Министерство образования и науки Российской Федерации
Московский физико-технический институт
(Государственный университет)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ Т. В. Кондранин
"___" _____ 20_ _ г.

Факультет управления и прикладной математики
Кафедра системного программирования

ПРОГРАММА

по курсу: ТЕОРЕТИЧЕСКАЯ КРИПТОГРАФИЯ

по направлению 511660
курс 4
семестр 7
лекции 68 часов — экзамен - 7 семестр
практические (семинарские)
занятия 0 часов
лабораторные занятия 0 часов

Программу составил: Н.П.Варновский

Программа обсуждена на заседании кафедры 25 августа 2009 г.

Программа обсуждена и одобрена на методической комиссии факультета
"___" _____ 20_ _ г.

Председатель методической комиссии ФУПМ
чл.-корр. РАН — Ю.А. Флеров

ТЕОРЕТИЧЕСКАЯ КРИПТОГРАФИЯ

Лекция 1. Введение. Предмет теоретической криптографии. Криптографические протоколы - прикладные и примитивные. Криптографические примитивы. Модель противника.

Лекция 2. Стойкость криптографических протоколов и криптографических примитивов. Три задачи криптографии - обеспечение конфиденциальности, целостности, неотслеживаемости.

Лекция 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.

Лекция 4. Класс P/poly. Теорема об эквивалентности двух определений эффективного алгоритма: через класс P/poly и через семейство схем полиномиального размера. Вложение класса BPP в класс P/po1y.

Лекция 5. Односторонние функции. Определения сильной и слабой односторонних функций. Теорема Яо об эквивалентности предположений о существовании сильных и слабых односторонних функций.

Лекция 6. Понятие трудного предиката функции. Теорема Гольдрайха-Левина о существовании у односторонней функции трудного предиката.

Лекция 7. Криптографически стойкие генераторы псевдослучайных последовательностей. Понятие вычислительной неотличимости семейств распределений вероятностей.

Лекция 8. Два определения генератора псевдослучайных последовательностей: через неотличимость от равномерно распределенных последовательностей и через тест следующего бита. Теорема Яо об эквивалентности этих определений.

Лекция 9. Построение генератора псевдослучайных последовательностей исходя из произвольной односторонней перестановки. Теорема Хостада и др. (без доказательства) о необходимом и достаточном условии существования генераторов псевдослучайных последовательностей.

Лекция 10. Криптосистемы с секретным ключом. Блоковые и потоковые криптосистемы.

Лекция 11. Атаки на криптосистемы и угрозы безопасности криптосистем. Определение стойкости криптосистемы.

Лекция 12. Доказательство существования стойкой потоковой криптосистемы с секретным ключом в предположении существования генератора псевдослучайных последовательностей.

Лекция 13-14. 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.

Лекция 15-16. Определение генератора обратимых псевдослучайных перестановок. Преобразование Файстеля. Теорема Луби и Ракоффа (без доказательства) о необходимом и достаточном условии существования обратимых псевдослучайных перестановок.

Лекция 17-18. Построение доказуемо стойких блоковых криптосистем исходя из генераторов псевдослучайных функций или генераторов псевдослучайных перестановок.

Лекция 19. Схемы электронной подписи. Понятие об аутентификации сообщений. Определение схемы электронной подписи.

Лекция 20. Арбитраж. Атаки на схемы электронной подписи и угрозы их безопасности.

Лекция 21. Определение стойкости для схемы электронной подписи. Схема Лампорта.

Лекция 22. Криптографические хэш-функции. Определения семейства односторонних хэш-функций и семейства функций с трудно обнаружимыми коллизиями. Теорема Наора и Юнга: если существуют односторонние перестановки, то существуют семейства односторонних хэш-функций.

Лекция 23. 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.

Лекция 24. Протоколы интерактивного доказательства с нулевым разглашением. Понятие интерактивной пары машин Тьюринга. Определение протокола интерактивного доказательства для языка.

Лекция 25. Свойство нулевого разглашения: вычислительное, статистическое, абсолютное. Протокол доказательства с абсолютно нулевым разглашением для языка ИЗОМОРФИЗМ ГРАФОВ.

Лекция 26-27. 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.

Лекция 28. Криптосистемы с открытым ключом. Определение криптосистемы с открытым ключом. Атаки и угрозы для криптосистем с открытым ключом.

Лекция 29. Определение функции с секретом. Криптосистема Рабина. Доказательство стойкости криптосистемы Рабина в предположении вычислительной трудности задачи факторизации целых чисел.

Лекция 30. Вероятностные криптосистемы с открытым ключом и их стойкость.

Лекция 31. Понятие неотслеживаемости. Системы электронных платежей. Электронная монета.

Лекция 32. Схема электронной подписи вслепую.

Пояснительная записка

Цель учебного курса – ознакомить студентов, специализирующихся в области программирования, с основными проблемами, возникающими в современной теоретической криптографии, основными понятиями и криптографическими примитивами, являющимися основой построения доказуемо стойких криптосистем и протоколов.

Основное внимание в курсе уделяется математически строгим определениям основных понятий современной теоретической криптографии и доказательствам стойкости различных типов криптосистем и криптографических протоколов.