Программа курса “Математическая криптография” ВШЭ 2014 года.

1. Односторонние функции (сильно и слабо). Обратимость любой функции при условии P=NP.
2. Теорема Левина - Гольдрайха о преобразовании слабо односторонней функции в сильно одностороннюю.
3. Обобщение понятия односторонней функции — частичные односторонние функции (с равномерным распределением). Односторонние перестановки. Функция Рабина, функция RSA, дискретная экспонента.
4. 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.
5. Понятие трудного бита для данной функции. Лемма о трудном бите (конкатенация значения функции и трудного бита неотличима от конкатенации значения функции и случайного бита).
6. Построение генератора ПСЧ, исходя из односторонней перестановки с трудным битом.
7. Построение генератора ПСЧ с произвольной степенью расширения из генератора $p(n) \to p(n) + 1$.
8. Теорема о вероятностном декодировании списком кода Адамара.
9. Теорема Левина-Гольдрайха о трудном бите для односторонних функций (доказательство по модулю теоремы о вероятностном декодировании списком кода Адамара).
10. Семейства псевдослучайных функций (ПСФ). Сильный и слабый варианты определения. Построение псевдослучайных функций исходя из генератора ПСЧ.
11. Односторонние перестановки с секретом (trapdoor permutations). Примеры. Трудный бит для необратимой перестановки с секретом.
12. Одноразовые схемы шифрования с закрытым ключом (СШЗК, симметричные схемы). Построение СШЗК на основе генератора ПСЧ.
13. Многоразовые схемы шифрования с закрытым ключом. Построение многоразовой СШЗК на основе семейства ПСФ и одноразовой СШЗК.
14. Схемы шифрования с открытым ключом (ШОК, асимметричные схемы). 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.
15. Неинтерактивные протоколы привязки к биту (НПБ). Построение НПБ на основе односторонней перестановки.
16. Интерактивные алгоритмы. Интерактивные протоколы привязки к биту (ИПБ).
17. Неразглашение информации интерактивным алгоритмом. Лемма о неразглашении информации в результате последовательного повторения алгоритма.
18. Интерактивные протоколы привязки к биту (ИПБ). Построение ИПБ на основе генератора ПСЧ

19. Протоколы бросания монетки и игры в орлянку по телефону. Построение таких протоколов на основе протокола привязки к биту.
20. Протоколы идентификации с закрытым ключом. Построение такого протокола на основе семейства ПСФ.
21. Неразглашение информации. Теорема о последовательном повторении неразглашающего интерактивного алгоритма.
22. Протоколы идентификации с открытым ключом. Построение протокола идентификации с открытым ключом на основе необратимости функции Рабина.
23. 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.
24. Протоколы цифровой подписи. Протокол цифровой подписи одного бита и протокол одноразовой подписи сообщений фиксированной длины на основе односторонней функции.
25. Протокол одноразовой цифровой подписи сообщений произвольной длины (на основе СТОК и протокола одноразовой подписи сообщений фиксированной длины).
26. 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.