# Программа экзамена по курсу "Теоретико-сложностные проблемы криптографии" (2010/2011).

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). Моделирование машин Тьюринга на PAM.
3. Моделирование PAM на машинах Тьюринга. Классы полиномиально вычислимых функций и полиномиально разрешимых предикатов. Независимость этих классов от вычислительной модели.
4. Схемы из функциональных элементов. Верхняя оценка $O(n2^n)$ схемной сложности любой булевой функции. Схемы полиномиального размера для сложения и умножения.
5. Вероятностные полиномиальные алгоритмы. Уменьшение вероятности ошибки с помощью повторения. Классы BPP и FBPP. Вероятностный полиномиальный алгоритм проверки полиномиального тождества.
6. Класс nuP. Включение P в nuP. Класс P/poly и его совпадение с классом nuP. Включение BPP в nuP.
7. 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.
8. Теорема Кука-Левина об NP полноте задачи выполнимости схем.
9. NP полнота задач 3-КНФ, КЛИКА, ВершинноеПокрытие,
10. NP полнота задач 3-раскраска и СуммаПодмножества.
11. Односторонние функции (сильно и слабо). Обратимость любой функции при условии P=NP.
12. Теорема Левина - Гольдрайха о преобразовании слабо односторонней функции в сильно одностороннюю.
13. Обобщение понятия односторонней функции — частичные односторонние функции (с равномерным распределением). Одностороние перестановки. Функция Рабина, функция RSA, дискретная экспонента.

14. Статистически и вычислительно неотличимые случайные величины. Свойства вычислительно неотличимых случайных величин. Полиномиально генерируемые и доступные последовательности случайных величин. Генераторы ПСЧ.
15. Понятие трудного бита для данной функции. Лемма о трудном бите (конкатенация значения функции и трудного бита неотличима от конкатенации значения функции и случайного бита).
16. Построение генератора ПСЧ, исходя из односторонней перестановки с трудным битом.
17. Надежность генераторов по Яо. Построение генератора ПСЧ с произвольной степенью расширения из генератора $p(n) \to p(n) + 1$.
18. Теорема Левина-Гольдрайха о трудном бите для односторонних функций (доказательство по модулю леммы о вероятностном декодировании списком кода Адамара).
19. Лемма о вероятностном декодировании списком кода Адамара.
20. Псевдослучайные функции. Сильный и слабый варианты определения. Построение псевдослучайных функций исходя из генератора ПСЧ.
21. Односторонние перестановки с секретом (trapdoor permutations). Примеры. Трудный бит для необратимой перестановки с секретом.
22. Схемы шифрования с закрытым ключом (одноразовые). Построение СШЗК на основе генератора ПСЧ.
23. Многоразовые СШЗК. Построение многоразовой СШЗК на основе семейства ПСФ и одноразовой СШЗК.
24. 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.
25. Неинтерактивные протоколы привязки к биту (НПБ). Построение протокола на основе односторонней перестановки с полиномиально разрешимой областью определения.
26. Интерактивные доказательства. Интерактивное доказательство неизоморфности графов.
27. Лемма об уменьшении ошибки при последовательном повторении интерактивного протокола.
28. Неразглашение информации. Лемма о неразглашении информации в результате последовательного повторения.

29. Интерактивные протоколы привязки к биту (ИПБ). Построение ИПБ на основе генератора ПСЧ
30. Протоколы бросания монетки по телефону. Построение такого протокола на основе протокола привязки к биту.
31. Интерактивные доказательства с нулевым разглашением (определение). Интерактивное доказательство с нулевым раглашением для изоморфности графов. Интерактивное доказательство с нулевым раглашением для любого NP языка (только протокол без доказательства корректности) на основе протокола привязки к биту.
32. Протоколы аутентификации. Построение протокола аутентификации на основе необратимости функции Рабина.
33. 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.
34. Протоколы цифровой подписи. Протокол цифровой подписи одного бита и протокол одноразовой подписи сообщений фиксированной длины на основе односторонней функции.
35. Протокол одноразовой цифровой подписи сообщений произвольной длины (на основе СТОК и протокола одноразовой подписи сообщений фиксированной длины).
36. Протокол многоразовой подписи на основе протокола одноразовой подписи сообщений произвольной длины и семейства случайных функций (без анализа корректности).

**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.