

Секция «Прикладная дискретная математика»

ДАМЕН Й., РЭМЕН В.

РАЗРАБОТКА RIJNDAEL:

**AES — ПЕРСПЕКТИВНЫЙ СТАНДАРТ
ШИФРОВАНИЯ¹⁾**

Содержание

Вступительное слово	98
Предисловие	100
Глава 1. Процесс разработки и принятия перспективного стандарта шифрования (AES)	103
§ 1.1. В самом начале	103
§ 1.2. AES: границы применения и значение	104
§ 1.3. Начальный этап конкурса AES.	104
§ 1.4. Первый тур	107
§ 1.5. Критерии оценки	107
1.5.1. Стойкость	107
1.5.2. Стоимость	107
1.5.3. Характеристики удобства и эффективности реализации алгоритма	108
§ 1.6. Выбор пяти финалистов	108
1.6.1. Вторая конференция конкурса AES	109
1.6.2. Пять финалистов	110
§ 1.7. Второй раунд	110
§ 1.7. Выбор победителя	111
Глава 2. Начальные сведения	112
§ 2.1. Конечные поля	113
2.1.1. Группы, кольца, поля	113
2.1.2. Векторные пространства	115
2.1.3. Конечные поля	116
2.1.4. Многочлены над полем	117
2.1.5. Операции с многочленами	118
2.1.6. Многочлены и байты	119
2.1.7. Многочлены и векторы-столбцы	120

© Редакция журнала «ОПиМ» и Научное издательство «ТВП», перевод на русский язык с разрешения Springer-Verlag — владельца прав на издание оригинала. 2016 г.

¹⁾ От Редакции. Начинаем публикацию журнальной редакции перевода И. В. Харламова на русский язык книги «Разработка Rijndael: AES — перспективный стандарт шифрования». Запланировано, что после завершения публикации журнальной редакции будет осуществлено издание полного перевода в форме защищенной от копирования π -книги (Портативной Интерактивной книги), а впоследствии Редакция намерена издать ее как очередную том в серии «Прогресс теоретической и прикладной дискретной математики».

Начатая в данном выпуске вводными гл. 1 и 2, публикация будет продолжена в выпусках (Продолжение примечания см. на с. 98.)

§ 2.2. Линейные коды	121
2.2.1. Определения	121
2.2.2. MDS-коды	122
§ 2.3. Булевы функции	123
2.3.1. Разбиение на блоки	124
2.3.2. Транспозиции	125
2.3.3. Блочные отображения	126
2.3.4. Итеративные булевы преобразования	127
§ 2.4. Блочные шифры	127
2.4.1. Итеративные блочные шифры	128
2.4.2. Блочные шифры с чередующимся прибавлением ключа	129
§ 2.5. Режимы использования блочных шифров	131
2.5.1. Режимы блочного шифрования	131
2.5.2. Режимы выработки блочной гаммы	132
2.5.3. Режимы выработки имитовставки	133
2.5.4. Криптографическое хеширование	134
§ 2.6. Заключение	134
Список литературы к гл. 1 и 2	134