|  |
| --- |
| 1. Основные свойства криптосистемы. Классификация атак на криптосистему с секретным ключом. 2. Основные понятия криптографии. Блочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Основные требования к шифрам. 3. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Одноалфавитные и многоалфавитные, шифры замены. 4. Принципы построения криптографических алгоритмов. Криптографическая стойкость шифров. Имитация и подмена сообщения. Характеристика имитостойкости шифров 5. Поточные и блочные шифры. Принципы блочного шифрования. Шифр Файстеля. 6. Режимы работы блочных шифров. Область применения. Достоинства и недостатки. 7. Стандарт шифрования данных (DES). Шифрование и дешифрование DES. 8. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». Логика построения шифра и структура ключевой информации. 9. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». Базовые циклы преобразования. 10. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». Основной шаг криптопреобразования. 11. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». Цикл выработки имитовставки. 12. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» Основные режимы шифрования. 13. ГОСТ 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры». Логика построения шифра и структура ключевой информации 14. Код аутентичности сообщения: требования, область применения, методы получения кода аутентичности (имитовставки). 15. Хэш-функция: классификация, свойства и требования, предъявляемые к хэш-функциям. 16. Гост 34.11- 94 «Информационная технология. Криптографическая защита информации. Функция хэширования». 17. Сравнение алгоритмов хеширования: MD5, SHA-3, RIPEMD-160, ГОСТ 34.11-94 18. Электронная подпись: требования предъявляемы к электронной подписи, непосредственная и арбитражная цифровая подпись. 19. Электронная подпись на основе задачи дискретного логарифмирования 20. Электронная подпись. Подход RSA и DSS. Гост 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки. 21. ФЗ №63 «Об электронной подписи». Использование простой электронной подписи. Признание квалифицированной электронной подписи. 22. ФЗ №63 «Об электронной подписи». Функции удостоверяющего центра. 23. ФЗ №63 «Об электронной подписи». Сертификат ключа проверки электронной подписи. Сертификаты открытых ключей. Распределение сертификатов открытых ключей. 24. ФЗ №63 «Об электронной подписи» Принципы использования электронной подписи. виды электронной подписи. Условия признания документов, подписанных электронной подписью, равнозначными на бумажном носителе, подписанным собственноручной подписью. 25. Криптографические функции аутентификации. 26. Традиционная криптография и криптография с открытым ключом: область использования, достоинства и недостатки. Требования, предьявляемые к алгоритмам шифрования 27. Криптосистемы с открытым ключом. Криптосистемы RSA и Эль-Гамаля. 28. Методы получения случайных и псевдослучайных последовательностей. 29. Потоковые шифры на основе РСЛОС. Генератор Геффе, «старт-стоп» Бета-Пайпера. Пороговый генератор. 30. Линейные конгруэнтные генераторы. Регистры с обратной линейной связью. Линейная сложность. Корреляционная стойкость. 31. Криптография в стандарте GSM. Алгоритм аутентификации А8 и алгоритм генерации ключа шифрования А3. 32. Криптография в стандарте GSM. Поточный алгоритм шифрования A5/х 33. Ключевая информация: сеансовый, секретный, мастер-ключ, открытый и закрытый ключ. Требования к качеству ключевой информации и источнику ключей 34. Распределение секретных ключей. Подход на основе алгоритма традиционного шифрования. Продолжительность использования сеансового ключа. 35. Распределение секретных ключей. Обмен ключами по Диффи-Хельмана. 36. Распределение сеансовых ключей по протоколу Kerberos. 37. Простой и защищенный протокол аутентификации (Kerberos) 38. Взаимосвязь между протоколами аутентификации и цифровой подписи. 39. Методы криптоанализа. Понятие криптоатаки. Классификация криптоатак. Классификация методов анализа криптографических алгоритмов. |