



THE FUTURE




---

**POST QUANTUM**

# 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)