**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?

## What is Encryption?

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

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?

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

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

## Classical Ciphers

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

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

## Modern Ciphers

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

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

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

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.

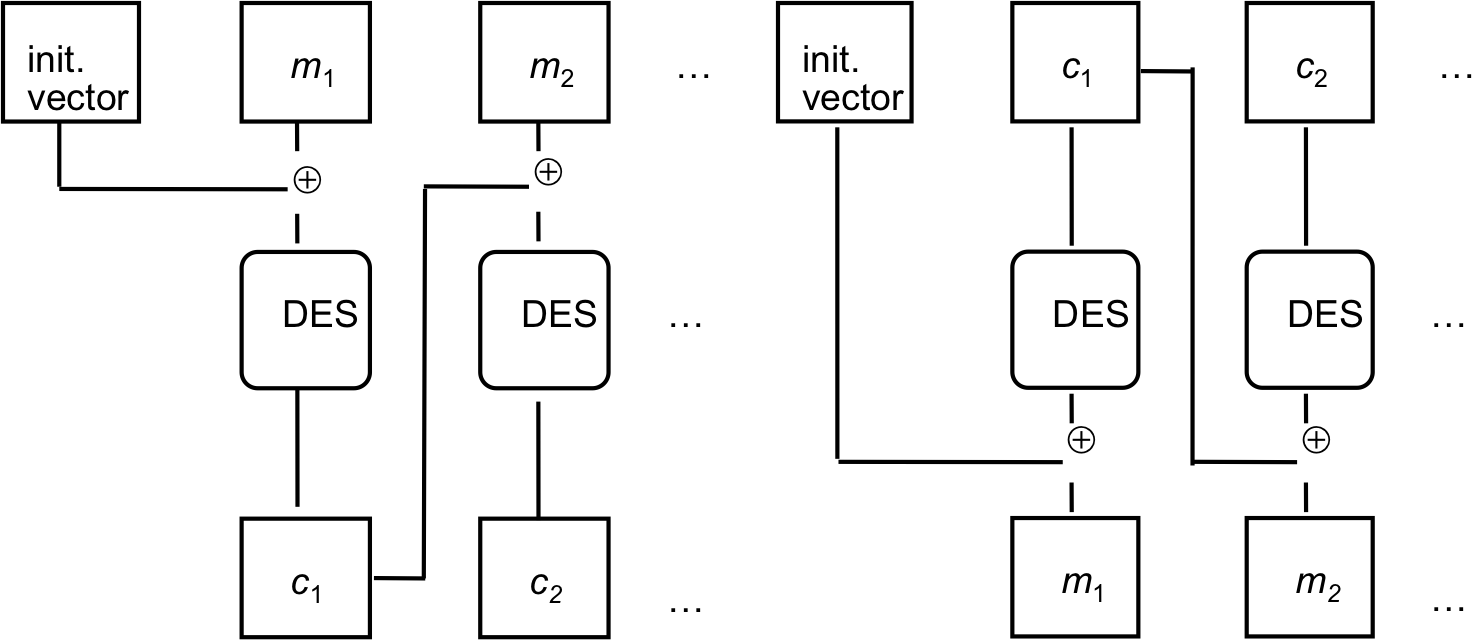
Q12 [3pts]: If you are starting a new project that does not depend on other legacy programs, which cipher would you use, 3DES or AES? Justify your answer.

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

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

## Encryption Modes

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



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.
2. [2 pts] What is this mode called?
3. [4 pts] What properties should the initialization vector (IV) have? Can one fix the initialization vector ahead of time? Why or why not?

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

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

# **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.