Основы криптографии.ти

1. Одна из целей поддержки информационной безопасности, означающая, что все изменения информации должны быть сделаны только разрешенными объектами и с помощью разрешенных механизмов:
2. Атаки, угрожающие конфиденциальности информации:
3. Атаки, угрожающие готовности информации:
4. Активные нападения:
5. Механизмы обеспечения безопасности услуги «Исключение отказа от сообщения»:
6. Современные блочные шифры:
7. n-разрядный блочный шифр подстановки может быть смоделирован как шифр перестановки с длиной ключа:
8. Особенности S-блоков (блоков подстановки) с n-входами и m-выходами:
9. Отбеливание - процесс проведения операции, которая
10. Одна из целей поддержки информационной безопасности, требующая сохранения секретности важной информации:
11. Одна из целей поддержки информационной безопасности, означающая, что информация, созданная и сохраненная организацией, должна быть доступна разрешенным объектам
12. Атаки, угрожающие целостности информации:
13. Пассивные нападения:
14. Методы, которые используются в настоящее время для шифрования данных:
15. Криптография с секретным ключом:
16. Механизм хэширования заключается в том, что

17 Стеганография

18 Атака криптоанализа, использующая некоторые характеристики, свойственные языку исходного текста:

19 Традиционные шифры с симметричным ключом разделяются на категории:

20 Моноалфавитный аддитивный шифр иногда называют, как

21 Максимальное множество возможных ключей аддитивного шифра

22 Особенности использования моноалфавитных шифров:

23 Особенности использования многоалфавитных шифров:

24 В многоалфавитном шифре каждый символ зашифрованного текста

25 Поток ключей шифра Виженера:

26 Шифр «Одноразовый блокнот»:

27 Роторный шифр - это

28 Шифр изгороди - это

29 Шифры потока:

30 Блочные шифры:

31 Особенности шифрования симметричными ключами:

32 Моноалфавитные шифры включают в себя:

33 Многоалфавитные шифры включают в себя:

34 В каком шифре шифрование и дешифрование одного символа производятся в один момент времени:

35 Современные блочные шифры с симметричным ключом:

36 n-разрядный шифр транспозиции может быть смоделирован как шифр перестановки с длиной ключа:

37 Прямой P-блок шифра транспозиции с n-входами и m-выходами:

38 P-блок расширения шифра транспозиции с n-входами и m-выходами

39 Свойства составного шифра:

40 Современные составные блочные шифры, использующие только обратимые компоненты:

41 В синхронном шифре потока ключ:

42 Шифр одноразового блокнота:

43 Максимальный период последовательностей длиной m, которые генерируются с помощью линейного регистра сдвига с обратной связью, равен:

44 Режимы работы для блочных шифров:

45 В несинхронном шифре потока ключ:

46 Длина ключа для стандарта шифрования данных DES составляет:

47 Процесс DES-шифрования состоит из:

48 Начальные и конечные перестановки в блочном шифре с симметричными ключами DES:

49 Два желательных свойства блочного шифра DES:

50 Слабые ключи блочного шифра DES:

51 Полуслабые ключи блочного шифра DES:

52 Возможно слабые ключи блочного шифра DES:

53 Кластерный ключ блочного шифра DES:

54 При использовании атаки знания исходного текста двукратный блочный шифр DES увеличивает устойчивость по испытаниям до

55 Размер ключа стандарта шифрования AES с 12 раундами:

56 Операция подстановка в стандарте шифрования AES:

57 Операция перестановка в стандарте шифрования AES:

58 Стандарт AES:

59 При реализации стандарта AES в ориентированной на слово версии алгоритм может использовать процессор на: