

Бабаш, Александр Владимирович.

Криптографические методы защиты информации : учебник/ А.В. Бабаш, Е.К. Баранова. — Москва: КНОРУС, 2024. — 192 с. — (Бакалавриат и магистратура).

ОГЛАВЛЕНИЕ

Предисловие	5
Глава 1. Математические основы криптографии.....	7
1.1. Операции над множествами	
1.2. Отображение множеств	12
1.3. Мощность множеств	14
1.4. Отношения на множествах	16
Тест к главе 1.	20
Глава 2. Эволюция симметричного шифрования	25
2.1. Классические шифры	25
2.2. Основные понятия теории классических шифров	35
2.3. Особенности построения блочных шифров	47
2.4. Блочный шифр DES	51
2.5. Отечественный стандарт шифрования данных	65
Тест к главе 2.	76
Глава 3. Элементы криптоанализа классических шифров	81
3.1. Открытые сообщения и их простейшие характеристики	81
3.2. Дешифрование некоторых классических шифров	85
3.3. Типовые задачи криптоанализа	98
3.4. Теоретическая и практическая стойкость шифров	99
3.5. Имитостойкость шифров в модели К. Шеннона	103
Тест к главе 3.	105
Глава 4. Основы асимметричного шифрования	109
4.1. Модулярная арифметика	109
4.2. Алгоритм Евклида для нахождения наибольшего общего делителя	110
4.3. Вычисления в конечных полях	115
4.4. Схема асимметричного шифрования	116
4.5. Алгоритм Диффи — Хеллмана	117
4.6. Алгоритм RSA	118
4.7. Схема шифрования Эль Гамала	122
4.8. Схема шифрования Полига — Хеллмана	124
Тест к главе 4.	125

Глава 5. Идентификация и аутентификация. Управление криптографическими ключами.	.128
5.1. Идентификация и аутентификация.	.128
5.2. Управление криптографическими ключами.	.131
Тест к главе 5.	.147
Глава 6. Электронная подпись.	.151
6.1. Процедуры постановки и проверки подписи.	.151
6.2. Хэш-функции.	.152
6.3. Алгоритм цифровой подписи RSA.	.162
6.4. Алгоритм цифровой подписи Эль Гамала.	.165
6.5. Алгоритм цифровой подписи DSA.	.167
6.6. Цифровые подписи с дополнительными функциональными свойствами.	.171
Тест к главе 6.	.174
Литература	.179
Приложение 1	.181
Приложение 2	.186