Защита информации. Экзаменационные вопросы.

Осенний семестр 2014 года.

1. Шифры простой замены. Их криптоанализ. Одноразовый блокнот.
2. Генераторы псевдослучайных чисел. Статистические тесты. Предсказуемость ГПСЧ. Криптостойкие ГПСЧ.
3. Поточные шифры. Атаки на них. Шифр RC4. Уязвимость WEP шифрования.
4. Блочные шифры. Схема Фейстеля. Шифр DES и его криптоанализ.
5. Шифры 3-DES, DESX, 2-DES. Причины появления. Криптоанализ. Атаки по побочным каналам.
6. Семантическая стойкость шифра к атаке с выбранным открытым текстом для одноразового ключа. Стойкость режима DetCTR при одноразовом ключе.
7. Семантическая стойкость шифра к атаке с выбранным открытым текстом для многоразового ключа. Режимы работы блочных шифров CBC, RandCTR.
8. Псевдослучайные функции (ПСФ) и псевдослучайные перестановки. Лемма о переключении. Построение генератора псевдослучайных чисел (ГПСЧ) с помощью ПСФ.
9. Криптостойкий код целостности сообщения (MAC). MAC на основе псевдослучайной функции. ECBC-MAC, NMAC. Атака на основе парадокса дня рождения.
10. Криптографические хэш-функции. Конструкция Меркля-Дамгарда. HMAC. Атаки по побочным каналам и на основе парадокса дня рождения.
11. Заверенное шифрование.
12. Протокол TLS после согласования ключей симметричного шифра. Оракул правильного окончания блока в режиме CBC.
13. Создание сессионных ключей симметричного шифра по первичному ключу. Совершенная прямая секретность. Хранение паролей.
14. Группа. Циклическая группа. Малая теорема Ферма. Обобщенный алгоритм Евклида.
15. Кольцо. Поле. Расширение конечного поля.
16. Функция Эйлера. Китайская теорема об остатках и ее применение.
17. Квадратичные вычеты и их свойства. Символ Лежандра.
18. Тест на простоту на основе малой теоремы Ферма. Тест Миллера-Рабина. Поиск случайного простого числа.
19. Асимметричная криптосистема. Модели ее стойкости к атакам. Криптосистема RSA.
20. Асимметричная криптосистема. Модели ее стойкости к атакам. Перестановка RSA. Атаки на перестановку RSA.
21. Электронно-цифровая подпись (ЭЦП). ЭЦП на основе перестановки RSA и ее уязвимости.
22. Инфраструктура открытого ключа.
23. Протокол Диффи-Хеллмана. Его возможные уязвимости. Использование надежных простых чисел.
24. Электронно-цифровая подпись (ЭЦП). ЭЦП DSA.
25. Протокол Нидхема-Шредера.
26. Система контроля доступа Kerberos.
27. Протокол TLS (согласование ключей симметричного шифра).
28. Протокол IPSec.
29. Утилита SSH.

30. Протокол авторизации без раскрытия информации.
31. Протокол подбрасывания монеты по телефону. Протоколы разделения секрета.
32. Группа точек эллиптической кривой. Ее свойства. Оптимизация операций над ее элементами.
33. Криптосистема RSA и протокол Диффи-Хеллмана для группы точек эллиптической кривой.
34. ЭЦП DSA для группы точек эллиптической кривой.
35. Скрытое получение информации. Протокол, основанный на квадратичных вычетах.
36. Скрытое получение информации. Локально декодируемые коды. Код Адамара. Код Рида-Маллера как локально декодируемый код.

Подготовка: 45 минут. Билет: 2 вопроса и задача. Нерешенная задача – обычно, минус 1 балл.

Считается, что вы знаете и умеете использовать все определения, теоремы, шифры, протоколы и т.д. Т.е. по ним могут быть доп. вопросы. Доказательства рассказываете только в вытянутом билете.

По некоторым вопросам в лекциях много материала. О каких-то второстепенных фактах можно и нужно умолчать при рассказе билета. Считайте, что на рассказ каждого вопроса у вас не более 5-7 минут.