Многопрофильная инженерная олимпиада «Звезда»
«Информационная безопасность»

11 класс **Заключительный этап** **2023-2024**

Задания

Требования к оформлению заданий. При проверке заданий учитывается не только ответ, но и само решение. Важно оформлять решения во всех заданиях. Ответы без решения оцениваются не более чем в 1 балл.

Задача 1 *(Максимум 10 баллов)*

Найдите все тройки натуральных чисел *(x, y, z)*, такие что $5^x + 5^y = z^2$ *и* $x, y < 10, z <= 50$

Задание 2 *(Максимум 20 баллов)*

Решите в натуральных числах уравнение 17m − 5n = 1, где m и n лежат в пределах от 1 до 100

Задание 3 *(Максимум 20 баллов)*

Дана последовательность s_n, где s_n - последняя цифра суммы квадратов первых n натуральных чисел, т.е. s_n - последняя цифра числа $1^2+2^2+3^2+...+n^2$. Определите периодичность этой последовательности. Создайте первую перестановку из последовательных уникальных цифр s_n и определите, образуют ли последующие перестановки периодическую последовательность.

Практическое задание. *(Максимум 50 баллов)*

Необходимо разработать и описать алгоритм с выбранными входными параметрами шифра RSA, один из основных методов асимметричного шифрования. Задача включает в себя три основных этапа: генерацию ключей, шифрование и дешифрование сообщений. Вы должны продемонстрировать понимание математических принципов, лежащих в основе RSA, а также умение применять эти принципы на практике.

RSA (названный в честь его создателей Рональда Ривеста, Ади Шамира и Леонарда Адлемана) является одним из первых и наиболее широко используемых алгоритмов асимметричного шифрования. Асимметричное шифрование означает использование различных ключей для шифрования и расшифровки данных. В RSA используются два ключа: открытый ключ для шифрования и закрытый ключ для расшифровки.

Процесс работы RSA включает в себя следующие шаги:

Генерация ключей

1. Выбор двух больших простых чисел (p и q): Эти числа генерируются и хранятся в секрете.

2. Вычисление произведения ($n = p * q$): Число n используется как часть обоих ключей и определяет длину ключа RSA.

3. Вычисление функции Эйлера ($\varphi(n) = (p-1) * (q-1)$): Эта функция используется для генерации ключей.

4. Выбор открытого ключа (e): Число e должно быть взаимно простым с φ(n) и обычно выбирается из набора стандартных значений (например, 65537).

5. Вычисление закрытого ключа (d): Число d вычисляется как мультипликативно обратное к e по модулю $\varphi(n)$, т.е. такое, что $d * e \equiv 1 \pmod{\varphi(n)}$.

После этого открытый ключ (e, n) может быть распространен, а закрытый ключ (d, n) должен быть сохранен в секрете.

Шифрование и расшифровка

1. Шифрование: Чтобы зашифровать сообщение M, отправитель использует открытый ключ получателя. Сообщение преобразуется в число m, меньшее n (например, с использованием кодировки ASCII). Затем зашифрованное сообщение C вычисляется по формуле: $C = m^e \bmod n$.

2. Расшифровка: Чтобы расшифровать сообщение C, получатель использует свой секретный ключ (d). Оригинальное сообщение m восстанавливается путем вычисления: $m = C^d \bmod n$. После этого m преобразуется обратно в текст сообщения.