

Глава 13. Функции хэширования	305
13.1. Определение и свойства	305
13.2. Блочнo-итерационные функции хэширования	306
13.3. Использование блочных криптосистем	306
13.4. Атака «дней рождения»	307
13.5. Криптосистемы аутентификации	309
13.6. Функция хэширования СТБ 1176.1—99	309
13.7. Задания	313
Глава 14. Электронная цифровая подпись	315
14.1. Обобщенная модель ЭЦП	315
14.2. Схема ЭЦП Рабина	317
14.3. Схема Диффи — Лампорта	318
14.4. Вероятностная схема подписи Рабина	319
14.5. Стандарт ЭЦП DSS	320
14.6. Схема ЭЦП Эль-Гамала	322
14.7. Арифметические свойства российского стандарта цифровой подписи	323
14.8. Эквивалентность задач фальсификации подписи в DSS и схеме Эль-Гамала	329
14.9. Электронная цифровая подпись СТБ 1176.2—99	330
14.10. Задача дискретного логарифмирования	332
14.11. Задания	333
Глава 15. Эллиптические кривые в криптографии	335
15.1. Цифровая подпись на эллиптических кривых	335
15.2. Особенности скалярного умножения на эллиптических кривых ..	338
15.3. Вычисление порядка эллиптической кривой	338
15.4. Задания	341
Глава 16. Протоколы управления криптографическими ключами	343
16.1. Протоколы генерации ключей	343
16.2. Протоколы взаимной аутентификации	344
16.3. Протоколы прямого обмена ключами	346
16.4. Протоколы распределения сеансовых ключей с использованием центра распределения ключей	348
Глава 17. Новые направления в криптологии	351
17.1. Возможности квантовой криптографии	351
17.2. Математическое разделение секрета	354
17.3. Стеганография и ее применение	356
17.4. Активный криптоанализ	358