Вопросы к экзамену по дисциплине
Практическая криптография (2017-2018)
Чергинец Д.Н.

1. Понятие криптографической функции хеширования.
2. Применение функций хеширования.
3. Функция хеширования MD5.
4. Функция хеширования SHA-1.
5. Функция хеширования SHA-2.
6. Функция хеширования SHA-3.
7. Алгоритм шифрования в криптосистеме AES.
8. Алгоритм расшифрования в криптосистеме AES.
9. Процедура SubBytes криптоситемы AES.
10. Процедура ShiftRows криптоситемы AES.
11. Процедура MixColumns криптоситемы AES.
12. Процедура AddRoundKey криптоситемы AES.
13. Алгоритм расширения ключа криптоситемы AES.
14. Способы дополнения сообщений.
15. Режимы сцепления блоков шифротекста.
16. Стандарт PKCS#1.
17. Методы преобразования сообщения: PKCS.
18. Методы преобразования сообщения: OAEP.
19. Криптосистема RSA с модулем, являющимся произведением более двух простых чисел.
20. Электронная цифровая подпись DSA.
21. Электронная цифровая подпись СТБ1176.2 – 99.
22. Электронная цифровая подпись ГОСТ3410 - 94.
23. Группа точек эллиптической кривой.
24. Порядок группы точек эллиптической кривой, алгоритм Шуфа.
25. Криптосистемы на основе группы точек эллиптической кривой.
26. Электронная цифровая подпись СТБ 34.101.45-2013.
27. Электронная цифровая подпись ГОСТ Р 34.10-2012.
28. Электронная цифровая подпись ECDSA.
29. Цифровой водяной знак. Свойства цифровых водяных знаков. Применение.
30. Цифровой водяной знак. Свойства цифровых водяных знаков. Классификация.
31. Цифровые водяные знаки на основе сингулярного разложения.
32. Схемы обязательств.
33. Доказательство с нулевым разглашением.

34. Разделение секрета.