

# Оглавление

---

|   |     |
|---|-----|
| 1 ■ Введение .....                          | 24  |
| 2 ■ Что такое криптография?.....            | 27  |
| 3 ■ Предварительные сведения .....          | 41  |
| 4 ■ Инструментарий криптографа .....        | 48  |
| 5 ■ Подстановочные шифры.....               | 61  |
| 6 ■ Контрмеры.....                          | 94  |
| 7 ■ Перестановка .....                      | 109 |
| 8 ■ Цилиндрический шифр Джефферсона.....    | 128 |
| 9 ■ Фракционирование .....                  | 135 |
| 10 ■ Фракционирование переменной длины..... | 163 |
| 11 ■ Блочные шифры.....                     | 188 |
| 12 ■ Принципы безопасного шифрования.....   | 214 |
| 13 ■ Поточковые шифры.....                  | 246 |
| 14 ■ Одноразовый блокнот .....              | 276 |
| 15 ■ Матричные методы .....                 | 292 |
| 16 ■ Трехпроходный протокол .....           | 326 |
| 17 ■ Коды .....                             | 342 |
| 18 ■ Квантовые компьютеры.....              |     |

# Содержание

---

|          |   |           |
|----------|---|-----------|
|          | Оглавление .....                                    | 5         |
|          | Вступительное слово.....                            | 13        |
|          | Предисловие .....                                   | 16        |
|          | Благодарности .....                                 | 18        |
|          | Об этой книге.....                                  | 19        |
|          | Об авторе .....                                     | 22        |
|          | Об иллюстрации на обложке.....                      | 23        |
| <b>1</b> | <b>Введение .....</b>                               | <b>24</b> |
| <b>2</b> | <b>Что такое криптография? .....</b>                | <b>27</b> |
|          | 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        |
| <b>3</b> | <b>Предварительные сведения .....</b>               | <b>41</b> |
|          | 3.1 Биты и байты.....                               | 41        |
|          | 3.2 Функции и операторы.....                        | 42        |
|          | 3.3 Булевы операторы .....                          | 43        |
|          | 3.4 Системы числения .....                          | 44        |
|          | 3.5 Простые числа.....                              | 46        |
|          | 3.6 Модульная арифметика.....                       | 46        |
| <b>4</b> | <b>Инструментарий криптографа .....</b>             | <b>48</b> |
|          | 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 |

|          |  |    |
|----------|--|----|
| <b>5</b> | <b>Подстановочные шифры</b> .....            | 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   | Однороторная машина.....                     | 90 |
| 5.12.2   | Трехроторная машина .....                    | 91 |
| 5.12.3   | Восьмироторная машина .....                  | 92 |

|          |  |     |
|----------|--|-----|
| <b>6</b> | <b>Контрмеры</b> .....                   | 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     | Соккрытие сообщений в изображениях ..... | 101 |
| 6.7      | Добавление null-битов.....               | 103 |
| 6.8      | Объединение нескольких сообщений.....    | 105 |
| 6.9      | Внедрение сообщения в файл.....          | 107 |

|          |                               |     |
|----------|-------------------------------|-----|
| <b>7</b> | <b>Перестановка</b> .....     | 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 |

|          |  |            |
|----------|--|------------|
| <b>8</b> | <b>Цилиндрический шифр Джефферсона .....</b> | <b>128</b> |
| 8.1      | Вскрытие при наличии известных слов .....    | 131        |
| 8.2      | Вскрытие при наличии только шифртекста ..... | 132        |

|          |  |            |
|----------|--|------------|
| <b>9</b> | <b>Фракционирование .....</b>            | <b>135</b> |
| 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        |

|           |   |            |
|-----------|---|------------|
| <b>10</b> | <b>Фракционирование переменной длины .....</b>                      | <b>163</b> |
| 10.1      | Шифр Morse3 .....   | 164        |
| 10.2      | Моном-биномные шифры .....  | 165        |
| 10.3      | Периодические длины .....   | 167        |
| 10.4      | Подстановка Хаффмана .....  | 168        |
| 10.5      | Тэг-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<br>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        |
| <b>11</b> | <b>Блочные шифры</b> .....                             | <b>188</b> |
| 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        |
| <b>12</b> | <b>Принципы безопасного шифрования</b> .....           | <b>214</b> |
| 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 |

|           |  |            |
|-----------|--|------------|
| <b>13</b> | <b>Потоковые шифры.....</b>                        | <b>246</b> |
| 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      | Сдвиговой 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        |

|           |  |            |
|-----------|--|------------|
| <b>14</b> | <b>Одноразовый блокнот .....</b>                             | <b>276</b> |
| 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        |

|           |  |            |
|-----------|--|------------|
| <b>15</b> | <b>Матричные методы.....</b>               | <b>292</b> |
| 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        |
| <b>16</b> | <b>Трехпроходный протокол .....</b>      | <b>326</b> |
| 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        |
| <b>17</b> | <b>Коды.....</b>                         | <b>342</b> |
| 17.1      | Джокер .....                             | 343        |
| <b>18</b> | <b>Квантовые компьютеры .....</b>        | <b>346</b> |
| 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 | Ультрапоточковый шифр US-B .....     | 364 |
|         | Развлечения .....                    | 366 |
|         | Задачи .....                         | 369 |
|         | Эпилог .....                         | 371 |
|         | Предметный указатель .....           | 374 |



# Вступительное слово

---

От тайных дешифровальных колец до правительственных директив, задачи сокрытия и обнаружения информации в составе другой информации давно будоражили человеческий ум. Криптология – завораживающий предмет, с которым на практике сталкивался едва ли не всякий школьник. И вместе с тем имеются веские причины, по которым эта дисциплина на протяжении веков была окутана глубочайшей тайной, поскольку государства использовали ее для защиты своего самого секретного оружия. В военных и дипломатических делах к криптографии всегда относились в высшей степени серьезно. Не будет преувеличением сказать, что успехи и провалы криптографии влияли на исход войн и ход истории, и точно так же они определяют нашу современную историю.

Возьмем сражение при Энтитеме в ходе Гражданской войны в США, произошедшее в сентябре 1862 года близ Шарпсбурга, штат Мэриленд, в котором Федеральная армия под командованием Джорджа Макклеллана противостояла армии Конфедерации под командованием Роберта Ли. За несколько дней до него два солдата федералов нашли недалеко от лагеря листок бумаги, оказавшийся копией приказа Ли, в котором были подробно изложены планы вторжения в Мэриленд. Приказ не был зашифрован. Располагая этой информацией, Макклеллан точно знал местоположение рассеянных отрядов и смог уничтожить армию Ли, не дав им соединиться.

Успехи и провалы криптографии оказывали влияние и на более близкие к нам события. Сокрушительное поражение русской армии при Танненберге в августе 1914 года стало прямым следствием перехвата сообщений немцами. Удивительно, но сообщения русских передавались открытым текстом, потому что у полевых командиров не было ни шифров, ни ключей. Поэтому русские не могли безопасно координировать действия соседних подразделений.

50 лет холодной войны, последовавшей за Второй мировой войной, тоже стали результатом провала криптографии, на этот раз со стороны японцев в битве за Мидуэй в 1942 году. Американские криптоаналитики взломали японские коды и могли читать многие донесения Объединенного флота. Подобные истории – вотчина классической криптографии. Книга «Криптография с секретным ключом» как раз на этом поле и играет.

Никто не сможет лучше доктора Фрэнка Рубина провести интересующего читателя по всем закоулкам классической криптологии на любительском уровне, от математических истоков до социальных последствий. Доктор Рубин получил образование в области математики и информатики. Тридцать лет он проработал в компании IBM, в отделе автоматизации проектирования, и свыше 50 лет занимался криптографией. Доктор Рубин был редактором журнала «Cryptologia» и других изданий. Он автор десятков статей по математике и компьютерным алгоритмам, а также тысяч математических головоломок.

«Криптография с секретным ключом» – не просто новая версия классической книги Helen F. Gaines «Elementary Cryptanalysis». Здесь предмет рассматривается с древних времен до эры квантовых компьютеров. И, что немаловажно, описывается уникальный метод измерения стойкости шифра<sup>1,2</sup>.

Книга выходит в стратегически важный момент. Это своевременный и существенный вклад в понимание критической технологии. Не важно, испытывает ли читатель бескорыстный интерес к криптологии как таковой или занимается практической защитой информации, материал, изложенный на этих страницах, благодаря глубине и широте охвата станет желанным источником полезной информации, а сама книга – ценным пополнением библиотеки.

– Рэндалл К. Николс, DTM

*Рэндалл К. Николс – бывший президент  
Американской ассоциации криптограмм,  
отвечавший, в частности, за обзоры книг;  
директор программы сертификации беспилотных летательных систем  
на предмет кибербезопасности в Канзасском университете в Салине;  
заслуженный профессор отделения послевузовского образования  
в области кибербезопасности и компьютерно-технической экспертизы  
в колледже Ютики.*

<sup>1</sup> И в книге R. K. Nichols «ICSA Guide to Cryptography», и в классическом труде Брюса Шнейера «Прикладная криптография» приведены методы оценки стойкости шифров и случайности. Первая посвящена в основном классической криптографии, вторая – в большей степени современным шифрам (Nichols, 1999; Schneier, 1995).

<sup>2</sup> В «Криптографии с секретным ключом» лучше отобран и лучше изложен материал, чем в двух моих первых книгах по классической криптографии: «Classical Cryptography Course», т. I и II (LANAKI, 1998; 1999).

## ЛИТЕРАТУРА

- Gaines, H. F. (1956). *Cryptanalysis: A Study of Ciphers and their Solution*. NYC: Dover.
- LANAKI. (1998). *Classical Cryptography Course Vol. I*. Laguna Hills, CA: Aegean Park Press.
- LANAKI. (1999). *Classical Cryptography Course Vol. II*. Laguna Hills, CA: Aegean Park Press.
- Nichols, R. K. (1999). *ICSA Guide to Cryptography*. New York City: McGraw Hill.
- Rubin, F. (2022). *Secret Key Cryptography*. Shelter Island, New York: Manning Books.
- Schneier, B. (1995). *Applied Cryptography: Protocols, Algorithms and Source Code in C*. New York: John Wiley & Sons.

# Предисловие

---

К идее написать эту книгу меня привели разные дорожки. Начну с моего школьного друга Чарли Роуза. Чарли работал в школьном книжном магазине. В один прекрасный день, заказывая книги для магазина, он обратил внимание на книгу Хелен Ф. Гейнс «Криптоанализ». Чарли захотел приобрести ее, да еще и с отраслевой скидкой. Но вот незадача – магазин должен был заказать как минимум три экземпляра.

Чарли нужно было найти еще двух желающих купить книгу. Он пообещал, что мы все вместе прочтем ее, а затем будем придумывать криптограммы, которые другие должны будут решать. Я книгу купил, прочел и начал составлять криптограммы, а Чарли утратил интерес.

На обратной стороне обложки «Криптоанализа» был напечатан давно устаревший адрес Американской ассоциации криптограмм ([www.cryptogram.org](http://www.cryptogram.org)), но я все-таки нашел ее и вступил в ее члены. И начал решать разные типы криптограмм, которые публиковались в бюллетене для любителей «The Cryptogram». А спустя несколько лет стал заместителем редактора. И вот уже более 40 лет остаюсь членом Ассоциации.

В 1977 году был основан более профессиональный журнал по криптографии, «Cryptologia». Его можно найти в интернете по адресу <https://www.tandfonline.com/toc/ucry20/current>. Сначала я читал статьи, потом начал писать и в конце концов стал редактором. Как-то так получилось, что ко мне стекались все статьи разных фриков, и приходилось продирааться сквозь хитросплетения нелогичной логики – вдруг где-то в глубине притаилась хорошая идея. И один раз такое случилось. Я превратил эту идею в статью для «The Cryptogram». Автор был так благодарен, что посадил в мою честь дерево в Израиле.

Этот опыт научил меня отделять статьи, которые просто плохо написаны или переоценивают стойкость шифра, от трудов совсем уж чокнутых авторов. И вот что я понял: любитель, придумавший слабый шифр, может его описать и разложить по шагам. Мечтатель не сможет излить смутные, но грандиозные плоды своего воображения на бумагу. Он будет изводить целые стопки бумаги, расписывая чудесные свойства своего шифра, но не в силах выписать его шаги. Он не способен превратить свои бессвязные мысли в конкретный алгоритм.

Начиная с 2005 года я стал посещать курсы в колледже Марист по программе непрерывного образования. Вскоре я читал лекции по sudoku, SumSum и другим головоломкам (я написал три книги о sudoku), своим путешествиям по Танзании и Монголии, конструкции Эмпайр Стейт Билдинг, жизни Алана Тьюринга и другим темам. Я стал членом комиссии по учебным планам.

В 2018 году я вызвался прочесть двухсеместровый курс по криптографии. Подготовив почти 450 слайдов, я понял, что материала достаточно для книги. И на мое счастье, обнаружилось, что годом раньше я уже начал писать как раз такую книгу. Вот эту.

# Благодарности

---

На днях я случайно услышал, как моя жена Мириам в разговоре по телефону сказала: «У нас тут секс втроем, я, Фрэнк и книга». Спасибо, Мириам, что ты 18 месяцев терпеливо сносила, как я писал эту книгу, потом год искал издателя, шесть месяцев охотился за литературным агентом, год наблюдал за отсутствием у агента каких-либо результатов и, наконец, месяц искал пристанище для этой книги в издательстве Manning. И еще 18 месяцев рецензирования, правки, редактирования, верстки, правки, составления указателя и всякой всячины.

Я благодарен всем сотрудникам издательства Manning Publications, которые помогли мне с этой книгой, особенно Майклу Стивенсу, который ухватился за шанс и предложил мне контракт, а потом помогал на всех стадиях процесса; Марине Майклз за обширную редакторскую правку; Ребекке Райнхарт, которая сделала мой путь не таким тернистым; Джэн Хоул и Сьюзан Хониуэлл за работу над иллюстрациями; Тиффани Тэйлор за многочисленные ценные замечания по поводу грамматики и пунктуации; Полу Уэллсу и Кэри Хейлз за работу над производством книги; Сэму Вуду за рекламный текст; Дэннису Далиннику за верстку и, конечно, Марджану Бейсу, издателя.

Отдельное спасибо профессору Рэндаллу К. Николсу, написавшему предисловие к книге и рецензию в «The Cryptogram», несмотря на крайне сжатые сроки. Спасибо также профессору Томасу Перера из Музея Энигмы за предоставленные изображения Фиалки.

Я благодарю рецензентов, которые прочитали рукопись и сделали множество полезных критических замечаний и предложений: Кристофера Карделла, Алекса Лукаса, Габора Хаджба, Михала Рутка, Джейсон Тэйлор, Роя Принса, Мэттью Харвелла, Риккардо Маротти и Пола Лава. Ваши предложения помогли сделать книгу лучше.

Наконец, не могу не отметить нечаянную роль Ли Харви Освальда: совершив чудовищное убийство президента Кеннеди, он помешал мне прийти на собеседование по безопасности в штаб-квартиру ФБР, что не дало мне возможности поступить на работу в АНБ, где написание подобной книги считалось бы преступным деянием.

# Об этой книге

---

## *Для кого предназначена эта книга*

Книга рассчитана на широкую аудиторию: массового читателя, криптографов-любителей, почитателей истории, студентов компьютерных специальностей, инженеров-электротехников, математиков и профессиональных криптографов. Это усложнило мне работу, потому что невозможно сделать все части книги одинаково интересными для всех. Для кого-то в некоторых частях окажется слишком много математики. А кому-то какие-то части покажутся чересчур элементарными. В этом разделе я попробую подсказать читателям, что, на мой взгляд, им стоит прочитать.

- **Массовые читатели** могут читать всё подряд до конца главы 8. Если математика покажется слишком сложной или изложение – перенасыщенным техническими подробностями, просто пропускайте соответствующие страницы. Начиная с главы 9 материал становится более трудным. Дальше можно читать выборочно, только то, что кажется интересным. Быть может, имеет смысл прочитать главу 12, чтобы получить общее представление, не вдаваясь в детали.
- **Криптографы-любители**, вероятно, захотят прочитать книгу целиком, а затем более внимательно изучить разделы 4.2–5.11, 6.1–6.5, 6.7, большую часть главы 7, а также разделы 9.1–9.9 и главы «Развлечения» и «Задачи».
- **Почитатели истории** могут прочитать книгу целиком, пропуская всю математику, но обращая внимание на то, когда и кем были изобретены различные методы.
- **Студентам компьютерных специальностей** рекомендую уделить особое внимание разделам 5.6–5.11, главе 8 и главам 11–16.
- **Инженеров-электротехников** могут заинтересовать практические методы. Им стоит прочитать главы 2 и 4, где излагаются

основы, а затем разделы 7.2–7.8, главу 9 и главы 11–16, обращая особое внимание на главу 12.

- **Математикам** будут особенно интересны раздел 4.5, разделы 5.6–5.12, 10.4–10.7, 11.7–11.10, 12.3–12.6, главы 13–16, в особенности раздел 16.4.6, и глава 18.
- Для **профессиональных криптографов** интерес могут представлять разделы 7.8, 8.2, 10.5, 10.7, 11.4, 12.3–12.6, 13.8, 13.15, 14.2, 14.4, 15.4–15.14, 16.4, 16.5 и 18.12.

## О шифрах

Я включил несколько развлекательных головоломок и более серьезных задач для читателей, которые хотят попробовать свои силы во вскрытии шифров. Для решения головоломок достаточно стандартных методов, описанных в книге.

При решении задач применяются методы, которые я придумал сам. Они достаточно просты, так что любитель сможет догадаться о методе и решить задачу. Я старался не вредничать и дать возможность интересующимся читателям найти решение. Не бойтесь – там нет ничего заумного или чрезмерно сложного. Никаких несуществующих слов или искаженных частот букв. И достаточно материала для решения.

Некоторые разделы начинаются символом \* и заканчиваются символами \*\*. Это факультативные разделы, которые могут содержать компьютерные алгоритмы или углубленную математику. Кто-то захочет их пропустить.

## Форум на сайте liveBook

Приобретение этой книги открывает бесплатный доступ к платформе liveBook онлайн-очтения, созданной издательством Manning. Средства обсуждения на liveBook позволяют присоединять комментарию как к книге в целом, так и к отдельным разделам или абзацам. Совсем несложно добавить примечания для себя, задать или ответить на технический вопрос и получить помощь от автора и других пользователей. Для доступа к форуму перейдите по адресу <https://livebook.manning.com/book/secret-key-cryptography/discussion>. Узнать о форумах Manning и правилах поведения на них можно по адресу <https://livebook.manning.com/discussion>.

Издательство Manning обязуется предоставлять площадку для содержательного диалога между читателями, а также между читателями и автором. Но это обязательство не подразумевает какого-то конкретного объема присутствия со стороны автора, участие которого в работе форума остается добровольным (и не оплачивается). Мы рекомендуем задавать автору трудные вопросы, чтобы его интерес не угасал! Форум и архивы прошлых обсуждений остаются доступны на сайте издательства до тех пор, пока книга продолжает допечатываться.



## *Другие онлайн-ресурсы*

Криптографические продукты, созданные автором, можно найти на его сайте по адресу [www.mastersoftware.biz](http://www.mastersoftware.biz).

## *Отзывы и пожелания*

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге, – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте [www.dmkpress.com](http://www.dmkpress.com), зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу [dmkpress@gmail.com](mailto:dmkpress@gmail.com); при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу [http://dmkpress.com/authors/publish\\_book/](http://dmkpress.com/authors/publish_book/) или напишите в издательство по адресу [dmkpress@gmail.com](mailto:dmkpress@gmail.com).

## *Список опечаток*

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг, мы будем очень благодарны, если вы сообщите о ней главному редактору по адресу [dmkpress@gmail.com](mailto:dmkpress@gmail.com). Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

## *Нарушение авторских прав*

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Manning Publications очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты [dmkpress@gmail.com](mailto:dmkpress@gmail.com).

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

## Об авторе

---



**Фрэнк Рубин** – обладатель степени бакалавра и магистра математики и доктора информатики. Он 28 лет проработал в подразделении автоматизации проектирования компании IBM, где разрабатывал специализированное программное обеспечение, которым инженеры IBM пользовались при проектировании компьютеров и электрических схем. Он владелец компании Master Software Corp., разрабатывающей криптографические продукты. Фрэнк – автор четырех патентов США по криптографическим методам. Он автор примерно 50 работ, опубликованных в реферируемых журналах по криптографии, а также нескольких внутренних документов IBM (руководств пользователя и проектных спецификаций). В области криптографии он известен прежде всего тем, что вскрыл цилиндрический шифратор Джефферсона. В информатике хорошо известен его метод арифметического кодирования, ставший одним из стандартных методов сжатия текстов, а также его алгоритм нахождения гамильтоновых путей. В чистой математике известна его идея применить распознаватель с конечным числом состояний к теории меры. Фрэнк опубликовал три книги по sudoku, а также две «самиздатовские» книги по головоломкам SumSum. Он автор более 3500 задач, опубликованных в журналах «The Cryptogram», «Technology Review» и «Journal of Recreational Mathematics» (JRM), и единственный, удостоившийся специального выпуска JRM, посвященного исключительно его задачам.

# Об иллюстрации на обложке

---

На обложке книги изображен «Le Garçon de Bureau», или «Канторский служащий». Рисунок взят из книги, изданной под редакцией Луи Кюрмера в 1841 году. Все иллюстрации мастерски нарисованы и раскрашены вручную. В те времена легко было по одежде определить, где человек живет, чем занимается и каков его статус. Издательство Manning откликается на новации и инициативы в компьютерной отрасли обложками своих книг, на которых представлено широкое разнообразие местных укладов быта в прошлых веках. Мы возвращаем его в том виде, в каком оно запечатлено на рисунках из таких собраний, как это.

# 1

## Введение

---

Я занимаюсь криптографией больше 50 лет. За это время я очень многому научился. И в этой книге я хочу передать свои знания следующему поколению криптографов. Многие изложенные здесь сведения – новые открытия, которых вы не найдете ни в какой другой литературе.

Я знаю, что на тему криптографии уже написано много книг. И если я хочу, чтобы мою книгу читали, то должен предложить какие-то мысли, которых нет в других книгах, идеи, о которых другие авторы не знают или считают их невозможными. Книга должна стать **СЕНСАЦИЕЙ**. Поехали! Вот что я сделаю:

- расскажу простым нетехническим языком, как построить невскрываемый шифр;
- предложу свыше 140 шифров, готовых к применению. 30 из них невскрываемые;
- снабжу вас инструментарием и методами, позволяющими комбинировать и дополнительно укреплять шифры;
- опишу вычисление, которое позволит точно измерить стойкость шифра и гарантировать, что он невскрываемый;
- покажу, как построить и включить в проект коды, сжимающие данные;
- раскрою практический метод получения невскрываемого шифра с помощью одноразового блокнота;
- расскажу, как генерировать сразу много истинно случайных чисел;

Конец ознакомительного фрагмента.

Приобрести книгу можно

в интернет-магазине

«Электронный универс»

[e-Univers.ru](http://e-Univers.ru)