Вопросы к экзаменационной сессии по дисциплине «Криптографические средства защиты информации» для 3 курса специальности 10.02.05.

Преподаватель: Двойкина А.С., группы БИ50-1-2-3-21, БИ50-11-22, семестр 6, 4.

1. Предмет и задачи криптографии. История криптографии, основные термины.
2. Алгоритм Плейфера, квадрат Полибия.
3. Математические основы криптографии. Элементы теории множеств.
4. Группы, кольца, поля.
5. Делимость чисел. Признаки делимости. Простые и составные числа.
6. Основная теорема арифметики.
7. Нахождение НОД
8. Наибольший общий делитель. Взаимно простые числа.
9. Алгоритм Евклида для нахождения НОД.
10. Функция Эйлера. Теорема Ферма-Эйлера.
11. Расширенный алгоритм Евклида.
12. Китайская теорема об остатках.
13. Разложение числа на множители.
14. Методы симметричного шифрования
15. Шифры замены.
16. Методы перестановки.
17. Гаммирование. Гаммирование с конечной и бесконечной гаммами
18. Криптографические атаки.
19. Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии.
20. Представление информации в двоичном коде. Таблица ASCII
21. Общие сведения о симметричном шифровании.
22. Шифры Виженера и Вернама.
23. Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.
24. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4
25. Криптосистемы с открытым ключом.
26. Структурная схема шифрования с открытым ключом.
27. Алгоритм RSA.
28. Алгоритмы хэширования
29. Аутентификация данных. Общие понятия. ЭП. MAC.
30. Деление методов шифрования на симметричные и асимметричные. Симметричные методы.
31. Квантовая и постквантовая криптография. Квантовые компьютеры.
32. Центры сертификации в компьютерных сетях.
33. Центр сертификации – это. . ?
34. Сертификаты. Сертификат как файл и как понятие.
35. Сертификаты по типу выдачи.

36. Сертификаты по типу валидации.
37. Явление коллизии в шифрах MD5.
38. Свойства сертификатов.
39. HTTP и HTTPS: работа протоколов, в чем ключевое различие? Порт по умолчанию.
40. В чем сложность получения сертификатов с повышенным уровнем валидации?
41. Отличие ЭЦП от цифровой подписи и электронной подписи.
42. Криптостойкость – это свойство. .?
43. Криптология и криптография. Основы стеганографии.
44. Хэш-функции и дайджесты. Основная информация о них.
45. Практическое применение SSL-сертификатов.
46. Современные методы шифрования. Алгоритмы SHA.
47. Функция Эйлера. Назначение.
48. Отличие поточного и блочного методов шифрования.
49. Абсолютно стойкие шифры. Оценка надежности.
50. Криптографические методы защиты информации.
51. Криптографический инструментарий OpenSSL.
52. Три основных функции ЦС.
53. Алфавит в криптографии.
54. Логическая операция «исключающее или».