



# QUANTUM COMPUTERS WILL BREAK YOUR CRYPTO (BE PREPARED)

Quantum computers are very good at solving puzzles

Cryptography is *all* about solving puzzles

	Security now	Quantum	
AES_128	128	64 bit	
AES_256	256	128 bit	
RSA 2048/3072	112/128	Trivial	

Key length equivalent for RSA: [https://en.wikipedia.org/wiki/Key\\_size](https://en.wikipedia.org/wiki/Key_size)

## HOW TO SOLVE THE POST QUANTUM PROBLEM?

- ▶ Post quantum will come - likely in the next 5-15 years. Or much earlier (see link below)
- ▶ AES256 and other symmetric algorithms likely still secure (but key length greatly reduced: bit length/2)
- ▶ We have **no** quantum safe asymmetric algorithms
- ▶ **Solution: Crypto Agility!** Design everything in ways that allow algorithms to be replaced (as shown throughout the slides)