**Hsiang Lo**

**CS 370 Introduction to Security Week 2: Problem Set 2**

Instructor Name: Rakesh Bobba

# **Introduction**

The purpose of this assignment is to help you gain a better understanding and insight into the cryptographic concepts and primitives we learned about in Week 2 and help you learn how they are applied.

Before beginning make sure you have watched the lecture videos on the following and completed the associated practice quizzes.

* What is Cryptography?
* What is Encryption?
* Classical Ciphers
* Modern Ciphers
* Encryption Modes

Also make sure you read th­­e following sections of Chapter 5 of the textbook: 5 – 5.2; 5.3.3; 5.4 – 5.4.1.2; 5.5 – 5.5.4;

# **Questions**

Please answer the questions below.

## What is Crypto?

Q1 [6 pts]: Name the four cryptographic tools discussed in the “What is Crypto” lecture video and list the security properties that each of those tools support?

The four cryptographic tools discussed are encryption/ciphers, cryptographic hashes, message authentication code and digital signatures. Encryption/Cipher supports confidentiality and privacy, cryptographic hashes supports integrity, Message Authentication Codes supports integrity and Digital Signaures support integrity, authenticity and non-repudiation

## What is Encryption?

Q2 [3 pts]: What is a cipher? What is it used for?

A cipher is a ciphertext that is an incomprehensible data that has been encrypted and transformed from plaintext or comprehensible data.

Q3 [4 pts]: What is the difference between a symmetric cipher and an asymmetric cipher? What is one advantage of a symmetric cipher over asymmetric and vice-versa?

The difference between a symmetric cipher and an asymmetric cipher is that the key used for encryption and decryption is the same and is traditionally more of a historical (classical) crypto. Asymmetry on the other hand, are keys used for enciphering (encryption) and deciphering but different. It is regarded as the more modern of the two encryption. Some benefits for symmetric key is that it is simple, fast, use less computer resources, and prevent widespread message security compromise.

Q4 [3 pts]: What is a brute force attack on a cipher? Explain it using “known plaintext” adversary and “ciphertext only” adversary.

A brute force on a cipher is an attack that systematically checks all keys (pass-phrases) with the hope of eventually finding the right key, also known as exhaustive search. The basics for the attack is based on mathematical attacks or statistical attacks. This can be explain using “known plaintext” adversary as these individual try to gues the plaintext by only looking at the ciphertext and checks it against multiple input in hope of finding parallels. “ciphertext only” adversary can also guess the key after looking at one or more (plaintext, ciphertext) pairs. The ideas behind these two attacks are based on correlation properties with the assumptions in order to crack the code.

Q5 [3 pts]: How may an adversary improve over a brute force attack?

An adversary may improve over a brute force attack by combing both known plaintext method and ciphertext only method, by checking both ends at the same time, they can find a matching pair faster. This can be done by checking all known pairs between the two. Also by using known methods to speed up the cracking process. Such as if the code was in English, they can first check for common letters such as the vowels and, within them, e, as it is the most common one.

## Classical Ciphers

Q6 [2 pts]: What is the difference between a substitution cipher and transposition cipher?

The main difference between a substitution cipher and transposition cipher is that a permutation cipher focuses on permuting the symbols or characters in the message whereas substitution cipher focuses on substituting the symbols or characters in the message from a different alphabet.

Q7 [4 pts]: What is a one-time pad? Why is the book cipher not as secure as one-time pad?

A one-time pad is a cipher with a random key at least as long as the message. It is recognized as the most secure way of encryption. A book cipher uses a common agreed book such as Bible or phone book, therefore it is not completely random and performance can be done to statistical analysis the result.

## Modern Ciphers

Q8 [3 pts]: What the difference between a stream cipher and a block cipher?

The major difference between a block cipher and a stream cipher Is that the block cipher encrypts and decrypts a block of the text at a time. On the other hand, stream cipher encrypts and decrypts the text by talking the one byte of the text at a time.

Q9 [2 pts]: What is the advantage of a stream cipher over a block cipher?

* 1. Block cipher technique involves encryption of one block of text at a time. Similarly decrypt the text by taking one block after another.
  2. In contest, stream cipher technique involves encryption and decryption of one byte of the text at a time.
  3. Block cipher uses both confusion and diffusion while stream ciphers relies only on confusion
  4. For block cipher, usually size can be 64 or 128 bits. 1 byte (8 bits) is converted in stream cipher at a time.
  5. Stream cipher uses XOR functions for converting the plaintext into cipher text, Block cipher does not use XOR bits.
  6. Block cipher uses the same key to encrypt each block while stream cipher uses a different key for each byte.

Q10 [2 pts]: What is the advantage of a block cipher over a stream cipher?

* 1. Because block cipher encrypt a whole block at a time, they are more susceptible to noise in transmission, that is if you mess up on one part of the data, all the rest is probably unrecoverable. Whereas with stream ciphers byte are individually encrypted with no connection to other chunk of data (in most ciphers/modes) and often have support for interruptions on the line. Block cyphers often have support for interruptions on the line, whereas stream ciphers do not provide integrity protection or authentication.

Q11 [2pts]: A good block cipher exhibits avalanche effect: if we flip one bit in the plain text, half of the bits are flipped in the cipher text. Two messages of the same length, m1 and m2, differ by 5 bits. With a good block cipher, how many bits differ in the two resulting cipher texts? Assume both cipher texts are n bits long.

Avalanche Effect is a key desirable property of an encryption algorithm. It states that when changing one input or key bit, it should results in changing of approximately half of the output bits.

Assume each bit change results in 50% change, it can be argued that the effect after the changing of the first bit is 50%. The result is then changed by 1 bit, which will induce another 50% change and so on. After 5 bits change, the bits difference between m1 and m2 will be 97% different. In another word, they will only share 3% of similarities.

Q12 [3pts]: If you are starting a new project that does not depend on other legacy programs, which cipher would you use, 3DES or AES? Justify your answer.

If I am starting a new project that won’t depend on other legacy programs, I would definitely choose AES. While 3DES is not practical to break, AES is much faster in comparison. AES is implemented and designed to withstand attack that were successful on DES. AES is also the new standard as well post 2001 and offer an open design that can gain the public’s trust more.

Q13 [4pts]: Why is DES no longer considered secure? Can we use Double DES (2DES) instead? Why or why not?

DES is no longer secure due to the fact that it only encrypts blocks of 64 bits using 56 bit keys. It was considered weak even back then. Diffie Hellman said in 1999 that in a few year’s technology can allow DES to be broken in days. We can’t use 2DES because it is susceptible to meet in the middle attack. Matching can be done for a given search in just O(log^2len(k) ) time.

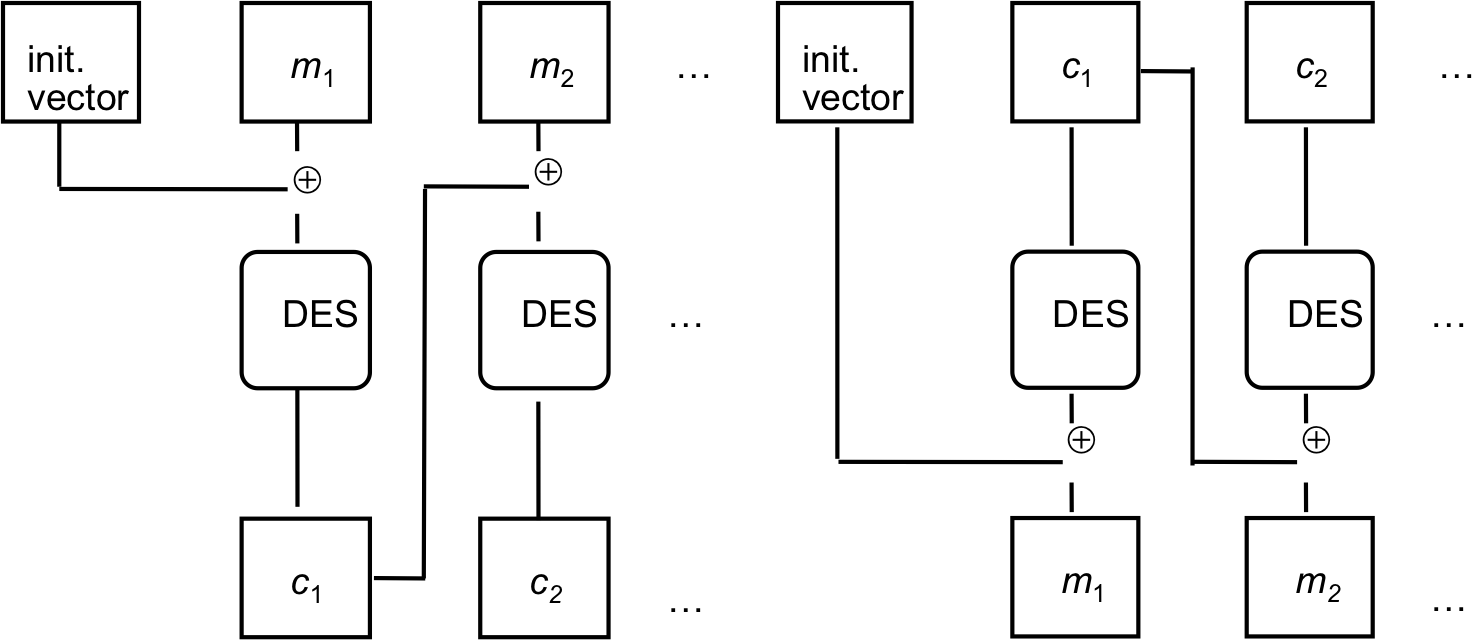
Q14 [4pts]: What is the bit strength of 3-DES when used in Encrypt-Encrypt-Encrypt mode? Explain Why. (Assume the keys are independent)

3-DES when used in Encrypt-Encrypt-Encrypt mode have a bit strength of 56 x 3 = 168 bits of bits strength since all three keys used are independe.t But only 112 bit security because of MTM attacks.

## Encryption Modes

Q15 [3pts]: What is an encryption mode or cipher mode? Name one disadvantage of using ECB mode.

An encryption/cipher mode is a way for block ciphers to encrypt messages larger than their block size. One disadvantage of using ECB is that for identical plaintext blocks, it produces identical ciphertext blocks. SO basically if there are 2 database records with only different character, it leaks the patterns of the information trying to secure.



Q16 [10pts]: The above picture represents encryption and decryption modes for a block cipher (here DES).

1. [4 pts] Complete the equations that describe the above encryption and decryption operations.

Receiver needs to know key and IV, once IV is known, c1 and c2 will be use for XORing. So the only information is sent is the IVs.

1. Take C0, Decrypt it
2. XOR it with IV and get M0 back
3. Take C1 Decrypt it
4. XOR that with Co to get M1 back
5. [2 pts] What is this mode called?

The mode in the picture shows the encryption and decryption mode of CBC or Cipher Block Chaining.

1. [4 pts] What properties should the initialization vector (IV) have? Can one fix the initialization vector ahead of time? Why or why not?

The initialization vector (IV) should be random, unpredictable and not secret. One cannot fix the initialization vector ahead of time due to the fact that this can lead to corruption of the data and let adversary alter result to decrypt.

Once the code has been encrypted, the IV can be released for public. For decrypting, IV is. needed

Q17 [3pts]: What are the advantages of Counter mode over OFB mode?

While both Counter Mode and Output FeedBack Mode can convert a block cypher into a stream cypher, Counter Mode lets you generate a bit in the middle of the stream, or point access, and lets you operate on blocks in parallel.

Q18 [3pts]: Is it feasible to convert a block cipher into a stream cipher? If yes, give an example.

It is possible however not feasible. It was discussed on Stack Exchange that you can build Two practictical and provable secure block ciphers called Bear and Lions. These blocks are built from stream cipher and uses a hash function, a keyed one for BEAR and an unkeyed one for Lion. So essentially the block ciphers built from a keyed hash function as follows.

https://crypto.stackexchange.com/questions/712/converting-a-stream-cipher-into-a-block-cipher?noredirect=1

# **Submission Details**

Submit a PDF file with the questions and your corresponding answers.

The assignment is worth 65 points. It is due Wednesday of Week 3 at Midnight.