

Сергей Панасенко

АЛГОРИТМЫ ШИФРОВАНИЯ

специальный
справочник

Санкт-Петербург

«БХВ-Петербург»

2009

УДК 681.3.06
ББК 32.973.26-018.2
П16

Панасенко С. П.

П16 Алгоритмы шифрования. Специальный справочник. —
СПб.: БХВ-Петербург, 2009. — 576 с.: ил.

ISBN 978-5-9775-0319-8

Книга посвящена алгоритмам блочного симметричного шифрования. Дана общая классификация криптографических алгоритмов. Рассмотрено более 50 алгоритмов шифрования: история создания и использования, основные характеристики и структура, достоинства и недостатки. Описаны различные виды криптоаналитических атак на алгоритмы шифрования и на их реализации в виде программных или аппаратных шифраторов. Рассказано о конкурсах по выбору стандартов шифрования США и Евросоюза.

*Для специалистов в области информационных технологий,
преподавателей, студентов и аспирантов*

УДК 681.3.06
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	<i>Екатерина Кондукова</i>
Зам. главного редактора	<i>Игорь Шишигин</i>
Зав. редакцией	<i>Григорий Добин</i>
Редактор	<i>Ирина Иноземцева</i>
Компьютерная верстка	<i>Натали Каравасовой</i>
Корректор	<i>Наталия Першакова</i>
Дизайн обложки	<i>Елены Беляевой</i>
Зав. производством	<i>Николай Тверских</i>

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 24.10.08.
Формат 70×100^{1/16}. Печать офсетная. Усл. печ. л. 46,44.
Тираж 2000 экз. Заказ №
"БХВ-Петербург", 194354, Санкт-Петербург, ул. Есенина, 5Б.
Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12

ISBN 978-5-9775-0319-8

© Панасенко С. П., 2008
© Оформление, издательство "БХВ-Петербург", 2008

Оглавление

Введение	1
Глава 1. Классификация алгоритмов шифрования и методов их вскрытия	3
1.1. Криптографические алгоритмы	3
1.2. Категории алгоритмов шифрования.....	7
1.3. Структура алгоритмов симметричного шифрования	8
Алгоритмы на основе сети Фейстеля	9
Алгоритмы на основе подстановочно-перестановочных сетей	11
Алгоритмы со структурой «квадрат».....	11
Алгоритмы с нестандартной структурой	12
1.4. Режимы работы алгоритмов.....	12
Электронная кодовая книга	13
Сцепление блоков шифра	14
Обратная связь по шифртексту	15
Обратная связь по выходу	16
Другие режимы работы.....	18
1.5. Атаки на алгоритмы шифрования	18
Цели атак	18
Классификация атак	19
Количественная оценка криптостойкости алгоритмов шифрования	21
Криптоанализ модифицированных алгоритмов	22
1.6. Криптоаналитические методы, используемые в атаках	23
Метод «грубой силы».....	23
Атаки класса «встреча посередине»	25
Дифференциальный криптоанализ	27
Линейный криптоанализ	34
Метод бумеранга	38
Сдвиговая атака	40

Метод интерполяции	42
Невозможные дифференциалы	43
Заключение.....	44
1.7. Атаки на шифраторы, использующие утечку данных	
по побочным каналам	44
Атака по времени выполнения	45
Атаки по потребляемой мощности	46
Другие пассивные атаки	47
1.8. Активные атаки на шифраторы, использующие утечку данных	
по побочным каналам	48
Виды воздействий на шифратор	48
Дифференциальный анализ на основе сбоев	50
Противодействие активным атакам	52
1.9. Криптоаналитические атаки на связанных ключах	53
Расширение ключа.....	53
«Классическая» атака на связанных ключах.....	54
Атакуемые алгоритмы.....	57
Другие возможные проблемы процедуры расширения ключа	59
Глава 2. Новейшая история симметричного шифрования	61
2.1. Конкурс AES.....	61
Алгоритмы — участники конкурса	63
Достоинства и недостатки алгоритмов-финалистов	65
2.2. Конкурс NESSIE.....	69
Глава 3. Описание алгоритмов	73
3.1. Алгоритм ГОСТ 28147-89	73
Описание алгоритма.....	73
Режимы работы алгоритма	75
Криптостойкость алгоритма	79
Анализ таблиц замен	79
Модификации алгоритма и их анализ	80
Анализ полнораундового алгоритма	81
Заключение.....	81
3.2. Алгоритм Aardvark.....	82
3.3. Алгоритм AES (Rijndael).....	84
Структура алгоритма.....	84
Процедура расширения ключа	88
Расшифровывание	89

Отличия AES от исходного алгоритма Rijndael	91
Первичная оценка криптостойкости алгоритма Rijndael.....	92
Криптоанализ алгоритма Rijndael в рамках конкурса AES	93
Криптоанализ алгоритма после конкурса AES.....	95
Заключение.....	97
3.4. Алгоритм Akelarre	97
Структура алгоритма	98
Процедура расширения ключа	101
Криптоанализ алгоритма.....	102
3.5. Алгоритм Anubis	103
Структура алгоритма	103
Процедура расширения ключа	107
Достоинства и недостатки алгоритма.....	108
3.6. Алгоритмы Bear, Lion и Lioness	108
Алгоритм Bear.....	109
Алгоритм Lion.....	111
Алгоритм Lioness.....	112
Варианты использования	113
Криптоанализ алгоритмов	114
3.7. Алгоритмы BEAST и BEAST-RK.....	114
Криптостойкость алгоритма BEAST	116
Алгоритм BEAST-RK.....	117
3.8. Алгоритм Blowfish	118
Структура алгоритма.....	119
Процедура расширения ключа	121
Достоинства и недостатки алгоритма.....	122
3.9. Алгоритм Camellia	123
Структура алгоритма.....	123
Таблицы замен	127
Расшифровывание	128
Процедура расширения ключа	129
Криптоанализ алгоритма Camellia	132
3.10. Алгоритм CAST-128	134
3.11. Алгоритм CAST-256	135
Основные характеристики и структура алгоритма	135
Процедура расширения ключа	139
Достоинства и недостатки алгоритма.....	141
3.12. Алгоритм Crypton.....	141
Основные характеристики и структура алгоритма	141

Процедура расширения ключа	145
Достоинства и недостатки алгоритма.....	147
3.13. CS-Cipher.....	148
Структура алгоритма.....	149
Расшифровывание	153
Процедура расширения ключа	154
Достоинства и недостатки алгоритма.....	155
3.14. Алгоритм DEAL	156
Основные характеристики и структура алгоритма	156
Процедура расширения ключа	157
Достоинства и недостатки алгоритма.....	160
3.15. Алгоритм DES и его варианты.....	160
История создания алгоритма	161
Основные характеристики и структура алгоритма	162
Процедура расширения ключа	166
Криптостойкость алгоритма DES	168
Продолжение истории алгоритма	171
Алгоритм Double DES	172
Алгоритм 2-key Triple DES.....	173
Алгоритм 3-key Triple DES.....	174
Режимы работы Double DES и Triple DES	175
Режимы работы с маскированием.....	178
Алгоритм Quadruple DES.....	181
Алгоритм Ladder-DES	181
Алгоритм DESX.....	184
Алгоритм DES с независимыми ключами раундов.....	185
Алгоритм GDES	186
Алгоритм RDES	188
Алгоритмы s^2 DES, s^3 DES и s^5 DES	190
Алгоритм Biham-DES	191
Алгоритмы $xDES^1$ и $xDES^2$	193
Другие варианты алгоритма DES.....	195
Заключение.....	195
3.16. Алгоритм DFC	195
Основные характеристики и структура алгоритма	195
Процедура расширения ключа	198
Достоинства и недостатки алгоритма.....	199
3.17. Алгоритм E2	201
Структура алгоритма.....	201
Почему алгоритм E2 не вышел в финал конкурса AES.....	206

3.18. Алгоритм FEAL	206
История создания алгоритма	206
Структура алгоритма	207
Процедура расширения ключа	209
Почему FEAL не используется	211
3.19. Алгоритм FROG	212
Основные характеристики и структура алгоритма	212
Процедура расширения ключа	214
Форматирование ключа	216
Достоинства и недостатки алгоритма	218
3.20. Алгоритм Grand Cru	219
Структура алгоритма	219
Расшифровывание	225
Процедура расширения ключа	226
Достоинства и недостатки алгоритма	229
3.21. Алгоритм Hierocrypt-L1	229
Структура алгоритма	229
Процедура расширения ключа	234
Достоинства и недостатки алгоритма	239
3.22. Алгоритм Hierocrypt-3	239
Отличия от Hierocrypt-L1	239
Процедура расширения ключа	241
Криптоанализ алгоритма	246
3.23. Алгоритм HPC	246
Основные характеристики алгоритма	246
Структура раунда	247
Процедура расширения ключа	250
Достоинства и недостатки алгоритма	253
3.24. Алгоритм ICE	254
История создания алгоритма	254
Структура алгоритма	254
Варианты алгоритма	257
Процедура расширения ключа	257
Криптоанализ алгоритма	259
3.25. Алгоритм ICEBERG	259
Структура алгоритма	259
Процедура расширения ключа	263
Криптоанализ алгоритма	265

3.26. Алгоритмы IDEA, PES, IPES.....	265
Основные характеристики и структура.....	266
Процедура расширения ключа.....	268
Криптостойкость алгоритма.....	268
3.27. Алгоритм KASUMI.....	270
Структура алгоритма.....	271
Процедура расширения ключа.....	275
Использование алгоритма.....	277
Криптоанализ алгоритма.....	279
3.28. Алгоритм Khazad.....	282
Структура алгоритма.....	282
Процедура расширения ключа.....	284
Модификация алгоритма.....	285
Криптоанализ алгоритма Khazad.....	287
3.29. Алгоритмы Khufu и Khafre.....	288
История создания алгоритмов.....	288
Структура алгоритма Khufu.....	289
Процедура расширения ключа и таблицы замен.....	290
Алгоритм Khafre.....	292
Сравнение алгоритмов.....	293
Алгоритм Snefru.....	294
Криптоанализ алгоритмов.....	294
3.30. Алгоритм LOKI97.....	295
История создания алгоритма.....	295
Основные характеристики и структура алгоритма.....	296
Процедура расширения ключа.....	299
Почему LOKI97 не вышел в финал конкурса AES.....	300
3.31. Алгоритм Lucifer.....	301
Вариант № 1.....	301
Вариант № 2.....	304
Вариант № 3.....	308
Вариант № 4.....	310
Криптоанализ вариантов алгоритма.....	311
3.32. Алгоритм MacGuffin.....	312
Структура алгоритма.....	313
Процедура расширения ключа.....	315
Криптоанализ алгоритма.....	316
3.33. Алгоритм MAGENTA.....	316
Структура алгоритма.....	317
Достоинства и недостатки алгоритма.....	319

3.34. Алгоритм MARS.....	319
Структура алгоритма.....	320
Процедура расширения ключа	326
Достоинства и недостатки алгоритма.....	328
3.35. Алгоритм Mercy	328
Структура алгоритма.....	328
Процедура расширения ключа	333
Криптостойкость алгоритма	334
3.36. Алгоритмы MISTY1 и MISTY2	334
Структура алгоритма MISTY1	334
Расшифровывание	342
Процедура расширения ключа	344
Алгоритм MISTY2.....	345
Алгоритм KASUMI.....	346
Криптоанализ алгоритмов MISTY1 и MISTY2.....	347
3.37. Алгоритм Nimbus	348
Структура алгоритма.....	348
Процедура расширения ключа	349
Достоинства и недостатки алгоритма.....	351
3.38. Алгоритм Noekeon	351
Структура алгоритма.....	352
Расшифровывание	356
Процедура расширения ключа	357
Криптоанализ алгоритма.....	357
3.39. Алгоритм NUSH.....	357
Структура алгоритма.....	357
Расшифровывание	362
Процедура расширения ключа	363
Криптостойкость алгоритма	363
128-битный вариант.....	364
256-битный вариант.....	368
Криптоанализ 128- и 256-битного вариантов алгоритма.....	373
3.40. Алгоритм Q.....	374
Структура алгоритма.....	374
Криптоанализ алгоритма.....	375
3.41. Алгоритм RC2.....	375
Структура алгоритма.....	376
Процедура расширения ключа	378
Расшифрование.....	380
Криптостойкость алгоритма	381

3.42. Алгоритм RC5.....	381
Структура алгоритма.....	382
Процедура расширения ключа	385
Криптоанализ алгоритма.....	386
Варианты RC5	387
Продолжение истории алгоритма	390
3.43. Алгоритм RC6.....	391
Структура алгоритма.....	391
Процедура расширения ключа	393
Достоинства и недостатки алгоритма.....	394
3.44. Алгоритмы SAFER K и SAFER SK	394
Структура алгоритма SAFER K-64	395
Расшифрование.....	399
Процедура расширения ключа	400
Криптоанализ алгоритма SAFER K-64	402
Алгоритм SAFER K-128.....	403
Алгоритмы SAFER SK-64, SAFER SK-128 и SAFER SK-40	404
Криптоанализ алгоритмов SAFER SK-64 и SAFER SK-128.....	408
3.45. Алгоритм SAFER+	408
Структура алгоритма.....	408
Расшифрование.....	412
Процедура расширения ключа	413
Криптоанализ алгоритма SAFER+	415
Единое расширение ключа SAFER+.....	416
3.46. Алгоритм SAFER++.....	418
Структура алгоритма.....	418
64-битный вариант SAFER++.....	421
Криптоанализ алгоритма SAFER++.....	423
Заключение.....	424
3.47. Алгоритм SC2000	424
Структура алгоритма.....	424
Расшифрование.....	428
Процедура расширения ключа	429
Криптоанализ алгоритма.....	432
3.48. Алгоритм SERPENT.....	432
Структура алгоритма.....	433
Расшифрование.....	439

Процедура расширения ключа	441
Криптостойкость алгоритма	442
3.49. Алгоритм SHACAL	442
Алгоритм SHACAL-1	442
Алгоритм SHACAL-0	445
Алгоритм SHACAL-2	446
Криптоанализ алгоритма SHACAL-1	449
Криптоанализ алгоритма SHACAL-2	450
3.50. Алгоритмы SHARK и SHARK*	451
3.51. Алгоритм Sha-zam	454
Структура алгоритма	454
Процедура расширения ключа	456
Криптостойкость алгоритма	456
3.52. Алгоритм Skipjack	457
Структура алгоритма	457
Криптостойкость алгоритма	461
3.53. Алгоритм SPEED	462
Структура алгоритма	462
Расшифровывание	465
Процедура расширения ключа	466
Достоинства и недостатки алгоритма	468
3.54. Алгоритм Square	469
Структура алгоритма	469
Процедура расширения ключа	472
Криптостойкость алгоритма	473
3.55. Алгоритмы TEA, XTEA и их варианты	474
Алгоритм TEA	474
Криптоанализ алгоритма TEA	476
Алгоритм XTEA	478
Криптоанализ алгоритма XTEA	480
Алгоритм Block TEA	480
Алгоритм XXTEA	481
3.56. Алгоритмы Twofish и Twofish-FK	483
Структура алгоритма	483
Процедура расширения ключа	486
Алгоритм Twofish-FK	491
Достоинства и недостатки алгоритма	492

Приложение. Таблицы замен.....	493
П1. Алгоритм Blowfish	493
П2. Алгоритм Camellia.....	498
П3. Алгоритм CAST-128.....	500
П4. Алгоритм CAST-256.....	510
П5. Алгоритм Crypton 0.....	515
П6. Алгоритм DES	517
П7. Алгоритм KASUMI	519
П8. Алгоритм MARS.....	522
П9. Алгоритм s^2 DES.....	525
П10. Алгоритм s^3 DES.....	527
П11. Алгоритм s^5 DES.....	529
Литература	531