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: Confidentiality; Privacy
- Hashes: Integrity
- Digital Signatures: Authenticity, Integrity, Accountability
- MACs: Integrity

What is Encryption?

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

- A Cipher is a way of encoding a message or data in a way that will make it hard or impossible to decode by unauthorized parties.

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?

- Symmetric Ciphers have one key that can encrypt and decrypt the plaintext and ciphertext respectively.
- Asymmetric ciphers have one private key and one public key. The sk encrypts the message while the pk decrypts it.

- Symmetric ciphers have a long history, and their use is well understood. This lineage provides a benefit that people know more what they are doing with relation to the creation of these ciphers, and thus are more likely to get them right.
- Asymmetric ciphers have no need to distribute keys as the public key is safe to share.

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 with known plaintext (pt) and ciphertext (ct) involves trying all the methods of getting from pt to ct. If the method of encryption is a given, then it is tried over the entire keyspace to see what k is in E(pt, k) = ct.
- A Brute force with only ciphertext (knowing the encryption method) involves brute forcing the entire (key | pt) space to find key or pt respectively.

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

- If there are flaws in the implementation, then an adversary might be able to leverage those to their benefit. There are also certain attacks against specific ciphers such as MITM + nDES (n=2,3).

Classical Ciphers

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

- Substitution substitutes a symbol in the pt with a different one in ct.
- Transposition rearranges the order of the symbols in the message.

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

- A OTP is a an encryption technique where two parties share a one time key that has the same length as the message. A book cipher cannot always be a OTP because there exist books without all the words in a some messages, so there does not always exist a key… Plus there is the issue of key length requirement for an OTP.

Modern Ciphers

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

- Stream Ciphers break up the message and encrypt each piece with the same key, whereas a block cipher encrypts each block differently (i.e. different key, and or different index in the case of Counter Mode.)

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

- Depending on the Block Mode, a stream cipher can distinguish itself by its ability to send any chunk of a message rather than necessitating the maintenance of a sequence. Therefore, multiple threads could be run at once.

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

- Block ciphers can obfuscate encrypted data chunks, such as when encrypting two identical chunks, most Block cipher Modes create different outputs for the same input chunk (because the factor in previous blocks, or the index of the block …).a

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.

- For every bit flipped in the input, on average 50% of the ciphertext bits will flip. With a good block cipher, nearly all if not all the bits will be different, when you consider that each result bit has a super high probability of being flipped.

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.

- AES, because the closed source design and the fact that this was developed by a government agency concerns me some. Well, the closed design decisions of DES worries me more than the government design, but either way, 3DES is also MITMable, which can reduce the keyspace.

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

- DES is not secure because the keyspace is easily crackable (2^56) with modern computing. 2DES can have its keyspace lowered to DES's amount (~2^56+1) because of MITM attacks.

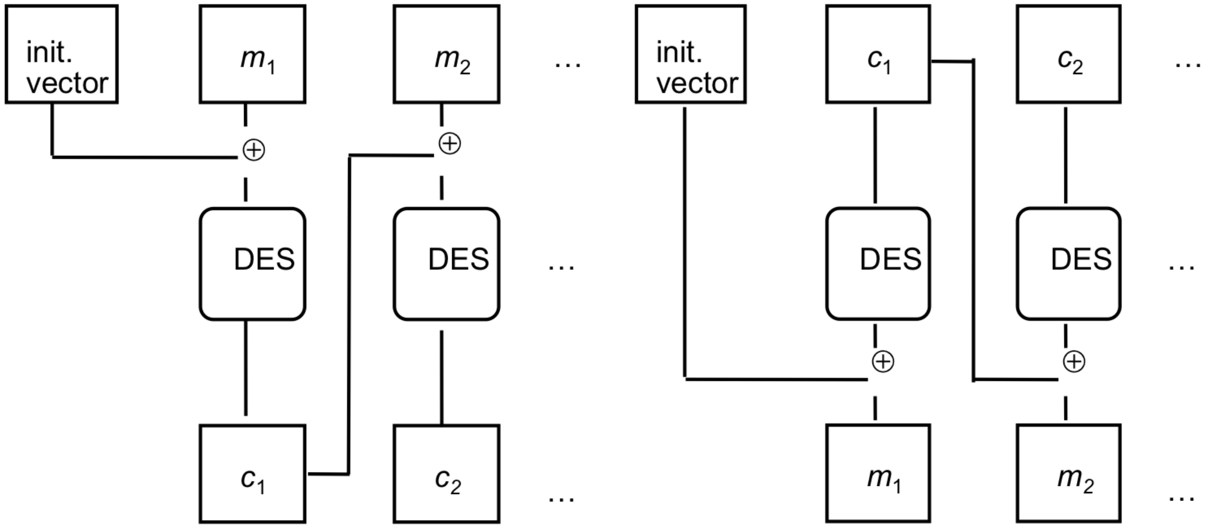
Q14 [4pts]: What is the bit strength of 3-DES when used in Encrypt-Encrypt-Encrypt mode? Explain Why. (Assume the keys are independent)

- Because of MTM, the keyspace is 2^112 (168 – 56 because of MTM)

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 of encrypting data using block ciphers. ECB has the advantage of simplicity, as well as parallelizeability, as the messages do not rely on the previous or following messages.



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.
   - a. Encryption:
     - i. $c_n = E((m_n \text{ xor } c_{n-1}), k)$
     - ii. $c_1 = E(m_1 \text{ xor } I), k)$
   - b. Decryption:
     - i. $m_n = E(c_n, k) \text{ xor } c_{n-1}$
     - ii. $m_1 = E(c_1, k) \text{ xor } I$

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

c) [4 pts] What properties should the initialization vector (IV) have? Can one fix the initialization vector ahead of time? Why or why not?
   - a. It needs to be random. I guess it can be fixed ahead of time, but that runs the high risk of It making the encryption mode vulnerable, so I would think it best to make the IV at runtime.

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

- Counter mode does not rely on the last message. Therefore it can be parallelized, or any chunk can be sent/repeated in case it gets dropped on a network or something.

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

- If you are asking about once the cipher has been composed, then no, it is not feisable, as you would need to decrypt them first to turn them into a stream.
- To convert an algorithm is completely feisable (i.e. turn Counter Mode from m_i xor E(i, k) to a simple E(k, m_i)).

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.