Вопросы к курсу «Криптография на решетках»

1. Пример: протокол Диффи-Хелмана. Определение односторонних функций. Криптосистемы с открытым ключом. Необходимое условие стойкости криптосистем с открытым ключом – существование односторонних функций. Пример таких систем. Криптосистема Эль-Гамаля. Дискретный логарифм. Сложность в наихудшем случае и в среднем. Теорема о сложности в среднем дискретного алгоритма, если имеется сложность в наихудшем случае.

2. Определение решетки. Дискретные абелевы группы и решетки. Абелевы группы конечного и бесконечного порядка. Теорема о базисе конечно порожденной абелевой группы. Ранг абелевой группы. Свойства базисов абелевых групп. Основной параллелепипед. Детерминант решетки. Полные решетки. Критерий полноты решетки.

3. Лемма Минковского о выпуклом теле. Неравенство Адамара. Вторая теорема Минковского. Следствие из теоремы Минковского об оценке длины кратчайшего вектора.

4. LLL-алгоритм нахождения кратчайшего вектора. Задачи SVP и CVP. Нахождение базиса из кратчайших векторов для размерности 2: алгоритм Гаусса. Полиномиальность алгоритма Гаусса. Приведенный базис. Свойства LLL-приведенного базиса. Оценка длины первого вектора в приведенном базисе. Описание LLL-алгоритма. Корректность алгоритма. Полиномиальность.

5. Задача ACVP. Алгоритм решения ACVP.

7. Эквивалентность задач поиска, оптимизации и распознавания для задачи CVP. Задача о рюкзаке. NP-трудность задачи CVP. Сводимость задачи SVP к задаче CVP.

6. Описание метода шифрования Айтаи. Описание NTRU: алгебраическое и геометрическое.