

Содержание

Предисловие автора ко 2-му изданию	5
Введение	7
Лекция 1. Платформы шифрования	10
Лекция 2. Модулярная арифметика	18
Лекция 3. Элементы шифрования	28
Лекция 4. Элементы криптоанализа	37
Лекция 5. Модели систем шифрования	45
Лекция 6. Простейшие шифры	55
Лекция 7. Группы	69
Лекция 8. Конечные поля	76
Лекция 9. Дискретный логарифм	83
Лекция 10. Криптосистема с открытым ключом	
Ривеста – Шамира – Адлемана	96
Лекция 11. Простые числа	112
Лекция 12. Разложимость целых чисел на множители	122
Лекция 13. Алгоритмы генерации псевдослучайных последовательностей	130
Лекция 14. Поточные криптосистемы	136
Лекция 15. Идентификация и аутентификация	143
Лекция 16. Электронные подписи	151
Лекция 17. Электронные платежи	161
Лекция 18. Управление ключами	170
Лекция 19. Эллиптические кривые	175
Лекция 20. Криптография, основанная на эллиптических кривых	183
Лекция 21. Алгебраическое шифрование	188
Приложение 1. Стандарт шифрования DES	193
Приложение 2. Стандарты электронной подписи	209
Приложение 3. Стандарт шифрования AES	217

Приложение 4. Практическое использование криптографии	226
Послесловие	231
Литература	233
Предметный указатель	235