Программа. Криптография

Шокуров А.В.

1. Введение. Предмет математической криптографии. Криптографические протоколы - прикладные и примитивные. Криптографические примитивы. Модель противника.
2. Стойкость криптографических протоколов и криптографических примитивов. Три задачи криптографии - обеспечение конфиденциальности, целостности, неотслеживаемости.
3. Элементы теории сложности вычислений. Вероятностная машина Тьюринга. Классы BPP и RP. Рандомизированные вычисления за полиномиальное в среднем время. Формализация понятия эффективного алгоритма в однородной и неоднородной моделях вычислений.
4. Односторонние функции. Определения сильной и слабой односторонних функций. Теорема Яо об эквивалентности предположений о существовании сильных и слабых односторонних функций.
5. Понятие трудного предиката функции. Теорема Гольдрайха-Левина о существовании у односторонней функции трудного предиката.

6. Криптографически стойкие генераторы псевдослучайных последовательностей. Понятие вычислительной неотличимости семейств распределений вероятностей.
7. Два определения генератора псевдослучайных последовательностей: через неотличимость от равномерно распределенных последовательностей и через тест следующего бита. Теорема Яо об эквивалентности этих определений.
8. Построение генератора псевдослучайных последовательностей исходя из произвольной односторонней перестановки. Теорема Хостада и др. (без доказательства) о необходимом и достаточном условии существования генераторов псевдослучайных последовательностей.
9. Криптосистемы с секретным ключом. Блоковые и потоковые криптосистемы.
10. Атаки на криптосистемы и угрозы безопасности криптосистем. Определение стойкости криптосистемы.
11. Доказательство существования стойкой потоковой криптосистемы с секретным ключом в предположении существования генератора псевдослучайных последовательностей.

12. Генераторы псевдослучайных функций и псевдослучайных перестановок. Определение генератора псевдослучайных функций. Теорема Гольдрайха и др. о существовании генераторов псевдослучайных функций в предположении существования генераторов псевдослучайных последовательностей.
13. Определение генератора обратимых псевдослучайных перестановок. Преобразование Файстеля. Теорема Луби и Ракоффа (без доказательства) о необходимом и достаточном условии существования обратимых псевдослучайных перестановок. 14. Построение доказуемо стойких блоковых криптосистем исходя из генераторов псевдослучайных функций или генераторов псевдослучайных перестановок.
15. Схемы электронной подписи. Понятие об аутентификации сообщений. Определение схемы электронной подписи. Определение стойкости для схемы электронной подписи. Схема Лампорта.

16. Криптографические хэш-функции. Определения семейства односторонних хэш-функций и семейства функций с трудно обнаружимыми коллизиями. Теорема Наора и Юнга: из существования односторонних перестановок следует существование семейства односторонних хэш-функций.
17. Применение хэш-функций к преобразованию одноразовой схемы электронной подписи в многоразовую. Теорема Ромпеля (без доказательства) о необходимом и достаточном условии существования стойких схем электронной подписи.
18. Протоколы интерактивного доказательства с нулевым разглашением. Понятие интерактивной пары машин Тьюринга. Определение протокола интерактивного доказательства для языка. Свойство нулевого разглашения: вычислительное, статистическое, абсолютное. Протокол доказательства с абсолютно нулевым разглашением для языка ИЗОМОРФИЗМ ГРАФОВ.
19. Протокол привязки к биту. Понятие блоба. Теорема Гольдрайха и др. (идея доказательства) о существовании протоколов доказательства с нулевым разглашением для всех языков из класса NP. Понятие интерактивной аутентификации.

20. Криптосистемы с открытым ключом. Определение криптосистемы с открытым ключом. Атаки и угрозы для криптосистем с открытым ключом. Определение функции с секретом. Криптосистема Рабина. Доказательство стойкости криптосистемы Рабина в предположении вычислительной трудности задачи факторизации целых чисел.
21. Понятие неотслеживаемости. Системы электронных платежей. Электронная монета. Схема электронной подписи вслепую.