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?

- Encryption/Ciphers: Support confidentiality and privacy
- Cryptographic Hashes: Support integrity
- Message Authentication Codes: support integrity
- Digital Signatures: support integrity, authenticity, non-repudiation

What is Encryption?

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

- A cipher is a cryptographic primitive that is used to preserve data confidentiality.

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?

- A symmetric cipher uses the same key to both encrypt and decrypt data, while an asymmetric cipher uses different keys for encryption and decryption.
- An advantage of using a symmetric cipher over an asymmetric one is ease of decryption.
- An advantage of using an asymmetric cipher over a symmetric one is better security.

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

- A “known plaintext” brute force attack is when an adversary has the ciphertext and the corresponding plaintext, and their goal is to find the key that encodes the plaintext to the ciphertext by guessing every possible way of encoding the plaintext to find out how the key encodes text.
- A “ciphertext only” brute force attack is when the adversary only has the ciphertext, and they guess every possible permutation of encoding to find a plaintext that makes sense. This could lead to discovery of the key as well.

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

- An improvement upon a brute force attack would be a statistical attack.

Classical Ciphers

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

- A transposition cipher permutes (rotates within the alphabet or language) the symbols in a plaintext, while a substitution cipher substitutes the symbols in the plaintext with other symbols to encode.

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 that is at least as long as the message it is being used to encode. The book cipher is not as secure as a one-time pad because book text is not random.

Modern Ciphers

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

- A block cipher uses the same encoding on every part of the plaintext message, while a stream cipher uses different encodings on every part of the message (until the cipher has to repeat due to reaching the end of its cycle).

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

- The advantage of a stream cipher over a block cipher is that the encoding of the message is different for each part of the message, while the same encoding is used on every part of the message with a block cipher. This makes stream ciphers harder to crack.

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

- The advantage of a block cipher over a stream cipher is that each block being encoded the same way makes it easier to decode, allowing easier communication.

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.

- n/2 bits difference.

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.

- A new project that does not need backwards compatibility would use AES. This is because 3DES is slower and allows backwards compatibility with DES, but since backwards compatibility is not needed, AES should be used.

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 because we currently have enough computing power to break it in a short time.
- 2DES is not recommended in place of DES, because of the amount of computing power we currently have, which renders 2DES as strong as DES due to MITM attacks.

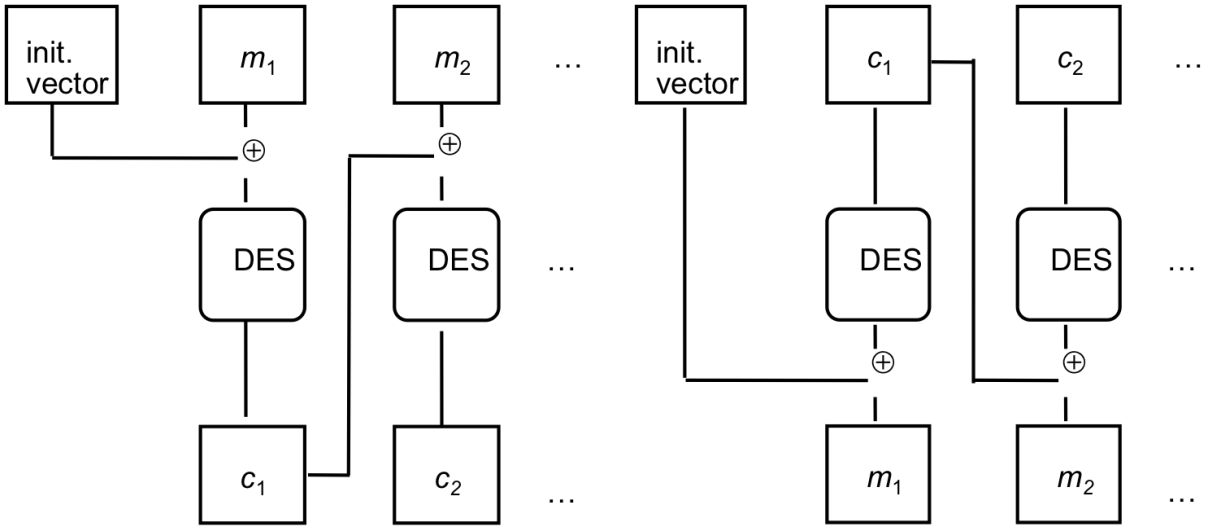
Q14 [4pts]: What is the bit strength of 3-DES when used in Encrypt-Encrypt-Encrypt mode? Explain Why. (Assume the keys are independent)

- Only 112-bit security because of backwards compatibility with DES, making it susceptible to Meet In The Middle attacks.

Encryption Modes

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

- An encryption mode is a way for block ciphers to encrypt messages larger than their block size.
- A disadvantage of using ECB mode is that it leaks patterns, allowing for easier decryption.



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

a) [4 pts] Complete the equations that describe the above encryption and decryption operations.
   - $C_i = E_k(M_i \oplus c_{i-1})$ for $i > 0$
     $C_0 = E_k(m_0 \oplus I)$

b) [2 pts] What is this mode called?
   - CBC mode

c) [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 should be random/pseudorandom, unique, and non-repeating.
   - One cannot fix the initialization vector ahead of time because of its random nature.

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

- Counter mode allows you to operate on blocks in parallel.
- OFB needs an initialization vector.

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

- Yes, a block cipher can essentially be converted into a stream cipher. This can be done with Output Feedback Mode, which successively encodes a key value using the previously encoded value.

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.