**CS 4732/57322 Homework #3**

***Due electronically by midnight July 7th, 2025***.

For submission, if done on paper please scan and submit as a pdf. If done in word, please submit the .docx or .doc format.

**IMPORTANT**: Clearly indicate outside resources utilized and sign below. Failure to cite use of outside resources will be reported for appropriate disciplinary actions. Note that discussions with other students are encouraged; copying – with or without modifications – is unacceptable and will also be reported.

I discussed one or more problems with the following people:

I hereby certify that any outside resources utilized, other than the textbook and class materials, are clearly cited. All other material I provide for this homework submission is my own original work.

Jamie Harris

*Printed name*

1. (8 points) We talked about the Feistel cipher in class. Why did we at least for now restrict ourselves to discussion of the feistel cipher, rather than an arbitrary reversible substitution block cipher like in Table 4.1 of our notes?

The Feistel cipher significantly reduces the amount of possible mappings compared to an arbitrary block cipher while maintaining a more-than-adequate level of security, which allows keys to be much smaller, therefore using less data to be used when storing and/or transmitting keys.

2. a) [4 points] Describe to me the difference between diffusion and confusion in regards to the design goals of a cipher.

The goal of diffusion is to spread the responsibility of each bit across multiple bits when encoding. That is, when enciphering a message, each bit of that message will be responsible for modifying multiple bits in the encryption. The goal of confusion is to have the function used between the key and the message be complex, so it is hard to reverse engineer exactly how the key modified the message. This way, even if the key is found out, it will still take time to properly decipher the message.

b) [6 points] Given the DES cipher, explain the parts of the algorithm that give diffusion and the parts of the algorithm that do confusion. While I know there is some crossover here, give a rationale for what parts more heavily focus on diffusion or confusion or why some function might have both.

The S-box step performs a lot of diffusion, since the entire 6 bits of the initial value affect the entire 6 bits of the resulting value (the 2 outer bits affect the row of the table, the 4 inner bits affect the column of the table). The steps permuting the key and shrinking it to 48 bits, as well as expanding the 32-bit message block to 48-bits, add layers of confusion, because you can not be sure what part of the key/message those bits belong to.

3. (10 points) a) What is the avalanche effect? Using a DES calculator found online, show an example of this. Give me enough data in this answer so I can replicate your result, so give me any keys, data or results that you get. Of course also tell me the calculator you used, as well as any initialization vector set.

The avalanche effect asks that if a single input bit into an S-box is inverted, that every output bit of that S-box should independently have a 50% probability of also flipping, and should have no statistical relation to any other output bit.

Calculator: simewu.com/des/

Message: 1CA039EDA8D90000

Key: AFD3A0D3DF32E8C7

Output: 408830A9325ECF80

4. a) [10 points] Encrypt the hexadecimal string C5 with a feistel cipher. Your function F should simply convert the bitstring it is given to all 1s. Do this for two rounds.

C5 = 11000101

LE0 = 1100 RE0=0101

F(RE0)=1111

LE1=0101 RE1=0011

F(RE1)=1111

LE2=0011 RE2=1010

LE3=1010 RE3=0011

Final = 10100011

b) [5 points] How secure is this cipher? Do you notice any pattern in what is being produced given the input?

This cipher would not be very secure. Since our function merely returns a bitstring of all 1s, it makes finding a key completely irrelevant. At the end of the encryption process, the resulting bitstring is just the mirror of the initial string.