CSI 30 LECTURE NOTES (Ojakian)

Topic 12: Cryptography

OUTLINE
(References: 4.6)

1. Shift Ciphers
2. RSA Public Key Cryptography

---

1. Cryptography - Basic setup

(a) Alice wants to send a secret message to Bob

(b) But Eve is eavesdropping.

(c) Competing goals:

i. Making Codes.
Alice and Bob want to devise a scheme for sending secret message that Eve cannot gain access to.

ii. Breaking Codes.
Eve wants to figure out how to crack the secret and read the hidden message.

(d) Terminology

i. Plaintext: The message to be sent (from Alice to Bob), in original form.

ii. Encryption: Putting plaintext into coded form (Alice does this).

iii. Decryption: Determining plaintext from coded message (Bob does this); i.e. the inverse of the encryption function.

(e) To use mathematics:

i. Use some method for converting natural language to numbers (this is simple translation! not encryption!)

ii. Example: A = 0, B = 1, etc

2. Cryptography - Shift Cipher

Simple example. More serious one at later topic.

(a) Pick a shift value k: $0 < k < 26$.

(b) Encryption: Letter x is mapped to $x + k \bmod 26$

(c) Decryption: Letter y is mapped to $y - k \bmod 26$

(d) Example 5 (Section 4.6): Breaking a code.

(e) Do group sending, with Alice, Bob, and Eve

3. Affine ciphers: better but they still suck! ...
   (a) Example 3 in section 4.6
4. Exercises
   (a) Section 4.1: 2, 5, 6, 7, 8, 15 - 18
   (b) Section 4.1: 26 - 29 (where "mod" is the same as "%")
   (c) Section 4.1: 30 - 35, 52
   (d) Section 4.6: 1, 2, 3 (also give the result of the encryption BEFORE "translating the numbers back into letters")
   (e) Section 4.6: 4 - 13 (shift and affine ciphers)
5. Public Key Cryptography - Basic setup
   (a) Cryptography from Caesar to 1976: Private Key
   (b) What is private key cryptography? (ex: k is shift cipher, or the pair (a, b) for affine cipher)
   (c) What is public key cryptography?
      i. RSA encryption: A version of public key cryptography
      ii. Understand how odd this seems at first!
      iii. Two tools for RSA: Modular Inverse, Modular Exponentiation
6. Doing RSA
   (a) Note on translating words to numbers.
      i. We will have a max number we can send: $< n$.
      ii. So max number of letters:
      maximum number of concatenated 25's so that $2525 \cdots 25 < n$.
   (b) See RSA Handout.
   (c) Examples.
      i. Small example: $p = 3$, $q = 11$, $e = 3$. Send "4"
      ii. Encryption example. Example 8 (Section 4.6).
      iii. Decryption example. Example 9 (Section 4.6).
   (d) Do group work of sending message - just Alice and Bob
   (e) Prove it with Fermat's Little Theorem and Chinese Remainder Theorem.
7. Exercises

   Section 4.6: 24 - 27