Контрольная работа №1. Вариант 2

**Задача 1**

Абоненты А и В обмениваются данными и хотят, чтобы при передаче никто не смог их изменить. Для этого они отправляют не просто сообщение m, а пару m и H(m), где H -- хэш-функция. Решает ли данная схема поставленную задачу? От чего может защитить данная схема? Ответ обосновать

**Задача 2**

Если максимальный размер блока в блокчейне составляет 1 МБ и блоки создаются каждые 10 минут, какова максимальная теоретическая пропускная способность сети в транзакциях в секунду, если средний размер транзакции составляет 250 байт?

**Задача 3**

Если сложность сети Ethereum увеличивается на 10% каждые 14 дней, на сколько процентов увеличится сложность через 70 дней?

**Задача 4**

Написать программу для подбора строки d, удовлетворяющие условию: первые 4 байта SHA256(d) меньше константы