CSI 30 LECTURE NOTES (Ojakian)

Topic 13: Cryptography

OUTLINE
(References: 4.6)

1. RSA Public Key Cryptography

---

1. 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
2. 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.
3. Exercises
   Section 4.6: 24 - 27