Cryptography and Data Encryption

Read the book chapters first, then make sure you can answer the questions in the notes. Following that, work on some skills-check problems and exercises. Then take the online quizzes.

Reading 17.4
Skills Check 10, 12, 13, 14, 15, 16, 17, 18, 19, 22, 23, 24
Exercises 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 43, 44, 49, 50, 51, 52
Quiz Take the quiz[1]

17.4

- What is *encryption*?
- What are some uses of cryptography in our world?
- Describe the *Caesar cipher*, then use it to encrypt the message "HANOVERCOLLEGE".
- How would we decrypt a message encrypted via the Caesar cipher?
- If we associate the numbers 0 through 25 to the letters A through Z, how can we mathematically represent the Caesar cipher?
- Describe the *Decimation Cipher*, and use it, with multiplier *5*, to encrypt the message "HANOVERCOLLEGE".
- How does a *linear cipher* work? How are the Decimation and Caesar cipher special cases of it?
- Describe the *Vigenere cipher*, and use it with keyword MATH to encrypt the message "HANOVERCOLLEGE".
- How do we *add* binary strings? What happens if we add the same string twice?
- Read carefully through the "Public Key Cryptography" section and describe the process, and what problem it solves.

[1] https://moodle.hanover.edu/mod/quiz/view.php?id=5200