Вопросы к экзамену «Современная криптография»

Осень 2014

1. Шифрование – краткая история. Сдвиг и перестановка. Симметричные и асимметричные шифры. Примеры алгоритмов.
2. Хэширование. Основные современные хэш-функции.
3. Криптоанализ. Простейший частотный анализ, атаки на криптографические протоколы.
4. Применение криптографии в сетях. SSL/TLS, ЭЦП, протоколы аутентификации, управление доверием. Примеры атак – перебор по словарю, rainbow таблицы.
5. Протоколы PGP и S/MIME и их реализации.
6. Шифр Вернама. Потоковые шифры. Регистр сдвига с линейными обратными связями. Алгоритм Берлекэмпа-Мэсси восстановления характеристического многочлена по выходу регистра сдвига.
7. Фильтрующий генератор. Атаки на фильтрующий генератор. Требования на функцию фильтрующего генератора.
8. Криптография с открытым ключом. Односторонние функции и односторонние функции с секретом. Криптосистема RSA. Взаимосвязь параметров криптосистемы. Условия на выбор простых чисел. Атака на RSA, использующая малый показатель расшифрования (на основе теоремы Винера).
9. Криптосистема Рабина. Вопрос неоднозначности расшифрования. Алгоритм решения квадратного уравнения в кольце вычетов по простому/составному модулю.
Связь криптосистемы Рабина с задачей факторизации.
10. Алгоритмы факторизации чисел: алгоритм полного перебора, алгоритм Ферма, ро-метод Полларда, (р-1)-метод Полларада, метод квадратичного решета.
11. Классическая криптосистема Эль-Гамаля. Задача дискретного логарифмирования.
12. Алгоритмы дискретного логарифмирования: алгоритм согласования, метод Похлига-Хэллмана, субэкспоненциальный алгоритм вычисления дискретного логарифма.
13. Эллиптические кривые. Группа точек эллиптических кривых, арифметика эллиптических кривых. Криптосистема Эль-Гамаля на эллиптических кривых.
14. Постквантовая эра, квантовый компьютер. Квантовые вычисления. Преобразование Фурье. Алгоритм решения проблемы скрытой подгруппы за полиномиальное время.
15. Проблема распределения ключей. Открытое распределение ключей. Головоломка Меркля. Протокол Диффи-Хэллмана. Протоколы идентификации. Протокол Нидхема--Шредера. Атака Лоу на этот протокол.
16. Протокол ЭЦП. Обзор основных протоколов ЭЦП (RSA, Эль-Гамаль, Эль-Гамаль на эллиптических кривых). Инфраструктура открытых ключей. Понятие удостоверяющего центра.