Forging a signature CTF

Tuong Nguyen

September 2019

In this challenge, we have to create a fake zero-knowledge proof. We have g as the standard base point of secp256k1 curve, and $h = g^{SHA("CoinbaesRulez")} = g^x$ as another base point.

It's easy to compute

$$y = g^{4011}h^{6420} = h^{4011/x+6420}$$

Finally, we just have to compute the proof. Note that the organizer have a mistake: h instead of g in the proof scheme. Below is my sample code: