

УДК 519.1(075.8)
ББК 22.176
Ж85

Рецензенты: *М.А. Басараб, С.В. Запечников*

Жуков А. Е.

Ж85 Системы блочного шифрования: учеб. пособие по курсу «Криптографические методы защиты информации» / А. Е. Жуков. — М.: Изд-во МГТУ им. Н. Э. Баумана, 2013. — 77, [3] с.: ил.

ISBN 978-5-7038-3753-5

Рассмотрены основные понятия, используемые для описания работы блочных шифров, примеры типовых узлов, входящих в их конструкцию, а также наиболее распространенные схемы построения блочных шифров. Для большинства вводимых терминов приведены соответствующие англоязычные эквиваленты.

Для студентов кафедры ИУ-8 МГТУ им. Н.Э. Баумана, изучающих курс «Криптографические методы защиты информации».

УДК 519.1(075.8)
ББК 22.176

ОГЛАВЛЕНИЕ

Глава 1. Основные понятия и определения криптографии	3
Однонаправленные функции	4
Обратимые криптографические преобразования	4
Необратимые криптографические преобразования	7
Криптографические генераторы псевдослучайных последовательностей	8
Криптографические примитивы	9
Модели нарушителя. Классификация криптографических атак ..	11
Глава 2. Блочные шифры. Основные определения	14
Математическая модель блочного шифра	15
Основные узлы блочных шифров	17
Глава 3. Основные схемы блочных шифров	21
SP-сети	21
Схемы Фейстеля	22
Обобщения схемы Фейстеля	24
Схема Лая — Месси	28
Глава 4. Стандарт США DES	30
Общие сведения	30
Алгоритм шифрования	32
Алгоритм выработки цикловых ключей	37
Алгоритм расшифрования	39
Режимы работы алгоритма DES	39
Глава 5. Стандарт СССР и РФ ГОСТ 28147–89	44
Алгоритм шифрования	44
Алгоритм выработки цикловых ключей	47
Режимы работы алгоритма ГОСТ	47
	77

Глава 6. Стандарт США AES (Rijndael):	51
Общие сведения	51
Структура шифра	52
Алгоритм выработки цикловых ключей (Key Schedule)	57
Процедура шифрования	61
Задачи	62
Литература	64
Словарь используемых терминов и выражений	66