Реализовать вычисление функций.

напишите программу для вычисления функции

1. Написать код Диффи Хелмана (С,С++, С#)

F(x)=2^x %p

p-простое число.

длина числа P- 1024 бита

2. RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — [криптографический алгоритм с открытым ключом](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%BC_%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%BC), основывающийся на [вычислительной сложности](https://ru.wikipedia.org/wiki/%D0%92%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%BB%D0%BE%D0%B6%D0%BD%D0%BE%D1%81%D1%82%D1%8C) [задачи факторизации](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%BA%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D1%86%D0%B5%D0%BB%D1%8B%D1%85_%D1%87%D0%B8%D1%81%D0%B5%D0%BB) больших целых чисел.

X3%n

(n=p\*q)

p-q - простые числа

p-q - 512 бит

n- (1024 бит)

# 3. Алгоритм Рабина-Карпа

# X2% n

# (n=p\*q)

# p-q - 512 бит.

# n-1024 бит.

Алгоритм (вопрос-ответ)

А -> B <начало сеанса> <команда>;

В ->A: случайное число r

r (128 бит);

A: y=f(x);

X=r||s||команда||0....0;

A->B:y

B: X=r||s|| команда||0.....0

y=f(x) и сравнительный

S- секретный ключ (1028)

 А (Брелок) В-Автомобиль

1. В соответствии с заданием рассматривается следующий протокол передачи
команды от брелка (B) к автомобилю (A):
(изначально в авто и брелок записан одинаковый секретный ключ длиной 128
бит минимум. f(x) -- односторонняя функция)

B -> A : номер авто, код команды
A -> B : случайное число длиной 128 бит минимум
B -> A : f (полученное случайное число || секретный ключ || номер авто,
код команды)
Авто вычисляет аналогичную функцию на основе своих данных. Если значение
вычисленной функции совпало с полученным, то выполняет команду. В
противном случае ничего не делает.

2. В качестве односторонних функций (в максимально упрощенном варианте
задания, не на "отлично") предлагается взять
f(x) = 2 ^ x mod p (функция Диффи-Хеллмана)
f(x) = x ^ 3 mod pq (функция RSA)
f(x) = x ^ 2 mod pq (функция Рабина)
По-хорошему, надо было изучить математические свойства этих функций, но
сейчас на это нет времени.

3. Для реализации f(x) необходимо выбрать средство для вычислений с
большими целыми числами (например, библиотеку libgmp). По поводу C#: я
сначала думал, что Вы используете имеющийся там стандартный класс Big
Integer, а оказалось, что это какая-то самоделка, которая неизвестно что
считает.

4. С использованием выбранной библиотеки реализовать 3 варианта протокола
с различными односторонними функциями в виде консольных приложений с
выводом на экран получающихся чисел.

5. Сравнить варианты по времени выполнения.