Современные задачи криптографии

Презентация курса

Юрий Лифшиц

Математико-Механический Факультет
Санкт-Петербургского Государственного Университета

Сентябрь 2005

Сегодня

- Программа курса и семинара
- Оргвопросы
  - Выбор времени
  - Рассылка
  - Требования к экзамену и зачету
  - Раздача тем на семинар
- Ваши вопросы

Программа курса

- Криптографические протоколы
  - Разделение секрета, подкидывание монетки
  - Покер по телефону, византийское соглашение
  - Электронные выборы, электронные деньги
  - Беспамятная передача данных
  - Многосторонние секретные вычисления
- Доказательства с нулевым разглашением
  - Примеры
  - Применение
- Псевдослучайные генераторы
  - Построение и использование
  - Псевдослучайные функции

Необходимые знания

Криптография активно пользуется основными понятиями:

- Теории сложности
- Теории чисел
- Теории вероятностей

Обязательных требований нет. Но вам будет проще, если вы уже знаете:

- Что такое класс NP?
- Что такое квадратичный вычет и первообразный корень?
- Что такое *распределение*?

Оргвопросы

- Статус курса и семинара
  - Годится для всех курсов, кафедры информатики, алгебры и СП
- Оценка за спецкурс
  - Решение задач + экзамен
- Зачет за семинар
  - Доклад на семинаре или электронный конспект лекции

Время проведения

Варианты:

- Четверг, 4-ая и 5-ая пары
- Вторник, 4-ая и 5-ая пары
- Среда, 4-ая и 5-ая пары
- Другие предложения?

Темы для семинара

1. Блочные шифры
2. Односторонние функции с секретом
3. Криптосистема RSA
4. Цифровая подпись
5. Хэш-функции
6. Аутентификация сообщений
7. Гомоморфное шифрование
8. Стеганография
9. Квантовая криптография

Есть желающие взять тему?

Делаем рассылку

Все желающие - запишите на мой листок свое имя, фамилию, группу и e-mail

Последний слайд

Контакт: **Юрий Лифшиц**

e-mail: yura@logic.pdmi.ras.ru

web: http://logic.pdmi.ras.ru/~yura/crypto.html

Рассылка: crypto СОБАКА logic.pdmi.ras.ru

Последний слайд

Контакт: **Юрий Лифшиц**

e-mail: yura@logic.pdmi.ras.ru

web: http://logic.pdmi.ras.ru/~yura/crypto.html

Рассылка: crypto СОБАКА logic.pdmi.ras.ru

Вопросы?