Перелік питань до екзамену

1.Поняття та визначення криптології.

2. Задачі криптографії.

3. Задачі криптоаналізу.

4. Симетричні криптоперетворення.

5. Криптоперетворення з відкритим ключем.

6.Поняття цифрового підпису.

7. Види та особливості симетричних криптосистем.

8. Перестановки. Приклади алгоритмів.

9. Підстановки. Приклади алгоритмів.

10. Блочні шифри. Їх структура. Основні алгоритмічні елементи.

11.Мережа Фейстеля.

12. Підстановочно-перестановочні мережі (SP мережі).

13. Режими роботи блочних шифрів.

17. Гамування та потокові шифри.

19. Алгоритм блочного шифрування Rijndael(Стандарт AES ).

20. Геш-функції та вимоги до них.

21. Поняття та види криптопротоколів.

22. Система з відкритим ключем RSA.

23. Алгоритми обміну ключами Діффі - Хелмана.

24. Алгоритм цифрового підпису Ель-Гамаля та його модифікації.

26. Алгоритми з відкритим ключем на основі проблеми обчислення дискретного логарифму над еліптичними кривими.

30. Електронний підпис на основі RSA

31. Цифровий підпис на основі алгоритму Эль-Гамалю