CSCI 6634/4534 – Cryptography – HW 1 – 24 Spring – Due (on Canvas): 2/21/24 Wednesday 10.00 pm

- Please read the policy on **hw guidelines (both paper and pencil and programming problems), late homework and plagiarism** (in the course outline handed out on the first day) and remember that I enforce these policies.
- The extra credit problems are to be done separately and should be handed in near the end of the semester, exact date to be announced later. What has to be turned in for the EC programming problems will also be announced later..
- The textbook uses the same numbering system for "Review Questions" and for "Problems." When you are asked to do a particular problem from the text, that refers to the Problem and not the Review Question.
- In this and other homeworks and possibly in the quizzes and final you may be asked the following type of question. You will be presented with some simple protocol or scheme and asked whether this is a good scheme. What you have to figure out here is not whether this is the best possible scheme or whether there is some subtle way in which a powerful cryptanalyst can attack the scheme with some brilliant technique, but rather whether there is a huge big gaping weakness in the scheme of not. If you think there is no huge weakness, you should say it is a good scheme, if you find a huge weakness you should say it is not a good scheme.
- You can assume that the Good Guys and the Bad Guy all know exactly the algorithms which are being used.
- Quiz 1 **in-person, closed book, closed notes** will be on 2/27/24 Tuesday and will cover those topics upto and including the DES modes of operation which we will have covered in Weeks 1,2,3,4.

1. (25 points)

   (a) The following is the ciphertext of a statement in English encrypted with Caeser cipher:
   SGHRHRZMDZRXOQNAKDL
   You have to figure out the key and the plaintext. You don't need to show any calculations, just the final result.

   (b) Using the monoalphabetic cipher, part of the ciphertext is the following:
   EDNA UBSAA NA MLCSE
   (I have left a blank space between the words to make the problem easier).
   The following are the approximate relative frequencies of the whole ciphertext:
   C:12,E:11,K:8,L:8,N:7,V:7,A:7,S:6,G:4,M:4,B:4,D:4
   Z:2,U:3,Y:2,I:1,J:1,P:1,O:1,R:1,F:1,H:1, X:1,T:0,W:0,Q:0
   You have to figure out what is the plaintext corresponding to the above ciphertext segment. You don't need to show any calculations, just the final result.

   (c) This question is about Hill cipher. The plaintext is "IT"
   The key K is $\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$.
   K^{-1} is $\begin{pmatrix} 3 & -2 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 24 \\ 25 & 1 \end{pmatrix}$.
      i. Show what the ciphertext C will be. You need to show your calculations.
      ii. Show the results (and calculations) of decrypting C. Remember that all operations are modulo 26.

2. (15 points) We studied three different modes of operations: ECB, CBC, OFB. One mode may be better than another according to a particular criterion. For the following, you don't have to give any explanations, just state which of the two modes is better according to that criterion:

   (a) Being able to transmit less than a full block of data. Which is better: OFB or ECB?
   (b) Being able to encrypt blocks in parallel: Which is better: CBC or ECB?
   (c) Preventing BG from fooling the recipient by switching two blocks. Which is better: CBC or ECB?
   (d) Recovering from a transmission error where a 0 got flipped to a 1. Which is better: CBC or ECB?
   (e) Preventing BG from building a code book of matching P, C pairs. Which is better: OFB or ECB?

3. (20 points)

   (a) Consider the following challenge-response protocol for A to convince B that he is indeed A. Here we are assuming that once a virtual circuit has been set up, the BG cannot alter messages in the middle. So the idea is that at the start when the virtual circuit is being set up, A has to convince B that he is indeed A. A and B share a secret value S. B sends A a nonce N. A takes the first 64 bits of N and treats this as a key K for DES, and returns $C = E_K(S)$ back to B. B checks whether $D_K(C) = S$ and if it is, accepts that A is indeed A (because he knows the secret S).

      i. Suppose this protocol was being used only once i.e. A has to convince B of who he is only one time. Once A has done this, this protocol is never going to be used again. Is this a good scheme?
         A. Give a YES/NO answer.
         B. If you said NO, explain your answer i.e. explain what you think is the *single biggest weakness* of the scheme.

      ii. Now suppose this protocol was being repeated many times i.e. A has to convince B of who he is repeatedly, and each time follows the above protocol. Each time the virtual circuit has to be re-established from scratch, and B generates a different nonce each time. Is this a good scheme?
         A. Give a YES/NO answer.
         B. If you said NO, explain your answer i.e. explain what you think is the *single biggest weakness* of the scheme.

   (b) Consider the following encryption scheme to provide confidentiality. A wants to send a message M to B. A calculates X, the ASCII representation of today's date. A then XORs M with X to get the ciphertext C. When B receives C, he XORs C with X to get M. You can assume that the number of bits in M is no more than the number of bits in X. Is this a good scheme?

      i. Give a YES/NO answer.
      ii. If you said NO, explain your answer i.e. explain what you think is the *single biggest weakness* of the scheme.

4. (40 points) Programming Problem: **Please read the programming guidelines** (in the course outline on Canvas) before starting to work on the programming problem. You need to read this carefully to understand what has to be turned in and how, including the self-critique.

   You have to implement encryption and decryption with Simplified DES, as discussed in the class and in Stallings 3rd edition. The permutations IP, P10, P8, and SW, and the functions f_k, F, and the S-box S0 are all as described, and can be hardwired into your program. For parts (a) and (b), you will use the original S1 box as described in Stallings 3rd edition. **However, for part (c), you have to use a modified S-box S1'.** In the modified S1', the rows 2 and 3 are the same as described for the original S1, but the rows 0 and 1 have been switched. So row 1 is $0, 1, 2, 3$ and row 0 is $2, 0, 1, 3$. Your program should:

   - take as input a 8-bit block of plaintext and a 10-bit key.
   - Show the following output (please only print what is being asked for, and nothing else):
     - the intermediate result after the SW operation while encypting.
     - the ciphertext.
     - the intermediate result after the SW operation while decrypting.
     - the result of the decryption process.
   - You have to run your programs on the following inputs:
     (a) with the original S1: the example from the textbook i.e. the plaintext is 10111101 and the key is 1010000010. In this case we know the ciphertext should come out to be 01110101, so this is a good way to check that your program is performing correctly on this input.
     (b) with the original S1: the plaintext is 01110111 and the key is 1101110111
     (c) with the modified S1': the plaintext is 10110101 and the key is 1000100100
   - Please note that you do not have to actually implement these operations as bit operations. For example, you can store the plaintext as an array of integers.
   - If you find it easier, you can hard-wire the S-boxes (S0,S1,S1') in your program.

Extra Credit Problems from Stallings (not from Review Questions, but from Problems:) Problem 3.5, Problem 3.20, Problem 4.14.

Extra Credit Programming Problem 1: Implement (program) an attack on the Hill cipher as discussed in class and the textbook. Your attack should work on a $2 * 2$ matrix. Show how your attack works on the example on page 84, and also run it on some other inputs.

Extra Credit Programming Problem 2: Implement (program) a brute-force attack on Simplified Des. Show how your attack works on an example.