Программа экзамена по курсу теоретико-сложностные проблемы криптографии (2008). Часть 2.

1. Определение необратимой и односторонней функции. Примеры предположительно односторонних функций. Слабо необратимые функции и слабо односторонние функции.
2. Построение односторонней функции из любой слабо односторонней функции (теорема Голдрейха).
3. Определение статистически и вычислительно неотличимых последовательностей случайных величин. Свойства вычислительно неотличимых последовательностей случайных величин.
4. Частично необратимые функции. Примеры: функция Рабина, функция RSA, функция Блюма–Микэли. Построение односторонней функции из любой частично односторонней функции. Если P=NP, то односторонних функций нет.
5. Определение генераторов ПСЧ типа $\mathrm{poly}(n) \to \mathrm{poly}(n)$ и $n \to \infty$. Генераторы и слабо односторонние функции.
6. Расширители. Построение генератора, исходя из расширителя. Трудный бит, характеризация расширителей в терминах трудного бита.
7. Универсальное семейство хэш-функций.
8. Код Адамара. Вероятностное декодирование списком кода Адамара за полиномиальное время (лемма, используемая в доказательстве теоремы Левина-Голдрейха).
9. Теорема Левина–Голдрейха: построение расширителя, исходя из односторонней обобщенной перестановки.
10. Схема шифрования одного сообщения с закрытым ключом. Построение такой схемы на основе генератора ПСЧ.
11. Псеводслучайные функции. Построение псевдослучайной функции на основе генератора ПСЧ типа $n \to 2n$.
12. Схема шифрования нескольких сообщений с закрытым ключом. Построение такой схемы на основе псевдослучайных функций.
13. Односторонние частичные перестановки с секретом (trapdoor permutations). Примеры предположительно односторонних перестановок с секретом.
14. Схема шифрования с открытым ключом. Построение такой схемы на основе односторонней частичной перестановки с секретом.
15. Неинтерактивные протоколы привязки к биту (bit commitment). Построение такого протокола на основе односторонней инъективной функции с полиномиально разрешимой областью определения.
16. Интерактивные протоколы привязки к биту. Построение такого протокола на основе генратора псевдослучайных чисел.
17. Протоколы бросания монетки по телефону (электронная монета). Построение такого протокола на основе протокола привязки к биту.
18. Протоколы аутентификации. Построение протокола аутентификации на основе 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.