случайными числами 120
7.6 Селекторная перестановка 121
7.7 Перестановка с ключом 122
7.8 Деление перестановки пополам 125
7.9 Множественные анаграммы 126

8 *Цилиндрический шифр Джефферсона* 128
8.1 Вскрытие при наличии известных слов 131
8.2 Вскрытие при наличии только шифртекста 132

9 *Фракционирование* 135
9.1 Квадрат Полибия 136
9.2 Шифр Плейфера 137
9.2.1 Вскрытие шифра Плейфера 139
9.2.2 Укрепление шифра Плейфера 140
9.3 Шифр Two Square 142
9.4 Шифр Three Square 143
9.5 Шифр Four Square 146
9.6 Шифр Bifid 148
9.6.1 Bifid с сопряженной матрицей 150
9.7 Диагональный Bifid 151
9.8 Квадраты 6×6 152
9.9 Шифр Trifid 152
9.10 Шифр Three Cube 154
9.11 Прямоугольные сетки 156
9.12 Шестнадцатеричное фракционирование 157
9.13 Битовое фракционирование 158
9.13.1 Шифр Cyclic 8×N 159
9.14 Другие виды фракционирования 160
9.15 Повышение стойкости блоков 161

10 *Фракционирование переменной длины* 163
10.1 Шифр Morse3 164
10.2 Моном-биномные шифры 165
10.3 Периодические длины 167
10.4 Подстановка Хаффмана 168
10.5 Таг-системы Поста 171
10.5.1 Таги одинаковой длины 172
10.5.2 Таги разной длины 174
10.5.3 Несколько алфавитов 176
10.5.4 Короткие и длинные перемещения 177
10.6 Фракционирование в системах счисления по другим основаниям 177
10.7 Сжатие текста 178

10.7.1 Метод Лемпеля–Зива 178
10.7.2 Арифметическое кодирование 181
10.7.3 Адаптивное арифметическое кодирование 184

11 *Блочные шифры* 188
11.1 Подстановочно-перестановочная сеть 189
11.2 Стандарт шифрования данных (DES) 191
11.2.1 Double DES 192
11.2.2 Triple DES 193
**11.2.3 Быстрая перестановка битов* 194
11.2.4 Неполные блоки 195
11.3 Умножение матриц 196
11.4 Умножение матриц 197
11.5 Улучшенный стандарт шифрования (AES) 198
11.6 Фиксированная подстановка и подстановка с ключом 200
11.7 Инволютивные шифры 201
11.7.1 Инволютивная подстановка 202
11.7.2 Инволютивная многоалфавитная подстановка 202
11.7.3 Инволютивная перестановка 202
**11.7.4 Инволютивный блочный шифр* 203
11.7.5 Пример – шифр Poly Triple Flip 204
11.8 Подстановки переменной длины 204
11.9 Пульсирующие шифры 205
11.10 Сцепление блоков 208
11.10.1 Многоалфавитное сцепление 209
11.10.2 Зашифрованное сцепление 210
11.10.3 Сцепление с запаздыванием 210
11.10.4 Внутренние отводы 210
11.10.5 Сцепление ключей 211
11.10.6 Сводка режимов сцепления 211
11.10.7 Сцепление с неполными блоками 211
11.10.8 Сцепление блоков переменной длины 211
11.11 Укрепление блочного шифра 212

12 *Принципы безопасного шифрования* 214
12.1 Большие блоки 214
12.2 Длинные ключи 215
12.2.1 Избыточные ключи 216
12.3 Конфузия 217
12.3.1 Коэффициент корреляции 219
12.3.2 Линейность по основанию 26 223
12.3.3 Линейность по основанию 256 226
12.3.4 Включение закладки 227
12.3.5 Конденсированная линейность 231
12.3.6 Гибридная нелинейность 232
12.3.7 Конструирование S-блока 232
12.3.8 S-блок с ключом 236

12.4 Диффузия 236
12.5 Насыщение 240
Резюме 245

13 *Потоковые шифры* 246
13.1 Комбинирующие функции 247
13.2 Случайные числа 248
13.3 Мультипликативный конгруэнтный генератор 249
13.4 Линейный конгруэнтный генератор 253
13.5 Цепной XOR-генератор 254
13.6 Цепной аддитивный генератор 256
13.7 Сдвиговый XOR-генератор 256
13.8 FRand 257
13.9 Вихрь Мерсенна 259
13.10 Регистры сдвига с линейной обратной связью 259
13.11 Оценивание периода 261
13.12 Укрепление генератора 263
13.13 Комбинирование генераторов 264
13.14 Истинно случайные числа 268
13.14.1 Линейное суммирование с запаздыванием 268
13.14.2 Наложение изображений 269
13.15 Обновление случайных байтов 270
13.16 Синхронизированные гаммы 272
13.17 Функции хеширования 273

14 *Одноразовый блокнот* 276
14.1 Шифр Вернама 278
14.2 Запас ключей 280
14.2.1 Возвращение ключей в оборот 281
14.2.2 Комбинированный ключ 281
14.2.3 Ключ выбора 281
14.3 Индикаторы 282
14.4 Алгоритм распределения ключей Диффи–Хеллмана 283
**14.4.1 Построение больших простых чисел, старый подход* 285
14.4.2 Построение больших простых чисел, новый подход 286

15 *Матричные методы* 292
15.1 Обращение матрицы 293
15.2 Матрица перестановки 296
15.3 Шифр Хилла 296
15.4 Шифр Хилла, компьютерные версии 299
15.5 Умножение больших целых чисел 303
15.5.1 Умножение и деление сравнений 304
*15.6 Решение линейных сравнений 305
15.6.1 Приведение сравнения 305
15.6.2 Правило половины 306

15.6.3 Лесенка ... 308
15.6.4 Цепные дроби ... 309
15.7 Шифры на основе больших целых чисел ... 310
15.8 Умножение на малое число ... 311
15.9 Умножение по модулю P ... 313
15.10 Изменение основания ... 315
*15.11 Кольца ... 317
15.12 Матрицы над кольцом ... 318
15.13 Построение кольца ... 319
15.13.1 Гауссовы целые числа ... 321
15.13.2 Кватернионы ... 322
15.14 Нахождение обратимых матриц ... 323

16 ***Трехпроходный протокол*** ... 326
16.1 Метод Шамира ... 328
16.2 Метод Мэсси–Омуры ... 329
16.3 Дискретный логарифм ... 329
16.3.1 Логарифмы ... 330
16.3.2 Степени простых чисел ... 330
16.3.3 Коллизия ... 331
16.3.4 Факторизация ... 331
16.3.5 Оценки ... 333
16.4 Матричный трехпроходный протокол ... 333
16.4.1 Коммутативное семейство матриц ... 334
16.4.2 Мультипликативный порядок ... 334
16.4.3 Максимальный порядок ... 335
16.4.4 Атаки Эмили ... 336
16.4.5 Некоммутативное кольцо ... 337
16.4.6 Решение билинейных уравнений ... 337
16.4.7 Слабые элементы ... 339
16.4.8 Как сделать побыстрее ... 339
16.5 Двусторонний трехпроходный протокол ... 340

17 ***Коды*** ... 342
17.1 Джокер ... 343

18 ***Квантовые компьютеры*** ... 346
18.1 Суперпозиция ... 347
18.2 Квантовая запутанность ... 348
18.3 Исправление ошибок ... 349
18.4 Измерение ... 350
18.5 Квантовый трехэтапный протокол ... 351
18.6 Квантовое распределение ключей ... 352
18.7 Алгоритм Гровера ... 352
18.8 Уравнения ... 353
18.8.1 Перестановки ... 353

18.8.2 *Подстановки* ... 354
18.8.3 *Карты Карно* ... 354
18.8.4 *Промежуточные переменные* ... 355
18.8.5 *Известный открытый текст* ... 355
18.9 Минимизация ... 356
18.9.1 *Восхождение на вершину* ... 356
18.9.2 *Тысяча вершин* ... 357
18.9.3 *Имитация отжига* ... 358
18.10 Квантовая имитация отжига ... 360
18.11 Квантовая факторизация ... 360
18.12 Ультракомпьютеры ... 360
18.12.1 *Подстановка* ... 361
18.12.2 *Случайные числа* ... 362
18.12.3 *Ультраподстановочный шифр US-A* ... 363
18.12.4 *Ультрапотоковый шифр US-B* ... 364

Развлечения ... 366
Задачи ... 369
Эпилог ... 371
Предметный указатель ... 374