Crack the Cipher

The Background

There is a terrorist organization onlined called the Society of Prevention of Cats (SPCAT)…they hate cats. Members of this organization often lurk in websites such as reddit to harass, demean, and verbally abuse anyone who posts heart warming content related to cats. Recently, our spy on the inside has revealed that the Society has somehow managed to doxx a few thousand reddit cat owners. They intend to kidnap all of their cats, and hold them up for a ransom of dramatic camera zoom…one million dollars.

As a member of the Interpol (internet police), you have been assigned on the case, your job is to destroy that database, stop the Society, and save the world (cats).

What used to stand in your way is the presence of 7 layers of proxies put in place by “C1pher”…the Society’s most l33t hacker. Luckily, “C1pher” happens to be a pompous know-it-all. He recently stumbled on a medium article about RSA encryption, and decided to “upgrade” his defenses by tearing down his 7 proxies and replacing it with an authentication system created using his mad encryption skills (that he picked up from a 20 minute medium article…that was incorrect in the first place).

Even luckier for you is the fact that “C1pher” isn’t aware that his premium l33thub subscription just expired, and as a result, his source code is now in a public repository. Before he managed to crowdfund for the fees and make his repo private, you managed to find out how his authentication system works:

The Challenge

the encryption formula is simply:

```
y = SHA256(K::f(x))
```

where:

- k is a positive integer
- x is a posive integer
- f(x) is a secret function of x, which outputs a floating point number rounded up to 3 decimal places

e.g. for K = 1234 and f(x) = 1.123, y = `SHA256("1234::1.123")`

The authentication process is as follows:

1. user sends a authentication request to the server
2. server will respond with a challenge containing:

- SHA265 string value of Y
- positive integer value of X
- difficulty multiplier D

3. user will respond to the challenge with the correct value of K
4. server will authenticate you

The Hint

"C1pher" also included the following hint for f(x):

Assuming that the daily number of cat posts uploaded on reddit are independent and identically distributed, where Cn = # of cat pictures uploaded on the nth day, we have a sequence:

C0 , C1 , C2.... Cn

(Note: All days from 0 through n are in the future.)

For any nth day, if Cn exceeds C0 for the first time since C0, it is considered a terrible day for SPCAT, and "C1pher" will be forced to work overtime to post anti-cat propaganda on reddit, so this day is noted as T (for terrible).

C1pher is interested in the expected value of T, but realized that it is unbounded unless given some constraints.

Suppose T <= x, where x is an integer, what is the expected value of T?

i.e.

$$f(x) = E[T|T <= x]$$

Requirement

Expose a POST endpoint /cipher-cracking on your application.

The format

Sample input JSON

You will receive 30 challenge sets in the following format as JSON request body.

```
[{"D": 1, "X": 12321, "Y": "sha256hash", "est_mins" : 1.5}]
```

D represents difficulty, it starts at 1 and will increase gradually.

Sample output JSON

Respond with an array of numbers representing the correct values of K in the following format as JSON response body.

```
[123, 321, 29582]
```

The more K you get correct, the more score you will get.

Note: Numbers in sample input/output are fabricated.

Constraints

You will have a 30 second timeout.

For this challenge, your known scope is:

$$0 < f(x) < 100$$

$$0 < x < 10^{D+5}$$

$$0 < k < 10^{D}$$