CISC 2210 – Introduction to Discrete Structures

Reading Assignment: Number Theory and Cryptography

Everything is made easy? by Randell Heyman.

The videos listed below can help you gain a better understanding of modern cryptography and the math behind it via examples. Note, that the order among the videos is not perfect because sometimes later videos explain concepts in earlier videos.

- The Lazy Mathematician: `https://youtu.be/FdmApk9V2-w`
- Modular arithmetic: `https://youtu.be/2zEXtoQDpXY`
- Modular exponentiation: `https://youtu.be/tTuWmcikE0Q`
- The Greatest Common Divisor: `https://youtu.be/klTIrnovoEE`
- The Chinese Remainder Theorem: `https://youtu.be/ru7mWZJlRQg`
- Euler's totient function `https://youtu.be/EcAT1XmHouk`
- Fermat's little theorem `https://youtu.be/oT7kRlh1nVQ`
- Euler's theorem `https://youtu.be/FHkS3ydTM3M`
- Modular inverse: `https://youtu.be/mgvA3z-vOzc`
- How encryption works: `https://youtu.be/IBocnou79yI`
- RSA code: `https://youtu.be/t5lACDDoQTk`

Journey into cryptography: by Khan Academy.
`https://www.khanacademy.org/computing/computer-science/cryptography`

- Watch the videos in the "Ancient Cryptography" and "Modern Cryptography" chapters and explore their "Exploration" sections.
- Study the "Modular Arithmetic" chapter and practice its "Practice" sections.
- Bonus I: Study the "Ciphers" chapter and challenge yourself with the "Cryptography challenge 101" chapter.
- Bonus II: watch the videos in the "Primality Test" and "Randomized algorithms" chapters.