Программа курса «Введение в математическую криптографию» (осенний семестр 2015/2016 уч. г.)

Введение. Предмет математической криптографии. Криптографические протоколы и криптографические примитивы. Параметр стойкости. Модель противника. Понятие об атаках на криптографические протоколы и об угрозах стойкости криптографических протоколов. Общее понятие стойкости криптографического протокола против данной угрозы на основе данной атаки. Три задачи криптографии — обеспечение конфиденциальности, целостности, неотслеживаемости. Вспомогательные понятия, используемые в курсе: полиномиальный параметр, пренебрежимо малая функция, статистическое расстояние, статистическая неотличимость, вычислительная неотличимость и т. д.

Сильно и слабо односторонние функции и перестановки. Построение сильно односторонней функции на основе произвольной слабо односторонней функции (теорема Яо). Сильно (слабо) односторонние семейства функций и их связь с сильно (слабо) односторонними функциями. Примеры гипотетически односторонних семейств функций.

Трудные и трудно аппроксимируемые функции и предикаты. Связь между трудными и трудно аппроксимируемыми функциями. Теорема Гольдрайха — Левина о трудном предикате.

Псевдослучайные генераторы (генераторы псевдослучайных последовательностей). Два определения псевдослучайного генератора: через вычислительную неотличимость и через непредсказуемость следующего бита. Теорема Яо об эквивалентности этих определений. Увеличение разности длин выхода и входа псевдослучайного генератора. Теорема Хостада и др. о необходимом и достаточном условии существования псевдослучайных генераторов (без доказательства). Построение псевдослучайного генератора исходя из произвольной односторонней перестановки.

Псевдослучайные семейства функций. Построение псевдослучайного семейства функций на основе произвольного псевдослучайного генератора, удваивающего длину входа (теорема Гольдрайха и др.).

Псевдослучайные и сильно псевдослучайные семейства перестановок. Преобразование Файстеля. Построение полиномиально инвертируемого псевдослучайного семейства перестановок на основе произвольного псевдослучайного семейства функций (теорема Луби — Ракоффа, без доказательства). Построение полиномиально инвертируемого сильно псевдослучайного семейства перестановок на основе произвольного псевдослучайного семейства функций (теорема Луби — Ракоффа, без доказательства).