Too secure system

Bob worries about security too much and decided to change the original Pedersen commitment scheme adding there several steps. Find the vulnerability in Bob's system!

Initialization

1) Choose two big primes p and q such that $q|(p-1)$ and choose $g \in Z_p^*$ of order q.
2) Choose $x \in \mathbb{Z}_q^*$. x is our secret.
3) Compute $G = g^x \; mod \, p$
4) Transform G into G': 1024-bit binary number with big endian.
5) Using hash-function SHA-512, compute $a = SHA512(G')$
6) Find a': transform binary a into an integer number.
7) Find $\hat{a} = (a'^{a'}) \; mod \; \phi(p)$, where $\phi(p)$ is Euler function.
8) Finally, calculate $h = g^{\hat{a}} \; mod \, p$.

Parameters p and g are well-known and open for everyone.

Commitment

To make a commitment we choose a random r from $\{2, \ldots, p-1\}$ and calculate $c = G \cdot h^r$. The commitment would be c.

Proof

After the decision is made by sender and verifier about the verification of the commitment, sender opens x and r values, and the verifier checks the equality $c = G \cdot h^r$.

Additional information

To get integer value from the string $S = S_1 S_2 \ldots S_n$ of n ASCII characters, use the following formula:

$$func(S) = \sum_{i=0}^{n-1} ASCII(S_{i+1}) \cdot 2^{8 \cdot i}$$

where $ASCII(...)$ is an ASCII value of the character.

Task

Break the system with the following parameters. As a result, you should get the value r_2 which you disclose to the verifier with the string M_2, and the verifier confirms the commitment as with (M_1, r_1) as with (M_2, r_2).

The parameters are:

- $p =$120391024901285091259250190100000124235156172352191276491824701825701950182659 27223
- $g =$107290725793070521848483023224513321924562296190441811050630117415 16558110216720725
- $r_1 =$31245182471
- $M_1 =$ 'Hi! I am Vadim Davydov from ITMO University'
- M_2 = 'Transfer the points for easy task to this team'