Introduction to Cryptography - Fall 2015

Homework 4

Due by 11/15

Notes:

- This homework assignment is for individual students. Discussion is encouraged. But you have to form your own solution.
- Only typed or electronic reports (hand drawing okay for figures if necessary and legible) are allowed for homework submission.
- Write in a concise way. The essay solution should not exceed one page for each exercise.
- Submit it through the given link at BlackBoard as a **PDF** file. If there are other files such as Sage codes in a text file, compress all files into one zip file. Verify that the submission is successful.
- If you need more time for this assignment, you need to let me know before the due time.

1. (35pts) Sage programming on S-DES (Simplified-DES) with the help of the description and example Sage code in Stalling's textbook.

a) Consider EP, the expansion permutation, find an inverse contraction permutation that takes 8 bits down to 4 and inverts EP. Note that these compressions permutations are not unique. Implement this function EPinv.

b) Take the function f_K from the example Sage code and modify it so that instead of calling the SBoxes, it calls EPinv after the round key is XORed in. Rename the modified function f_K_NoSBox.

c) Modify the functions SDESEncrypt and SDESDecrypt as necessary so that they call f_K_NoSBox from part (b). Call the new functions SDESEncryptNoSBox and SDESDecryptNoSBox.

d) Do these new functions function as Encrypt/Decrypt functions of each other? That is, will SDESDecryptNoSBox give you back the input of SDESEncryptNoSBox, given that they are using the same key?

2. (15pts) Compare AES to DES. For each of the following elements of DES, indicate the comparable element in AES with justification or briefly explain why it is not needed in AES.

a) XOR of subkey material with the input to the *f* function

b) *S-box* function

c) XOR of the *f* function output with the left half of the block

d) swapping of halves of the block