Программа экзамена по курсу теоретико-сложностные проблемы криптографии (2007).

1. Машины Тьюринга (одноленточные), выполняющие арифметические операции над n-битовыми числами за время poly(n).
2. Машина Тьюринга (одноленточная), возводящая в степень по данному модулю за полиномиальное время. Вычисление НОД двух натуральных чисел за полиномиальное количество шагов.
3. Теорема о том, что любая функция, вычислимая некоторой многоленточной машиной Тьюринга за полиномиальное время, вычисляется некоторой одноленточной машиной Тьюринга за полиномиальное время. Классы P и FP.
4. Схемы из функциональных элементов. Схемы полиномиального от n размера, складывающие и умножающие n-битовые числа.
5. Класс n.u.P и включение P $\subset$ n.u.P.
6. Вероятностные полиномиальные алгоритмы и классы BPP и FBPP. Теорема о том, что ошибку вероятностного алгоритма можно сделать сколько угодно малой.
7. Включение BPP $\subset$ n.u.P.
8. Вероятностный полиномиальный алгоритм Миллера–Рабина распознавания простоты чисел.
9. Класс NP. Примеры проблем из класса NP. Полиномиальная сводимость. Понятие NP-полной проблемы.
10. Теорема Кука–Левина об NP-полноте проблемы выполнимости схем из функциональных элементов.
11. NP-полнота задачи выполнимости формул в 3-КНФ.
12. NP-полнота задачи о раскраске графа в 3 цвета.
13. NP-полнота задач КЛИКА, НЕЗАВИСИМОЕ МНОЖЕСТВО и ВЕРШИННОЕ ПОКРЫТИЕ.
14. NP-полнота задачи о сумме подмножеств.
15. NP-полнота задач о гамильтонове цикле и о коммивояжере.
16. Необратимые и односторонние функции. Три примера предположительно односторонних функций.
17. Не всюду определенные односторонние функции. Построение односторонней функции из не всюду определенной односторонней функции. 18. Слабо необратимые и слабо односторонние функции. Построение односторонней функции из любой слабо односторонней функции.
19. Определение статистически и вычислительно неотличимых последовательностей случайных величин. Свойства неотличимых последовательностей случайных величин. 20. Частично односторонние функции. Примеры: функция Рабина, функци RSA, функция Блюма–Микэли. Построение односторонней функции из любой частично односторонней функции. Если P=NP, то односторонних функций нет.
21. Генераторы псевдослучайных чисел. Теорема об эквивалентности гипотезы о существовании генератора и гипотезы о существовании необратимой функции (в одну сторону без доказательства). 22. Расширители. Построение генератора, исходя из расширителя. 23. Односторонние перестановки. Односторонние обобщенные перестановки, примеры. 24. Трудный бит, характеризация расширителей в терминах трудного бита. 25. Вероятностное декодирование списком кода Адамара
26. Построение генератора псевдослучайных чисел на основе любой обобщенной односторонней перестановки (теорема Левина-Голдрайха).

27. Построение надежной схемы шифрования с закрытым ключом на основе генератора псевдослучайных чисел.
28. Односторонние обобщенные перестановки с секретом.
29. Определение надежной схемы шифрования с открытым ключом. Построение такой схемы на основе односторонней обобщенной перестановки с секретом.
30. Неинтерактивные протоколы привязки к биту (bit commitment). Построение такой схемы на основе односторонней инъективной функции.
31. Интерактивные протоколы привязки к биту. Построение такого протокола на основе генератора псевдослучайных чисел.
32. Протоколы бросания монетки по телефону. Построение такой схемы на основе протокола “привязки к биту”.
33. Определение надежной схемы аутентификации. Построение такой схемы в предположении необратимости функции Рабина.

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. 372 p.