COSC/MATH 314 Cryptography

Class Log

Professor: Marius Zimand

- Sept. 7. Topics: Mathematical justification for the attack against Vigenere cipher. Read Section 2.3 in the textbook.

  Hill cipher- Read section 2.7 in the textbook.

- Sept. 5. Topics: Topics: the substitution cipher and an example of how to break it with the frequency attack (the attack is posted on the course web site). (

  Then we moved to the Vigenere cipher, and discussed a ciphertext-only attack. Read Section 2.3 in the textbook.

- Aug. 31. Topics: Shift Cipher (Section 2.1 in the textbook); Affine cipher (Section 2.2).

- Aug. 29. We discussed the syllabus, logistical aspects, and I presented the structure of the course, and introduced the basic terminology.

  We introduced some basic notions: plaintext, ciphertext, encryption, decryption, ciphertext-only attack, known plaintext attack, chosen plaintext attach, chosen ciphertext attack.

  Services of a cryptosystem: confidentiality, data integrity, authentication, nonrepudiation.

  Read the posted slides.

- Aug. 22. Here I'll keep the class log: a concise list of the concepts covered in class, and pointers to reading material.