Программа экзамена по курсу "Теоретико-сложностные проблемы криптографии" (2009/2010).

1. Однолентночные и многоленточные машины Тьюринга. Время работы и память как меры сложности. Оценка количества шагов для переворачивания слова. Полиномиальные машины Тьюринга (по времени и памяти).
2. Равнодоступные адресные машины, меры сложности: количество операций, длина машинного слова, количество использованных регистров. Полиномиальные PAM (по всем трем мерам сложности).
3. Моделирование машин Тьюринга на PAM. Моделирование PAM на машинах Тьюринга. Классы полиномиально вычислимых функций и полиномиально разрешимых предикатов. Независимость этих классов от вычислительной модели.
4. Вероятностные алгоритмы. Полиномальные по времени вероятностные алгоритмы (время ограничено полиномом от длины входа при любых исходах бросаний). Определение вычисления с ограниченной ошибкой.
5. Вероятностный полиномиальный алгоритм проверки полиномиального тождества.
6. Уменьшение вероятности ошибки с помощью повторения. Классы BPP и FBPP.
7. Схемы из функциональных элементов. Верхняя оценка $O(n2^n)$ схемной сложности любой булевой функции.
8. Класс nuP. Включение P в nuP. Класс P/poly и его совпадение с классом nuP. Включение BPP в nuP. Схемы полиномиального размера для сложения и умножения.
9. Класс NP. Примеры языков из NP: Составные числа, Изоморфные графы, Выполнимость формул и схем, 3-раскраска, Сумма подмножества, Разбиение, Вершинное покрытие.
10. Сводимость задач (по Карпу). Определение NP полной и NP трудной задачи. Теорема Кука-Левина об NP полноте задачи выполнимости схем.
11. NP полнота задач 3-КНФ, КЛИКА, ВершинноеПокрытие, 3-раскраска и СуммаПодмножества.
12. Односторонние функции (сильно и слабо). Обратимость любой функции при условии P=NP.
13. Теорема Левина - Гольдрайха о преобразовании слабо односторонней функции в сильно одностороннюю.
14. Статистическое расстояние между случайными величинами. Статистическая и вычислительная неотличимость последовательностей случайных величин. Свойства вычислительно неотличимых случайных величин. Полиномиально генерируемые и доступные последовательности случайных величин. Определение генераторов ПСЧ $k(n) \to l(n)$.
15. Обобщение понятия односторонней функции — частичные односторонние функции (с равномерным распределением). Одностороние перестановки. Функция Рабина, функция RSA, дискретная экспонента.
16. Понятие трудного бита для данной функции. Лемма о трудном бите.
17. Построение генератора ПСЧ с произвольной степенью расширения из генератора $p(n) \to p(n) + 1$. Построение генератора, исходя из односторонней перестановки с трудным битом.
18. Лемма о декодировании списком кода Адамара (без доказательства). Теорема Левина-Гольдрайха о трудном бите.
19. Доказательство леммы о декодировании списком кода Адамара.
20. Семейства псевдослучайных функций (ПСФ): слабое и сильное определения. Построение семейства псевдослучайных функций. Доказательство слабой и сильной надежности.
21. Схемы шифрования с закрытым ключом. Одноразовые и многоразовые схемы. Два вида атаки на многоразовые схемы: перехват зашифрованных сообщений и атака с выбором шифруемых сообщений и последующим перехватом одного сообщения. Построение одноразовой схемы. Построение многоразовой схемы, исходя из одноразовой схемы и семейства ПСФ.
22. Необратимые перестановки с секретом (trapdoor permutations): определение и кандидаты. Трудный бит для необратимой перестановки с секретом.
23. Схемы шифрования с открытым ключом (ШОК). Конструкция ШОК одного бита на основе необратимой перестановки с секретом. Конструкция ШОК сообщений любой длины на основе ШОК

одного бита. Прямая конструкция ШОК сообщений любой длины на основе необратимой перестановки с секретом.
24. Неинтерактивные протоколы привязки к биту (НПБ). Построение НПБ на основе односторонней инъекции с полиномиально разрешимой областью определения. Построение НПБ на основе односторонней инъекции, для которой полиномиально генерируемая трудная случайная величина принимает значения только в области определения функции.
25. Протоколы бросания монетки по телефону. Построение такого протокола на основе протокола привязки к биту.
26. Интерактивные протоколы привязки к биту (ИПБ). Построение ИПБ на основе генератора ПСЧ
27. Интерактивные доказательства. Интерактивное доказательство неизоморфности графов.
28. Интерактивные доказательства с нулевым разглашением (определение). Лемма о последовательном повторении неразглашающей стратегии (без доказательства). Интерактивное доказательство с нулевым разглашением изоморфности графов.
29. Протоколы аутентификации. Построение протокола аутентификации на основе необратимости функции Рабина.
30. [1] Интерактивное доказательство с нулевым разглашением раскрашиваемости графа в три цвета.
31. 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.
32. Универсальные семейство односторонних хэш-функций (УСОХ). Построение УСОХ на основе тотальной односторонней перестановки.
33. Протоколы цифровой подписи, разные виды атаки на протоколы цифровой подписи. Протокол цифровой подписи одного бита.
34. Протокол одноразовой цифровой подписи сообщения фиксированной длины. Протокол одноразовой цифровой подписи сообщения произвольной длины (на основе УСОХ).
35. Протокол многоразовой подписи на основе протокола одноразовой подписи сообщения произвольной длины и семейства случайных функций.
36. Пороговые протоколы разделения секрета (схема Блейкли и Шамира). Протоколы разделения секрета с произвольной схемой доступа.
37. Протоколы конфиденциальных вычислений: определение с получестными игроками. Забывающая передача (oblivious transfer) OT_1^k.
38. Улучшенные односторонние перестановки с секретом (УПС) и построение протокола OT_1^k, исходя из УПС (для получестных игроков).
39. Протокол конфиденциального вычисления любой пары полиномиально вычислимых функций на основе протокола OT_1^4 (для получестных игроков).

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.

[1] Этот вопрос дополнительный, его нужно знать только на тем, кто претендует на "отлично".