Лабораторная работа №1

Все задания выполняются в ПО SAGE. Ознакомиться и бесплатно скачать данные пакеты можно на официальном сайте: sagemath.org.

Задание 1. **Работа с простыми числами**

Во многих криптосистемах, например, криптосистеме RSA или Рабина используются простые числа. Но как определить, что число простое? Последовательное деление чисел, состоящих из миллиона знаков, не самая лучшая идея. Данную процедуру можно сильно упростить, если воспользоваться тестами на простоту.

1. Реализуйте тест на простоту Миллера-Рабина и продемонстрируйте его выполнение для чисел, состоящих из 10 знаков.
2. Реализуйте тест Ферма. Покажите, что тест Ферма и тест Миллера-Рабина дают разные результаты для некоторых чисел и обоснуйте данные расхождения.

Задание 2. **Криптопримитивы для алгоритмов**

В 1980 году Ральф Меркле опубликовал замечательную работу «Protocols for public key cryptosystems», в которой содержится база современной криптографии. Работу можно считать классикой – в ней сформулированы почти все протоколы, разработанные великими учёными до 80х годов прошлого столетия. В данном задании Вам нужно внимательно изучить труд Меркле, а также реализовать в свободной творческой форме на SAGE два протокола из этой работы:

распределение ключа с помощью дерева аутентификации (глава 6) и протокол отметки о времени (глава 10).

Задание 3. **Поиск дискретного логарифма**

Самостоятельно реализуйте алгоритм Baby-step-giant-step (на модульной арифметике) и алгоритм Полига-Хэллмана для решения задачи дискретного логарифма. Объясните корректность алгоритмов, покажите их временную сложность, объясните, за счёт чего достигается ускорение по сравнению с полным перебором.

Задание 4. **Работа с конечными группами и конечными полями**

Создайте две мультипликативные группы Z^*_{101} и Z^*_{150}.

1. Напишите функцию, которая определяет, является ли группа циклической или нет;
2. Напишите функцию, которая выводит на экран все генераторы групп;
3. Средствами SAGE найдите мультипликативный порядок числа 15 в группе Z^*_{101};
4. Определите количество подгрупп группы Z^*_{150}.

Создайте конечное поле $GF(2^7)$, где α – примитивный элемент.

1. Выведите на экран всё поле;
2. Вычислите $\alpha^{10} + \alpha^{99} - \alpha^{52}$;
3. Найдите минимальный многочлен для элемента α^{15}.

Задание 5. **Задача факторизации**

1. Пусть $N = 537069139875071$. Пусть также известно, что

$$85975324443166^2 \equiv 462436106261^2 \; mod \; N$$

Разложите N на множители, используя эту информацию (не используйте функцию factorize!).

2. Пусть $N = 985739879 \cdot 1388749507$. Найдите x и y такие что $x^2 \equiv y^2 \mod N$, но $x \not\equiv y \mod N$.