COSC/MATH 314 Cryptography

Class Log

Professor: Marius Zimand

- Sept 14. Topics: We have discussed how to define rigorously the fact that an encryption scheme is secure or not. There are two types of security: perfect security, and computational security. Perfect security means intuitively that the attacker does not get any additional information from the ciphertext (compared to the information the attacker had before seeing the ciphertext), no matter how long time the attack takes. One-time is perfectly secure, but it is impractical. Shannon Theorem shows that any encryption scheme that has perfect security is impractical because it requires that the number of keys should be greater or equal to the number of messages. The other type of security is *computational security*: we require that no attacker that does N operations (where N is a huge number such as 2^{128}) will get additional information.

  Read my notes (posted on the course web site)

  `http://orion.towson.edu/~mzimand/cryptostuff/N2-SecurityNotion.pdf`

- Sept 12. Topics: Rotor machines and Enigma (textbook, section 2.12), one-time pad (section 2.9). We also started the discussion on how to formally define what security means, see Sept 14.

- 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.