ПЕРЕЛІК ПИТАНЬ ДО ЗАЛІКУ

1.Криптографія: етапи історичного розвитку.

2. Класичні техніки шифрування: шифри перестановок.

3. Класичні техніки шифрування: шифри підстановок.

4. Елементи теорії зв’язку в секретних системах: основні положення роботи Клода Шеннона.

5. Класифікація сучасних криптосистем.

6. Вимоги до сучасних криптосистем.

7. Комбіновані криптосистеми.

8. Шифрувальна система на основі шифру Цезаря.

9. Шифрувальна система на основі шифру простої заміни.

10. Дослідження афінної системи шифрування Цезаря.

11. Шифрувальна систем на основі шифру гамування.

12. Симетричні криптосистеми: блокові шифри.

13. Особливості стандарту DES.

14. Опис алгоритму DES.

15. Стійкість алгоритму DES.

16. Модифікації алгоритму DES (3DES, DESX, S-DES).

17. Особливості стандарту ГОСТ 28147-89.

18. Порівняння криптостійкості DES та ГОСТу.

19. Режим застосування блокових шифрів.

20. Міжнародний стандарт шифрування даних IDEA.

21. Особливості стандарту AES.

22. Симетричні криптосистеми: потокові шифри.

23. Алгоритм потокового шифру RC4.

24. Асиметричні криптосистеми: елементи теорії чисел.

25. Криптосистема RSA.

26. Криптостійкість RSA.

27. Криптосистема Ель-Гамаля.
28. Електронний цифровий підпис: загальна схема.
29. Електронний цифровий підпис: функції хешування.
30. Алгоритм хешування сімейства MD (MD2, MD4-MD5).
31. Алгоритм хешування SHA-1.
32. Алгоритм цифрового підпису DSA.
33. Стандарти цифрового підпису ГОСТ Р 34.10-94 та ГОСТ Р 34.10-2001.
34. Типи загроз при обміні інформацією.
35. Типи атак на криптосистеми.
36. Атака на криптосистему RSA.
37. Атака на електронний підпис.
38. Елементи частотного криптоаналізу.
39. Різницевий криптоаналіз.
40. Лінійний криптоаналіз.
41. Проблеми розподілу криптографічних ключів: генерування ключів.
42. Проблеми розподілу криптографічних ключів: ієрархія ключів.
43. Проблеми розподілу криптографічних ключів: накопичення ключів.
44. Проблеми розподілу криптографічних ключів: розподіл ключів.
45. Розподіл ключів у симетричних криптосистемах.
46. Розподіл ключів у асиметричних криптосистемах.
47. Ієрархічна модель сертифікації ключів.
48. Протокол прямого обміну ключами.
49. Протокол Діффі-Хеллмана.
50. Проблеми генерування випадкових послідовностей.
51. Проблеми генерування псевдовипадкових послідовностей.
52. Застосування пароля для підтвердження істинності користувача.