Программа экзамена по курсу теоретико-сложностные проблемы криптографии (2008/2009).

1. Однолентночные и многоленточные машины Тьюринга. Оценка количества шагов для копирования и для выполнения арифметических операций на одноленточных и двухленточных машинах Тьюринга. Алгоритм быстрого возведения в степень по данному модулю.
2. Моделирование многоленточных машин Тьюринга на одноленточных машинах Тьюринга с квадратичным замедлением. Класс P языков, разрешимых за полиномиальное время. Класс FP функций, вычислимых за полиномиальное время.
3. Равнодоступные адресные машины (PAM). Моделирование PAM на многоленточных машинах Тьюринга.
4. Вероятностные машины Тьюринга (два равносильных определения). Определение вычисления данной функции с ошибкой не более ϵ. Классы FBPP и BPP. Независимость этих классов от разрешенной вероятности ошибки.
5. Вероятностный алгоритм Миллера–Рабина распознавания простоты данного числа.
6. Схемы из функциональных элементов. Классы n.u.P и P/poly. Включение класса P в класс n.u.P
7. Совпадение классов n.u.P и P/poly. Включение класса BPP в класс P/poly.
8. Класс NP. Примеры языков из класса NP. Классы PSPACE и EXP. Включение класса NP в класс PSPACE и класса PSPACE в класс EXP.
9. Сводимость Карпа и основные ее свойства. Теорема Кука-Левина о NP-полноте задачи выполнимости схем из функциональных элементов.
10. NP-полнота задачи о выполнимости 3-КНФ. NP-полнота задачи КЛИКА. NP-полнота задачи о вершинном покрытии.
11. NP-полнота задачи о сумме подмножества.
12. Определение сильно необратимой и сильно односторонней функции. Примеры предположительно сильно односторонних функций. Слабо необратимые функции и слабо односторонние функции. Если P=NP, то односторонних функций нет.
13. Построение односторонней функции из любой слабо односторонней функции.
14. Определение статистически и вычислительно неотличимых последовательностей случайных величин. Свойства вычислительно неотличимых последовательностей случайных величин.
15. Частично односторонние функции. Функция Рабина, функция RSA, дискретная экспонента. Построение односторонней функции из любой частично односторонней функции.
16. Определение генераторов ПСЧ типа $\mathrm{poly}(n) \to \mathrm{poly}(n)$ и $\mathrm{poly}(n) \to \infty$. Генераторы и слабо односторонние функции.
17. Трудный бит для данной функции. Построение генератора, исходя из обобщенной перестановки и трудного бита для нее.
18. Неотличимость случайных величин по Яо. Эквивалентность неотличимости по Яо и вычислительной неотличимости (в случае, когда одна из величин равномерно распределена).
19. Лемма о декодировании списком кода Адамара.
20. Теорема Левина-Голдрейха о трудном бите для данной односторонней функции.
21. Схема шифрования одного сообщения с закрытым ключом. Построение такой схемы на основе генератора ПСЧ.
22. Псеводслучайные функции. Построение псевдослучайной функции на основе генератора ПСЧ типа $n \to 2n$.
23. Схема шифрования нескольких сообщений с закрытым ключом. Построение такой схемы на основе псевдослучайных функций.
24. Односторонние частичные перестановки с секретом (trapdoor permutations). Примеры предположительно односторонних перестановок с секретом.
25. Схема шифрования с открытым ключом. Построение такой схемы на основе односторонней частичной перестановки с секретом.

26. Неинтерактивные протоколы привязки к биту (bit commitment). Построение такого протокола на основе односторонней инъективной функции с полиномиально разрешимой областью определения.
27. Интерактивные протоколы привязки к биту. Построение такого протокола на основе генератора псевдослучайных чисел.
28. Протоколы бросания монетки по телефону (электронная монета). Построение такого протокола на основе протокола привязки к биту.
29. Интерактивные доказательства. Интерактивное доказательство неизоморфности двух графов.
30. Неразглашение информации интерактивным алгоритмом. Лемма о неразглашении информации при последовательном выполнении неразглашающего алгоритма.
31. Протоколы аутентификации. Построение протокола аутентификации на основе необратимости функции Рабина.
32. Схемы цифровой подписи: общее определение. Схемы цифровой подписи одного бита. Схемы одноразовой цифровой подписи сообщения фиксированной длины.
33. Семейства хэш-функций с трудно обнаружимыми коллизиями (свободные от коллизий хэш-функции.) Схема одноразовой цифровой подписи сообщения произвольной длины на основе семейства хэш-функций с трудно обнаружимыми коллизиями.
34. Семейства пар функций с трудно обнаружимыми зацеплениями. Использование таких семейств для построения семейств хэш-функций с трудно обнаружимыми коллизиями.
35. Схема цифровой подписи произвольного количества сообщений на основе одноразовой цифровой подписи сообщения любой длины.
36. Схема Лампорта подписи одного сообщения произвольной длины на основе одноразовой цифровой подписи сообщения фиксированной длины и семейства односторонних хэш-функций (без доказательства).
37. Интерактивное доказательство с нулевым разглашением для раскрашиваемости графов (с использованием протокола привязки к биту).
38. Oblivious transfer (забывающая передача). Улучшенные перестановки с секретом. Построение забывающей передачи с помощью улучшенной перестановки с секретом.

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.