Вопросы к экзамену по Криптопротоколам и стандартам (сквозная нумерация)
1. Основные понятия и виды криптографических протоколов
2. Цифровые подписи. Основные понятия
3. Подписи RSA и Рабина
4. Подпись Эль-Гамаля. Одноразовость k (показать)
5. Подписи Эль-Гамаля с сокращённой длиной
6. Подпись Шнорра
7. Подписи DSA и **ГОСТ** Р34.10-**94**
8. Эллиптические кривые над полем вещественных чисел
9. Эллиптические кривые над полем Zp
10. Цифровые подписи на эллиптических кривых
11. Слепые и затемнённые подписи
12. Подписи со скрытым каналом
13. Неотрицаемые подписи
14. Коллективные подписи
15. Электронная жеребьёвка. Протоколы на основе дискретного логарифмирования. Связанность. Секретность.
16. Электронная жеребьёвка. Протоколы на основе хэш-функции и симметричного шифрования. Связанность. Секретность
17. Разделение секрета. Основные понятия. Схемы на основе xor
18. Схемы разделения секрета (СРС) Блэкли
19. СРС Шамира
20. СРС на основе китайской теоремы об остатках
21. СРС для произвольной структуры доступа. Проверяемое разделение секрета
22. Совершенность и идеальность СРС
23. Покер по телефону
24. Идентификация и аутентификация. Основные понятия и виды протоколов
25. Парольная схема. Схема Лампорта
26. Протоколы рукопожатия
27. Интерактивные системы доказательства. Пример для квадратичных невычетов
28. Интерактивные системы доказательства. Пример для неизоморфизма графов
29. Интерактивные системы доказательства с нулевым соглашением. Пример для изоморфизма графов
30. Схема Фиата-Шамира. Схема Фейга-Фиата-Шамира
31. Схема Гиллу-Кискатра. Полнота и корректность
32. Схема Шнорра. Полнота и корректность
33. Схема Окамото. Полнота и корректность
34. Управление ключами. Жизненный цикл ключей
35. Формирование ключей. Алгоритм фон Неймана
36. Распределение ключей
37. Распределение ключей средствами симметричной криптографии. Wide-mouth-frog
38. Протокол Нидхема-Шредера (с уязвимостью). Yahalom.
39. Протоколы Шамира и Диффи-Хэллмана. Атака «человек посередине».
40. Широковещательное распределение ключей.
41. Инфраструктура открытых ключей.
42. Структура сертификата по стандарту X.509.