Программа коллоквиума 15 февраля 2012 года по курсу "Теоретико-сложностные проблемы криптографии".

1. Однолентночные и многоленточные машины Тьюринга. Время работы и память как меры сложности. Оценка количества шагов для переворачивания слова. Полиномиальные машины Тьюринга (по времени и памяти).
2. Равнодоступные адресные машины, меры сложности: количество операций, длина машинного слова, количество использованных регистров. Полиномиальные PAM (по всем трем мерам сложности). Моделирование машин Тьюринга на PAM.
3. Моделирование PAM на машинах Тьюринга. Классы полиномиально вычислимых функций и полиномиально разрешимых предикатов. Независимость этих классов от вычислительной модели.
4. Схемы из функциональных элементов. Верхняя оценка $O(n2^n)$ схемной сложности любой булевой функции. Схемы полиномиального размера для сложения и умножения.
5. Вероятностные полиномиальные алгоритмы. Уменьшение вероятности ошибки с помощью повторения. Классы BPP и FBPP. Вероятностный полиномиальный алгоритм проверки полиномиального тождества.
6. Класс nuP. Включение P в nuP. Класс P/poly и его совпадение с классом nuP. Включение BPP в nuP.
7. Класс NP. Примеры языков из NP: составные числа, изоморфные графы, выполнимость формул и схем, 3-раскраска, Сумма подмножества, Разбиение, Вершинное покрытие. Сводимости задач (по Карпу). Определение NP полной и NP трудной задачи.
8. Теорема Кука-Левина об NP полноте задачи выполнимости схем.
9. NP полнота задач 3-КНФ, КЛИКА, ВершинноеПокрытие,
10. NP полнота задач 3-раскраска и СуммаПодмножества.
11. Односторонние функции (сильно и слабо). Обратимость любой функции при условии P=NP.
12. Теорема Левина - Гольдрайха о преобразовании слабо односторонней функции в сильно одностороннюю.
13. Обобщение понятия односторонней функции — частичные односторонние функции (с равномерным распределением). Односторониие перестановки. Функция Рабина, функция RSA, дискретная экспонента.