УДК 003.26
ББК 81.2-8
А28

Адаменко, Михаил Васильевич.
А28 Основы классической криптологии: секреты шифров и кодов / М. В. Адаменко. — 3-е изд., эл. — 1 файл pdf : 297 с. — Москва : ДМК Пресс, 2023. — Систем. требования: Adobe Reader XI либо Adobe Digital Editions 4.5 ; экран 10". — Текст : электронный.

ISBN 978-5-89818-556-5

Предлагаемая книга посвящена вопросам, касающимся истории появления и развития шифров и кодов, а также основам криптографии, криптоанализа и криптологии. Особое внимание уделено особенностям использования кодов и шифров различной степени сложности, которые каждый человек при необходимости может применять в повседневной жизни.

В первой главе в простой и доступной форме разъясняется значение понятий «код» и «шифр», приводятся краткие сведения об основных терминах и определениях, используемых при работе с кодами и шифрами. Во второй и третьей главах коротко изложены наиболее знаменательные и интересные события из истории появления различных кодов, а также из истории криптографии. Советы по использованию наиболее известных кодов даны в четвертой главе. Разделы пятой главы посвящены вопросам практического применения простых шифров в повседневной жизни. Шестая глава содержит специальные упражнения и простые задачи по кодированию и раскодированию, а также по шифрованию сообщений и криптоанализу шифрограмм.

В приложениях приводятся некоторые наиболее часто применяемые в различных областях жизнедеятельности человека коды. Это, в первую очередь, азбука Морзе и азбука Брайля, а также семафорная азбука и флажный код. Причем даны не только русские, но и международные варианты этих кодов.

Все главы и разделы сопровождаются поясняющими рисунками и таблицами, благодаря которым восприятие и усвоение изложенной информации происходит значительно эффективнее.

УДК 003.26
ББК 81.2-8

Электронное издание на основе печатного издания: Основы классической криптологии: секреты шифров и кодов / М.В. Адаменко. — 2-е изд., испр. и доп. — Москва : ДМК Пресс, 2016. — 296 с. — ISBN 978-5-97060-166-2. — Текст : непосредственный.

ISBN 978-5-89818-556-5

Удалено по требованию правообладателя

Содержание

От автора 11

Предисловие 12

Глава 1. Основные понятия и определения 15

1.1. Отрывки из теории информации 15
Информация об информации 16
Преобразование, передача и хранение информации 17
Сообщение, сигнал, система связи 19
1.2. Коды вокруг нас 20
Язык как система звуков и знаков 21
Системы условных обозначений 23
Код, кодирование и декодирование 26
Пароли и ключи 29
1.3. Познакомимся с шифрами 30
Защита информации 31
Шифр, шифрование и дешифрование 33
Различие между шифром и кодом 36
1.4. Наука о шифрах 38
Криптография, криптоанализ, криптология 38
Стойкость шифра. Проверка стойкости 40
Ключ к шифру 42
Выбор шифра 45
1.5. Классические шифры 46
Шифры перестановки 47
Шифры замены 48

Глава 2. История кодов – знаки и время 50

2.1. Первые знаки – первые коды 51
Рисунки, пиктограммы, клинопись 51
Индейские ребусы 53
Иероглифы 54

2.2. Ключ к тайнам Древнего Египта 55
Розеттский камень 55
Разгадка языка древних египтян 57
2.3. Кодированные сигналы 60
Дым, барабан, бочка и корзина 60
Световые сигналы 62
2.4. Сигналы для связи на море 63
Сигнальные флаги и флажки 63
Сигнальные флаги российского флота 64
Международный свод сигналов 66
2.5. Телеграф и азбука Морзе 67
Телеграф 67
Азбука Морзе 68
2.6. Системы кодовых знаков для слепых 71
Азбука Брайля 71
Азбука Муна 73
2.7. Коды в нашей жизни 74
Знаки на дорогах 74
Картинки как коды 75
2.8. Самые распространенные коды современности 77
Компьютерный код 78
Коды в мобильном телефоне 80
Смайлики: просто и забавно 81
Главный код в истории человечества 82

Глава 3. История шифров 85

3.1. Шифры Древней Греции и Римской империи 86
Тайная палочка «Сцитала» 86
Квадрат Полибия 87
Шифр Цезаря 88
3.2. Шифры арабского мира 89
Новые системы шифрования 89
Частотный анализ 90
3.3. Европа просыпается 91
Шифры Темных веков 92
Эпоха Возрождения 92
Первая криптографическая служба в Европе 94

История одного заговора 95
3.4. Многоалфавитные шифры 97
Шифры итальянского архитектора 97
Таинственный монах 98
Шифр Виженера и метод Казисски 99
3.5. Средние века 100
«Черные комнаты» 101
Создатели и взломщики шифров 102
Человек в железной маске 103
Криптография в России 104
3.6. Криптология в XIX веке 105
Старые и новые шифры 105
А. С. Пушкин и А. С. Грибоедов 107
Первые шифровальные механизмы 109
Тайны книг и чисел 111
3.7. XX век начинается 113
Первая мировая война 114
Телеграмма Зиммермана 115
3.8. Шифровальные машины 116
«Энигма» и «Лоренц» 117
Таинственный «Пурпур» 121
«SIGABA» или M-143-C 124
«Type X» 126
3.9. Вторая мировая война 128
Проект «Ultra»: победа над «Энигмой» 128
Говорящие шифром 132
3.10. Итоги XX века 136
Шифры и компьютерные технологии: теория и практика 136
Мобильный телефон: защита от несанкционированного использования и прослушивания 137
Наступление эры компьютеров 140
3.11. Компьютерные алгоритмы шифрования: прошлое, настоящее и возможное будущее 141
Симметричные алгоритмы шифрования 142
Асимметричные алгоритмы шифрования 144
Криптология в будущем 145

Глава 4. Использование кодов 148
4.1. Флажные коды и семафорная азбука 148
Флаги Военно-морского свода сигналов 149
Флажная сигнализация Международного свода сигналов 152
Семафорная азбука 157
4.2. Телеграфная азбука 160
Азбука Морзе 160
Особенности изучения азбуки Морзе 163
4.3. Шрифты для слепых и слабовидящих 165
Азбука Брайля 165
Азбука Муна 167
4.4. SMS-сообщения: коротко и понятно 168
Сокращения в SMS-сообщениях 169
Смайлики 169

Глава 5. Шифры в нашей жизни 171
5.1. Простые шифры перестановки 172
Шифр «Перевернутые группы» 173
Шифр «Перевернутые и случайные группы» 173
Шифр «Вставка в середину» 174
Шифр «Перевернутые пары» 175
Шифр «Сэндвич» 175
5.2. Простые шифры замены 176
Шифр Цезаря 176
Шифр «Замена букв» 177
«Еврейский» шифр 178
Шифр с паролем 179
5.3. Многоалфавитные шифры 180
Шифр Виженера 181
Шифр Гронсфельда 188
5.4. Числовые шифры 190
Простой числовой шифр 190
Шифр гласных букв 191
Календарный шифр 192
5.5. Книжные шифры 196
Простой книжный шифр 196
Усовершенствованный книжный шифр 198

5.6. Тайны решеток и таблиц ... 199
Простая шифровальная таблица ... 200
Таблица с паролем ... 201
Квадрат Полибия ... 205
Шифр «Большой крест» ... 207
5.7. Перестановки в таблицах ... 208
Простая перестановка ... 209
Перестановка с паролем ... 210
Двойная перестановка ... 213
5.8. Магические квадраты ... 216
Простейший магический квадрат ... 216
Индийский квадрат ... 218
Квадрат Эйлера ... 220
Магический квадрат 9×9 ... 220
5.9. Трафареты в системах шифрования ... 221
Простой шифр с трафаретом ... 222
Решетка Кардано ... 223
5.10. Биграммные шифры ... 226
Шифр «Playfair» ... 226
Шифр «Двойной квадрат» ... 228

Глава 6. Коды и шифры в упражнениях и задачах ... 231

6.1. Кодируем сообщения и шифруем открытые тексты ... 232
Упражнения по кодированию сообщений ... 232
Упражнения по шифрованию открытых текстов ... 234
Ответы к упражнениям ... 238
6.2. Задачи для начинающих криптоаналитиков ... 249
Разгадываем кодированные сообщения ... 250
Разгадываем шифрованные сообщения ... 259
Занимательная криптоаналитика ... 265
Подсказки к задачам и заданиям ... 267
Ответы к задачам и заданиям ... 268

Приложения ... 272

Приложение 1. Флажный код Военно-морского свода сигналов ... 272
Флаги Военно-морского свода сигналов ... 272

Цифровые флаги Военно-морского свода сигналов 274
Дополнительные и специальные флаги Военно-морского свода сигналов 275
Значения некоторых флагов Военно-морского свода сигналов 276
Приложение 2. Флажный код Международного свода сигналов ... 277
Флаги Международного свода сигналов 277
Цифровые флаги Международного свода сигналов 278
Заменяющие флаги Международного свода сигналов 279
Значения некоторых флагов Международного свода сигналов 280
Приложение 3. Семафорная азбука 281
Русская семафорная азбука 281
Международная семафорная азбука 282
Знаки азбуки Морзе, передаваемые семафорной азбукой 283
Приложение 4. Азбука Морзе 284
Русская азбука Морзе 284
Цифры в русской азбуке Морзе 285
Обозначения флагов азбукой Морзе 286
Международная азбука Морзе 287
Цифры в Международном своде сигналов 288
Приложение 5. Азбука Брайля и азбука Муна 289
Азбука Брайля для русского языка 289
Международная азбука Брайля 290
Международная азбука Муна 291
Приложение 6. Сокращения и смайлики 292
Перечень сокращений в SMS-сообщениях 292
Смайлики 293
Приложение 7. Передача букв русского алфавита латинскими буквами 295