**Контрольная работа №1. Вариант 1**

**Задача 1.** Удовлетворяет ли следующая хэш-функция основным криптографическим требованиям? Ответ обосновать.

H(m1||m2||...||mt) = m1\*m2\*...\*mt mod 2^n, где mi -- битовая строка длины n, \* -- умножение (mi переводится в число естественным образом).

**Задача 2**.

Для обеспечения сложности майнинга в сети Bitcoin требуется, чтобы хеш блока начинался с определенного количества последовательных нулей. Если текущая сложность требует 20 нулей в начале хеша, сколько возможных хешей удовлетворяет этому условию? Примите во внимание, что хеш представляет собой 256-битное число.

**Задача 3**

Если размер блока в Ethereum увеличен с 1 МБ до 2 МБ, как это повлияет на максимальную пропускную способность сети, если средний размер транзакции остается неизменным?

**Задача 4**

Написать программу для подбора строки d, удовлетворяющие условию: первые 5 байт SHA256(d) меньше константы