Программа экзамена по курсу "Теоретико-сложностные проблемы криптографии" (2013/2014).

1. Одноленточные и многоленточные машины Тьюринга. Время работы и память как меры сложности. Оценка количества шагов для копирования слова. Полиномиальные машины Тьюринга (по времени и памяти).
2. Оценка времени работы машин Тьюринга, выполняющих арифметические операции над натуральными числами.
3. Равнодоступные адресные машины, меры сложности: количество операций, длина машинного слова, количество использованных регистров. Полиномиальные RAM (по всем трем мерам сложности). Полиномиальные RAM для нахождения НОД и возведения в степень по данному модулю.
4. Моделирование машин Тьюринга на RAM.
5. Моделирование многоленточных машин Тьюринга на одноленточных машин Тьюринга.
6. Моделирование RAM на машинах Тьюринга.
7. Классы полиномиально вычислимых функций и полиномиально разрешимых предикатов. Независимость этих классов от вычислительной модели.
8. Схемы из функциональных элементов. Верхняя оценка $O(n2^n)$ схемной сложности любой булевой функции. Нижняя оценка $2^n/3n$ схемной сложности некоторой булевой функции от n переменных. Схемы полиномиального размера для сложения и умножения.
9. Вероятностные полиномиальные алгоритмы. Уменьшение вероятности ошибки с помощью повторения. Классы BPP и FBPP. Вероятностный полиномиальный алгоритм проверки полиномиального тождества.
10. Класс nuP. Включение P в nuP. Включение BPP в nuP.
11. Класс NP. Примеры языков из NP: составные числа, изоморфные графы, выполнимость формул и схем, 3-раскраска, Сумма подмножества, Разбиение, Вершинное покрытие. Сводимости задач (по Карпу). Определение NP полной и NP трудной задачи.
12. Теорема Кука-Левина об NP полноте задачи выполнимости схем. NP полнота задач 3-КНФ,
13. Односторонние функции (сильно и слабо). Обратимость любой функции при условии P=NP.
14. Теорема Левина - Гольдрайха о преобразовании слабо односторонней функции в сильно одностороннюю.
15. Обобщение понятия односторонней функции — частичные односторонние функции (с равномерным распределением). Односторонние перестановки. Функция Рабина, функция RSA, дискретная экспонента.
16. Статистически и вычислительно неотличимые случайные величины. Свойства вычислительно неотличимых случайных величин. Полиномиально генерируемые и доступные последовательности случайных величин. Генераторы псевдослучайных чисел (ПСЧ). Слабая необратимость генераторов ПСЧ.

17. Понятие трудного бита для данной функции. Лемма о трудном бите (конкатенация значения функции и трудного бита неотличима от конкатенации значения функции и случайного бита).
18. Надежность генераторов по Яо и эквивалентность этого определения обычному. Преобразование генератора, добавляющего лишь один бит в генератор, добавляющий сколько угодно битов.
19. Построение генератора ПСЧ, исходя из односторонней перестановки с трудным битом.
20. Теорема о вероятностном декодировании списком кода Адамара.
21. Теорема Левина-Гольдрайха о трудном бите для односторонних функций (доказательство по модулю теоремы о вероятностном декодировании списком кода Адамара).
22. Семейства псевдослучайных функций (ПСФ). Сильный и слабый варианты определения. Построение псевдослучайных функций исходя из генератора ПСЧ.
23. Односторонние перестановки с секретом (trapdoor permutations). Примеры. Трудный бит для необратимой перестановки с секретом.
24. Одноразовые схемы шифрования с закрытым ключом (СШЗК, симметричные схемы). Построение СШЗК на основе генератора ПСЧ.
25. Многоразовые схемы шифрования с закрытым ключом. Построение многоразовой СШЗК на основе семейства ПСФ и одноразовой СШЗК.
26. Схемы шифрования с открытым ключом (ШОК, асимметричные схемы). Конструкция ШОК на основе необратимой перестановки с секретом.
27. Неинтерактивные протоколы привязки к биту (НПБ). Построение НПБ на основе односторонней перестановки.
28. Интерактивные алгоритмы. Интерактивные протоколы привязки к биту (ИПБ).
29. Неразглашение информации интерактивным алгоритмом. Лемма о неразглашении информации в результате последовательного повторения алгоритма.
30. Интерактивные протоколы привязки к биту (ИПБ). Построение ИПБ на основе генератора ПСЧ
31. Протоколы бросания монетки. Построение таких протоколов на основе протокола привязки к биту.
32. Протоколы идентификации с закрытым ключом. Построение такого протокола на основе семейства ПСФ.
33. Протоколы идентификации с открытым ключом. Построение протокола идентификации с открытым ключом на основе необратимости функции Рабина.
34. Семейства функций с трудно обнаружимыми коллизиями (СТОК). Семейства функций с трудно обнаружимыми зацеплениями (СТОЗ), построение такого семейства на основе функции Рабина. Построение СТОК на основе СТОЗ.
35. Протоколы цифровой подписи. Протокол цифровой подписи одного бита и протокол одноразовой подписи сообщений фиксированной длины на основе односторонней функции.
36. Протокол одноразовой цифровой подписи сообщений произвольной длины (на основе СТОК и протокола одноразовой подписи сообщений фиксированной длины).

37. Протокол многоразовой подписи на основе протокола одноразовой подписи сообщений произвольной длины и семейства ПСФ.

Литература.

1. Введение в криптографию. Под общей редакцией В.В.Ященко. — 3-е изд. доп. — М.: МЦНМО: "ЧеРо 2000. — 288 с.

2. М.И. Анохин, Н.П.Варновский, В.М.Сидельников, В.В. Ященко. Криптография в банковском деле. М.: МИФИ, 1997.

3. O. Goldreich. Foundations of cryptography. Basic tools. Cambridge Univ. Press. 2001. 400 p.

4. O. Goldreich. Foundations of cryptography. Basic applications. Cambridge Univ. Press. 2004.