Вопросы экзамена по криптографии

Группа 114 (лектор А. Ю. Лузгарев)

Весна 2015

1. Симметричное шифрование. Принцип Керкгофса.
2. Примеры применения криптографии. Классы атак.
3. Подстановочный шифр и его взлом.
4. Шифр Виженера, роторная машина.
5. Определение шифра. Шифр Вернама и совершенная секретность.
6. Вероятностные переформулировки совершенной секретности.
7. Эксперимент по взлому. Длина ключа в случае совершенной секретности.
8. Псевдослучайный генератор и его предсказуемость. Линейный конгруэнтный генератор.
9. Атаки на потоковые шифры.
10. Статистические тесты, преимущество. Надежность псевдослучайного генератора.
11. Непредсказуемость надежного генератора. Вычислительная неразличимость.
12. Определение схемы шифрования с закрытым ключом. Вычислительная стойкость.
13. Стойкость потокового шифра. Шифрование нескольких сообщений.
14. Стойкость относительно chosen plaintext-атак. Функции с ключом и псевдослучайные функции.
15. Шифрование с помощью псевдослучайной функции и его устойчивость.
16. Псевдослучайные перестановки. Методы работы блочных шифров.
17. Конструкции псевдослучайных перестановок. Сеть Фейстеля.
18. Аутентификация сообщений. Код аутентификации сообщений и его надежность.
19. Конструкция кода аутентификации сообщений из псевдослучайной функции.
20. Протокол интерактивного обмена ключами, его надежность. Описание протокола Диффи–Хеллмана.
21. Задача DDH и надежность протокола Диффи–Хеллмана.
22. Схема шифрования с открытым ключом, ее надежность относительно подслушивания и относительно chosen plaintext-атак.
23. Шифрование нескольких сообщений, его надежность. Гибридное шифрование.
24. Наивная схема шифрования RSA. Ускорение дешифровки, маленький показатель.
25. RSA с набивкой, задача RSA и надежность схемы шифрования RSA с набивкой.
26. Схема Эль-Гамаля и ее надежность.
27. Квадратичные вычеты и символ Якоби.
28. Задача определения квадратичных вычетов и схема шифрования Гольдвассер–Микали.
29. Извлечение квадратных корней и схема шифрования Рабина.
30. Остатки по модулю N^2 и схема шифрования Пайе.
31. Схема цифровой подписи, ее надежность. Наивная схема RSA.
32. RSA с хэшем. Схема одноразовой подписи Лэмпорта.
33. Доказательства с нулевым разглашением.
34. Сертификаты. Схемы разделения секрета.