UC Berkeley, MICS, W202-Cryptography

Week 11 Breakout 2

Quantum Computing

Questions from the Asynchronous (for discussion)

Exercise 12.6 – Quantum Computing

Do some research and look up what is the state of the art of quantum computing (as of the time you are completing this response). Check in particular with relation to cryptography. Answer the following:

(a) What crypto claims are being made by quantum computing advocates?

(b) What claims are made by quantum computing skeptics?

Exercise 12.7: Post-Quantum Cryptography

Explore and do research to determine what the current state of post-quantum cryptography is. Answer the following:

(a) What promising approaches (if any) have been suggested?

(b) How has the crypto community responded to the challenge thrown down by the NSA?

(c) What is the likely midterm forecast (10 to 20 years out) for current cryptographic algorithms and potential new post-quantum cryptography algorithms?