

Современные задачи криптографии

Юрий Лифшиц

Спецкурс и спецсеминар для 1-5 курсов.

Оргсобрание и презентация курса: 12 сентября, понедельник, 13-00,
аудитория 2412.

Примерное содержание курса:

- Доказательства с нулевым разглашением
 - Разделение секрета
 - Псевдослучайные генераторы
 - Задача о византийском соглашении
 - Беспамятная передача данных
 - Многосторонние секретные вычисления
 - Электронные выборы
 - Квантовая криптография
-

Предположительное время проведения: спецкурс - четверг, 4-ая пара;
спецсеминар - 5-ая пара.

Курс читается в рамках учебной программы лаборатории системного программирования и информационных технологий (SPRINT Lab), созданной при поддержке компании Интел.

Присылайте пожелания по времени проведения на адрес:

`yura@logic.pdmi.ras.ru`