Homework 6

Due: March 22, 2023

All homeworks are due at 11:59 PM on Gradescope.

Please do not include any identifying information about yourself in the handin, including your Banner ID.

Be sure to fully explain your reasoning and show all work for full credit.

Problem 1

Read the following article and share your thoughts for each of the questions below.

1. Prior to Craig Gidney and Martin Ekerå's innovation, how many qubits were expected to be required to reliably factor a 2048-bit RSA key? And after?
2. In what timeline does the article expect 2048 RSA encryption to no longer be secure from quantum computing?
3. Who is at risk if RSA is no longer secure? Consider the implications (and potentially disproportionate impact) of this scenario at multiple levels and sectors of society.

Problem 2

1. [2-3 sentences] In what ways can developers and relevant stakeholders prepare for the advancement of quantum computing?

2. [5-6 sentences] The question above presents itself as an argument for strengthening encryption; your responses on problem 1 have already touched on the potentially dire impact of insecure encryption and widespread reliance on "breakable" systems.

   What are the main ethical justifications for prioritizing the strength of encryption systems? What are the arguments against it (in other words, arguments for imposing limits on encryption)? What responsibilities do encryption service providers owe their clients and the public at large? Think back to the SRC section from recitation, about the tradeoff between individual right to privacy and circumstances that might require access to encrypted data.

Problem 3 (Mind Bender — *Extra Credit*)

Make a video of a short rap, lyric, or skit (1-2 minutes) about quantum cryptography or encryption in general for extra credit! The best video will receive an additional point of extra credit, and recognition on ED.