Thoughts on the Nostradamus attack article: <https://www.win.tue.nl/hashclash/Nostradamus/>

I was obviously disappointed after reading this article. I feel silly because I don’t know what I expected from this article, I don’t know why I would think this did some actual type of math to produce an accurate guess for the presidential election winner.

After getting past my initial disappointment with the article, it is still quite interesting how they designed hash functions to reveal different, meaningful plaintexts.

I originally thought I might do my project on this, but while I think it is interesting how to design a hash that can be broken, I am more interested in getting a peek into how cryptology might look in a post-quantum computing world. So on to lattice-based cryptography!