If possible please upload assignments to Canvas as .docx not .pdf to make editing easier. #6 is a good question.

**CS 4732/57322 Homework #2**

Due electronically by midnight 7/03/2018. There will be a one letter grade penalty for every day late, until 3 days after this date. No homework will be accepted after that time.

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.

<https://security.stackexchange.com/questions/45101/how-does-des-provide-confusion-and-diffusion>

<https://en.wikipedia.org/wiki/Data_Encryption_Standard>

<https://crypto.stackexchange.com/questions/9674/how-does-des-decryption-work-is-it-the-same-as-encryption-or-the-reverse>

<http://www.crypto-it.net/eng/attacks/meet-in-the-middle.html>

<https://www.tutorialspoint.com/cryptography/triple_des.htm>

<https://kodu.ut.ee/~lipmaa/papers/lrw00/ctr.pdf>

<https://crypto.stackexchange.com/questions/34890/question-about-cipher-block-chainingcbc>

<https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation>

Course Notes, Course Book

*Printed name*

THOMAS MARK MINTUN

1. (6 points) What problem does the autokey system of the vigenere cipher try to solve? Does it successfully solve the problem? If not, why not.

The problem the Vigenere autokey cipher tries to solve is **letter frequency analysis.** In particular the autokey system protects a regular Vigenere more because it provides a running key. A cryptanalyst can NOT do known frequency analysis, get the length ‘m’ of the keyword, and then do ‘m’ separate monoalphabetic ciphers repeating to get the plaintext. Surely this helped make Vigenere more secure for a very short while, but now NO the autokey system does not solve the problem of letter frequency analysis. Because the key and plaintext share same frequency distribution of letters, a statistical technique can be applied and exploited for successful cryptanalysis. The periodic nature of the keyword is eliminated though.

2. (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 discuss arbitrary mappings from one sized block to an equivalent sized block?

We discussed the Feister cipher rather than arbitrary mappings from one sized blick to an equivalent sized block… because an arbitrary reversible substitution cipher (the ideal block cipher) for large block size is not practical for implementation and performance. the mapping itself would constitute the key. There is an example in the book, but imagine lines being drawn from one set of numbers to another set of numbers and that is the key (one key out of all possible mappings (16! mappings for 16 bits)). This is vulnerable to cryptanalysis by an attacker that is aware of this algorithm because it is essentially a Hill cipher applied to binary data, and a simple linear system is quite vulnerable.

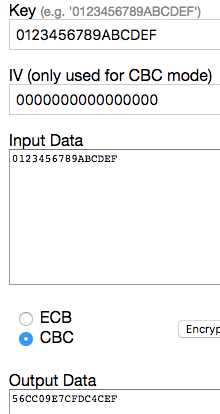
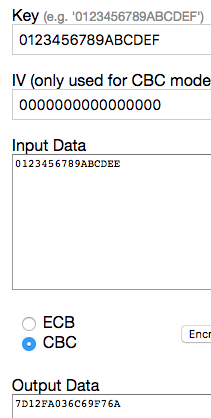
3. (8 points) Describe to me the difference between diffusion and confusion in regards to the design goals of a cipher. Then, given the DES cipher, explain the parts of the algorithm that give diffusion and the parts of the algorithm that do confusion. While I know there is some crossover here, give a rationale for what parts more heavily focus on diffusion or confusion.

The terms diffusion and confusion capture the basic building blocks for any cryptographic system. Diffusion is when the statistical structure (word/letter frequencies, series of numbers, etc) of the plaintext is camouflaged in long-range statistics of ciphertext. Each plaintext symbol affects one or more cipher symbols. The result is letter frequencies of the cipher are more close to equal than in the plaintext which is susceptible to letter frequency analysis. Contrastingly, confusion makes the relationship between the ciphertext and key as complex as possible to thwart discovery of the key; achieved by a complex substitution algorithm.

In DES confusion is implemented in the alternation of S-box substitutions, and diffusion is implemented by the permutation of bits from the P-box. The S-box is chosen at random and makes the relationship between key and cipher complicated. The permutation of bits from the P-box introduces irregularities in the next round camouflaging the data better.

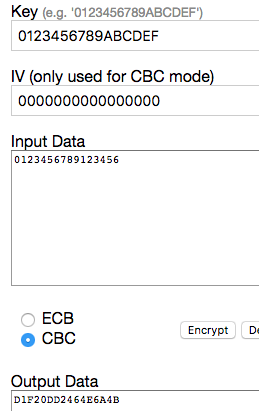
4. (10 points) What is the avalanche effect? Using a DES calculator found online, show an example of this. Give me enough data in this answer so I can replicate your result, so give me any keys, data or results that you get. Of course also tell me the calculator you used, as well as any IV set.

The avalanche effect is when a small change is made either in the plaintext or the key should produce a significant change in cipher text. Namely changing one bit of plaintext should change many bits in the ciphertext. As seen in screenshots, I changed the last letter (one letter, from F to E) of the plaintext message, and the entire encrypted message changed! I used: https://www.emvlab.org/descalc/?key=0123456789ABCDEF&iv=0000000000000000&input=0123456789ABCDEF&mode=cbc&action=Encrypt&output=7D12FA036C69F76A



5. (8 points) Make an argument for why DES decryption is the opposite of encryption. In a similar fashion to the last example, use a calculator online to show this result. Again, give me your data that you used to show this.

DES decryption is the opposite of encryption. In DES encryption and decryption are identical except for the order of the subkeys. Decryption works the same as encryption just with the ‘round key order’ reversed. In DES, after the last (encryption) step or before the first (decryption) step the left subkey and right subkey are NOT swapped making the process reversible; the key scheduling algorithm can also be reversed. The screenshot on the left is encryption, and the screenshot on the right is decrypting that enciphered message with the same key resulting in the original message. FUNCTION F IN FEISTEL OR DES CIPHER DOES NOT NEED TO BE REVERSIBLE. One half of ciphertext is passed through one way function, but there is always a copy of it remaining. One half goes through the function to mask the other half, but still becomes half of the ciphertext, which lets you use it again during decryption to undo the XOR operation used to mask the other half. The one way function is used to mask each half in an interleaved fashion, and can be done again in decryption as long as same key is used, hence decryption is the opposite of encryption.



6. (8 points) Explain what a meet-in-the-middle attack is in broad terms (as if I was a small child or a golden retriever).

A meet in the middle attack is a known plaintext attack meaning the attacker knows some plaintext and their ciphertexts. First the attacker creates a table with possible decryptions using Key2 of the ciphertext1. Next, the attacker creates a second column on the table containing all possible encryptions of plaintext1 and Key1. The attacker then matches or “meets in the middle” of the table columns for pair of secret keys that satisfy one Key1 encrypting plaintext matches Key2 decrypting ciphertext. And those are the keys!

Find the keys using domain (cipher) and range (plaintext) of the composition of several functions (block ciphers) such that the forward mapping of the first function is the same as backwards mapping through the last functions, literally meeting in the middle of the composed function. The result is significantly less possibilities of a key to brute force. Attacker needs a lot of computer storage, and the attack is passive.

7. (6 points) Why is the middle step of a 3DES decryption?

Decryption 3DES is 1) decrypt using Key3 2) encrypt using Key2 3) decrypt using Key1. So the middle step is to encrypt using Key2. This process if opposite of encrypting useing 3DES; the steps are 1) encrypt using Key1 2) decrypt using Key2 3) encrypt using Key3.

8. (6 points) Considering block cipher modes, what part of CTR encryption can be pre-processed?

Considering block cipher modes, the part of CTR are both the encryption and decryption. More specifically: one can compute the pad in “spare cycles,” even before one knows the plaintext. When plaintext is known , it is XORed with the already-computed pad. The latter can be done with throughput 10-25 Gbit/s on contemporary processor.

9. (6 points) What would be the effect of one bit getting corrupted in a CBC encryption. Justify your answer.

One bit being corrupted in a CBC encryption would only cause 2 blocks to become corrupted; its own block and the subsequent block. Assuming the message is at least 100 blocks long, the corruption of one bit would not have a catastrophic effect on the message. “One bit being corrupted in encryption…” means the one bit error is in plaintext. On the wikipedia page I found “Note that a one-bit change to the ciphertext causes complete corruption of the corresponding block of plaintext, and inverts the corresponding bit in the following block of plaintext, but the rest of the blocks remain intact.” I almost changed my answer, but the error that quote is referring to is a one bit change to the ciphertext, which would be the process of decryption.