Вопросы по курсу «Криптографические протоколы»

1. Предмет и задачи. Определение шифра, понятие стойкости.
2. Предположения об исходных условиях криптоанализа
3. Симметричные и асимметричные криптосистемы, хэш-функции, криптографические протоколы.
4. История криптографии. Криптография древности, частотный критоанализ.
5. Криптография нового времени.
6. Криптография XX века. Принцип Керкгоффса.
7. Понятие абсолютной стойкости или теоретико-информационной стойкости. Одноразовый блокнот.
8. Понятие псевдослучайности.
9. Поточные шифры. Синхронные и самосинхронизирующиеся шифры
10. Требования к поточным шифрам: Постулаты Голомба, профиль линейной сложности.
11. Методы построения больших периодов в поточных шифрах. Регистры сдвигов с линейной обратной связью.
12. Статистические тесты.
13. Семантическая стойкость. CPA модель атаки.
14. Требования к блочным шифрам. PRP и PRF.
15. Способы построение блочных шифров: подстановки, перестановки, сети фейстеля. DES, AES.
16. Подходы к криптоанализу: линейный, дифференциальный, «встреча посередине».
17. Режимы использования блочных шифров (“электронная кодовая книга”, режимы с зацеплением, режимы использования блочных шифров для получения поточных шифров).
18. Детерминированные и недерминированные алгоритмы шифрования.
19. Влияние случайности на стойкость. Слабости блочных шифров.
20. Контроль целостности. MAC.
21. Определение, модель безопасности. Построение на базе Блоковых шифров.
22. HMAC. Хэш-функции. Требования к хэш-функциям.
23. Аутентифицированное шифрование.
24. CCA модель атаки. Примеры активных атак.
25. Понятие алгоритма с открытым ключом.
26. Схема RSA. Атаки на RSA.
27. Схема шифрования ElGamal. Базовые задачи, допущение Диффи и Хелмана.
28. Управление ключами. Групповые ключи. Попарные ключи. Использование мастер-ключей.
29. Система Диффи и Хелмана. Человек посередине.
30. Групповые ключи. Попарные ключи. Использование мастер-ключей и KDF.
31. Протоколы обмена. С сервером, без сервера.
32. Известные атаки на протоколы обмена ключами.
33. K-надежные схемы распределения ключей.
34. Протоколы разделения секрета.
35. Пороговая криптография.
36. Протоколы цифровых денег и электронного голосования.
37. Слепая подпись.
38. Схема идентификации Schnorr – Shamir.
39. Схема идентификации Feige – Fiat – Shamir.
40. Инфраструктура открытых ключей и альтернативные подходы(ID-based распределенные системы).

41. Понятие анонимности пользователей. Постановки задачи
42. PIR (протоколы конфиденциального получения информации).
43. Понятия квантовых вычислений.
44. Построение криптосистем на доказано сложных задачах. Линейные коды. Способы задания. Декодирование линейных кодов как «трудная» задача. Декодирование линейных кодов как «простая» задача.
45. Системы Макэлиса и Нидерайтора.