Программа курса «Математическая криптография» (весенний семестр 2020/2021 уч. г.)

1. Предмет математической криптографии. Криптографические протоколы и криптографические примитивы. Три задачи криптографии — обеспечение конфиденциальности, целостности, неотслеживаемости. Параметр стойкости. Понятие об атаках на криптографические протоколы и об угрозах стойкости криптографических протоколов. Модель противника. Общее понятие стойкости криптографического протокола против данной угрозы на основе данной атаки.

2. Полиномиальные параметры и полиномиально перечислимые множества. Односторонние и слабо односторонние функции и перестановки. Существование (слабо) односторонних функций, определенных на $\{0,1\}^*$ и сохраняющих длину, в предположении существования (слабо) односторонних функций, определенных на $\bigcup_{n\in N}\{0,1\}^n$, где N — полиномиально перечислимое множество целых неотрицательных чисел. Пример слабо односторонней функции, не являющейся односторонней (в предположении существования слабо односторонних функций). Построение (без доказательства) односторонней функции (перестановки) на основе слабо односторонней функции (перестановки).

3. Полиномиальная конструируемость. Односторонние и слабо односторонние семейства функций и перестановок. Связь (слабо) односторонних семейств функций со (слабо) односторонними функциями. Примеры гипотетически односторонних семейств функций.

4. Вычислительная неотличимость. Трудные и трудно аппроксимируемые функции и предикаты. Связь между трудностью и трудной аппроксимируемостью функций. Трудные предикаты для односторонних функций. Односторонность полиномиально вычислимой инъективной функции, для которой существует трудный предикат. Теорема Гольдрайха—Левина (без доказательства).

5. Псевдослучайные генераторы. Условие непредсказуемости следующего бита. Теорема Яо об эквивалентности вычислительной неотличимости от семейства равномерных распределений и непредсказуемости следующего бита. Увеличение разности длин выхода и входа псевдослучайного генератора.

6. Теорема Хостада и др. о необходимом и достаточном условии существования псевдослучайных генераторов (без доказательства). Односторонность псевдослучайного генератора, отображающего $\{0,1\}^n$ в $\{0,1\}^{m(n)}$, где функция m инъективна. Построение псевдослучайного генератора на основе произвольной односторонней перестановки.

7. Псевдослучайные семейства функций. Конструкция Гольдрайха—Гольдвассер—Микали псевдослучайного семейства функций на основе псевдослучайного генератора, отображающего $\{0,1\}^n$ в $\{0,1\}^{2n}$ (без доказательства псевдослучайности построенного семейства). Построение псевдослучайного генератора исходя из псевдослучайного семейства функций $(f_{n,d}\colon\{0,1\}^{k(n)} \to \{0,1\}^{m(n)} \mid n \in \mathbb{N},\, d \in \{0,1\}^n)$ такого, что $n < 2^{k(n)}m(n)$ при всех достаточно больших n.

8. Псевдослучайные и сильно псевдослучайные семейства перестановок. Связь псевдослучайных семейств перестановок с псевдослучайными семействами функций. Преобразование Файстеля. Конструкции Луби—Ракоффа псевдослучайного и сильно псевдослучайного семейства перестановок на основе псевдослучайного семейства

функций (без доказательства псевдослучайности и сильной псевдослучайности построенных семейств перестановок).

9. Семейства хэш-функций с трудно обнаружимыми коллизиями. Конструкция Меркле—Дамгора. Построение семейства хэш-функций с трудно обнаружимыми коллизиями в предположении трудности задачи факторизации целых чисел.

10. Специфические и экзистенциальные коллизии функций. Универсальные односторонние семейства хэш-функций. Теорема о композиции для таких семейств. Теорема Ромпеля о существовании универсальных односторонних семейств хэш-функций (без доказательства). Конструкция Наора—Юнга универсального одностороннего семейства хэш-функций на основе односторонней перестановки.

11. Семейства функций и перестановок с секретом. Семейство перестановок RSA. Семейство функций Рабина (по модулям, являющимся числами Блюма). Семейство функций Рабина, ограниченных на элементы нечетного порядка.

12. Элементы теории Шеннона систем секретной связи (secrecy systems). Понятия замкнутой и совершенной системы секретной связи. Нижняя оценка мощности носителя распределения ключей для произвольной совершенной системы секретной связи. Чистые системы секретной связи. Разложение чистой системы секретной связи в дизъюнктное объединение совершенных систем. Система секретной связи Вернама.

13. Системы шифрования (криптосистемы). Системы шифрования с секретным и с открытым ключом. Блоковые системы шифрования. Атаки на системы шифрования. Угрозы стойкости систем шифрования. Построение IND-CPA-стойкой блоковой системы шифрования с секретным ключом на основе псевдослучайного полиномиально инвертируемого семейства перестановок.

14. Построение IND-стойкой (на основе атаки с открытым ключом) блоковой системы шифрования с открытым ключом исходя из семейства F перестановок с секретом и семейства функций, трудного для F. Преобразование блоковой системы шифрования с открытым ключом в систему с открытым ключом, позволяющую шифровать сообщения произвольной длины, с сохранением IND-стойкости на основе атаки с открытым ключом.

15. Протоколы электронной подписи. Атаки на протоколы электронной подписи. Угрозы стойкости протоколов электронной подписи. Теорема Ромпеля о существовании стойких протоколов электронной подписи (без доказательства). Протокол Лэмпорта электронной подписи.

16. Протоколы интерактивного доказательства. Границы полноты и корректности. Абсолютная полнота. Игры Артура и Мерлина. Класс сложностей IP. Пример: протокол интерактивного доказательства для языка КВАДРАТИЧНЫЕ НЕВЫЧЕТЫ.

17. Протоколы доказательства с нулевым разглашением. Вычислительно, статистически и абсолютно нулевое разглашение. Классы сложностей CZK, SZK и PZK. Теорема Бен-Ора и др. о протоколах интерактивного доказательства с вычислительно нулевым разглашением для языков из IP (без доказательства). Теорема Гольдрайха—Микали—Вигдерсона о протоколах интерактивного доказательства с вычислительно нулевым разглашением и с полиномиальным доказывающим для языков из NP (без доказательства). Пример: протокол интерактивного доказательства с абсолютно нулевым разглашением для языка ИЗОМОРФИЗМ ГРАФОВ.