Homework 1 – due next Monday before class

Rules:

- Any student who sends the HW to the mailing list will get a 0
- Work alone
- Read the problems carefully!
- DO NOT include the text of the problems in your submission
- Use only plain ASCII text for submission
- DO NOT type more than 80 characters per line!
- DO NOT send it as email attachment
- DO NOT send me both text and HTML
- EMAIL to gts@ics.uci.edu by 9:30am of the due date
- Spell-check your answers
- Late submissions will not be accepted
- Answers such "yes", "no", "secure", "insecure", etc., will get no credit!
- Explain your answers and your reasoning without being too verbose. Use consistent notation!

Homework 1 (contd)

Problem 1

- Refer to Problem 3.2 in Stinson book (page 110).

Problem 2

As we already know, when there is a lot of data to encrypt,
using a block cipher (such as DES EBC mode) is insecure because
of the block permutation attack. In other words, blocks of encrypted data
can be swapped without the receiver (decryptor) noticing.

One way to fix this problem is to use the Chained-Block-Cipher (CBC)
encryption mode. However, CBC mode has problems; in particular,
if there is an error in one encrypted block, the data following
it will be lost and/or will have to be re-sent.

Suggest a secure way to address these issues. The rules of the game are:

- Use must only the basic block cipher (ECB mode)
- Your solution must be resistant to the block permutation attack
- Your solution must be resistant to the loss of any number of encrypted data blocks

Homework 1 (contd)

Problem 3

Let X be the last 4 digits of your Student ID. If X starts with a zero, let X be the first 4 digits of the ID.

- Find the smallest prime number greater than X, let's call it P. Explain how you found it.
- Find the largest prime number smaller than X, let's call it Q.
- Find Ö(P). Explain how you found it.
- Find X^{-1} mod P, i.e., the inverse of X in Z_P . Explain how you found it.
- Let n=PQ. Find Ö(n) and explain what it means.

Problem 4

Consider the following ways to "strengthen" DES:

DESv: E (K2, K1 ⊕ M)
DESw: K1 ⊕ E (K2, M)

Show that both these proposals do not increase the work needed to break the cryptosystem using brute-force key search. That is, show how to break these schemes using on the order of 2^{56} DES encryptions/decryptions. You may assume that you have a moderate number of (plaintext, ciphertext) pairs.