CS 4732/57322 Homework #3

Due electronically by midnight July 6th, 2020.

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.

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?

An arbitrary reversible substitution cipher (the ideal block cipher) for a large block size is not practical, however, from an implementation and performance point of view.
An example:
If a small block size, such as n = 4, is used, then the system is equivalent to a classical substitution cipher. For small n , such systems are vulnerable to a statistical analysis of the plaintext. For a large block size, the size of the key, which is on the order of n * 2 n , makes the system impractical.

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

Diffusion :- Diffusion is used to create cryptic plain texts and It is achieved through Transposition algorithm. It is used by Stream cipher and block cipher and it will result in increased redundancy. While in diffusion, if one image within the plain text is modified then many or all image within the cipher text also will be modified. The relation between the cipher text and the plain text is masked by diffusion.
Confusion :- Confusioni s a cryptographic technique which is used to create faint cipher texts and It is achieved through Substitution algorithm. It is used by block cipher only and it will result in increased vagueness. While in confusion, if one bit within the secret's modified then most or all bits within the cipher text also will be modified. The relation between the cipher text and the key is masked by confusion.

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.

<u>In DES cipher algorithm,</u>
Confusion is the S-box substitution
After mixing in the subkey in the algorithm, the block is divided into eight 6-bit pieces before processing by the S-boxes, or substitution boxes. Each of the eight S-boxes replaces its six input bits with four output bits according to a non-linear transformation, provided in the form of a lookup table. The S-boxes provide the core of the security of DES without them, the cipher would be linear, and trivially breakable.

The S-boxes of DES were much more resistant to the attack than if they had been chosen at random.

Diffusion is where the output of the S-boxes is rearranged according to the P-box permutation rules.
In this part of the algorithm, the 32 outputs from the S-boxes are rearranged according to a fixed permutation, the *P-box*. This is designed so that, after permutation, the bits from the output of each S-box in this round are spread across four different S-boxes in the next round.

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 is a behavior of a mathematical function used for encryption. It is the desirable property of a cryptographic algorithms, which is especially true for hash functions. A slight change in the key or plain text should result in a significant change in the cipher text. This is the avalanche affect.

Even if we add a small character it will be a huge difference. A good encryption should have above 50% OF ALVALCHE effect.

Consider SHA 256 algorithms (a very popular one) Enter a string that says "hello" and click generate hash. You should see the hash, now if you change the "h" to a capital H, it should result in a completely different hash. If you compare them there wont be any similarity between them even if we don't change the remaining characters.

The avalanche effect ensures that an attacker cannot easily predict a plain-text through statistical analysis.

www.convertstring.com/Hash/SHA256

4. a) [10 points] Encrypt the hexadecimal string A3 with a feistel cipher. Your function F should simply convert the bitstring it is given to all 1s. Do this for two rounds.

hexadecimal string = A3

In binary = 10100011

1. Divide the string into equal halves i.e L1 = 1010 and R1 = 0011
2. Let's generate two random keys K1 and K2.
Let K1 = 0110 and K2 = 0011

3. First encryption round :

f1 = R1 xor K1 = 0011 xor 0110 = 0101

Now the new L2 and R2 after round 1 are as follows:

R2 = f1 xor L1 = 0101 xor 1010 = 1111

L2 = R1 = 0011

4. Second encryption round :
f2 = R2 xor K2 = 1111 xor 0011 = 1100

Now the new L3 and R3 after round 2 are as follows:

R3 = f2 xor L2 = 1100 xor 0011 = 1111

L3 = R2 = 1111

Hence, cypher text is concatenation of R3 to L3

i.e **11111111**
Hence, encrypted bits = **11111111** (All 1's)

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

The round number of functions of fiestel cipher will be depending on the desired system of security. The no of rounds of the system will be depending on the security of efficient settlement. Analyzing the process is to look at all available input and dis-simble patterns. In short he security of this cipher is dependent on the number of rounds encrypted.