ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
МАТЕМАТИКИ
Том 23 Выпуск 4
2016

Секция **«Прикладная дискретная математика»**

ДАМЕН Й., РЭМЕН В.

РАЗРАБОТКА RIJNDAEL: AES — ПЕРСПЕКТИВНЫЙ СТАНДАРТ ШИФРОВАНИЯ [1)]

Содержание

[1)] От Редакции. Продолжаем 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 (*П*ортативной *И*нтерактивной книги), а впоследствии Редакция намерена издать ее как очередной том в серии «Прогресс теоретической и прикладной дискретной математики».

(Продолжение примечания см. на с. 290.)

Начатая во втором выпуске этого года вводными «Гл. 1. Процесс разработки и принятия перспективного стандарта шифрования (AES)» и «Гл. 2. Начальные сведения» и продолженная в третьем выпуске тома 23 (2016) («Гл. 3. Описание алгоритма Rijndael», «Гл. 4. Вопросы реализации», «Гл. 5. Принципы конструирования», «Гл. 6. Стандарт шифрования данных (DES)»), публикация будет далее продолжена в выпусках 4 и 6 («Гл. 8. Разностные соотношения» и «Гл. 9. Стратегия «широкого хвоста»»), и в первом выпуске тома 24 (2017) («Гл. 10. Результаты криптоанализа» и «Гл. 11. Родственные блочные шифры»).

Издание каждого отрывка книги сопровождается списком упомянутых в ней литературных источников.