CMPS 5363 – Cybersecurity – Practice Paper 1 & 2

- Thursday, Feb. 2 midnight: First version of paper submitted to TurnItIn.com. Be sure to use Word and make it “as good as possible” before submitting. (Practice Paper 1)
- Once submitted, email Ranette.halverson@mwsu.edu so that the GRADEMARKS can be released.
- Make corrections based on GRADEMARKS & ORIGINALITY Reports
- Monday, Feb. 6 midnight: Second & Final version of paper submitted to TurnItIn. (Practice Paper 2)

Content of Practice Paper 1 & 2
Watch the next 2 parts of the video, taking notes. (See below for outline of video.) Write a short essay, 1 to 2 pages, including a discussion of the following topics. Try to be concise & brief.
- What is a prime number? What is a semi-prime number? Why are semi-primes hard to factor?
- What is encryption?
- How are prime & semi-prime numbers used in RSA-Public Key Encryption? Explain.
- How are the public key & private key determined? How are they distributed? (Who possessed them?)
- Why is quantum computing a considered a threat to RSA-Public Key encryption?
- How does quantum computing offer the possibility of better encryption?

Rise of the Hackers Video Notes

(3) Encryption Codes – Security (~ 16 - 21 minutes)
James Lyne – SOPHOS
Prime number, Semi-Prime
RSA - Public Key Encryption
  - Public key vs. Private key

(4) Quantum Computing – Computers & Physics (~ 21 - 27 minutes)
Erik Lucero – UC Santa Barbara
Supercomposition
Very Cold
Qubit
Simultaneous Calculations
Breaking encryption or better encryption?

Seth Lloyd – MIT “Quantum Group” (~ 27 – 31 minutes)
Quantum Cryptography
  - Observer Effect
  - Photons – Eavesdropping on quantum messages
  - New key from untampered bits
  - Privacy guaranteed