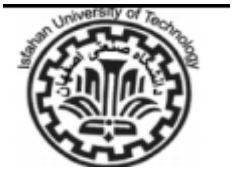

Understanding Cryptography

Homework No.4 **Due Date: 99.02.10**

Chapter 5

1.

1.1. Compare five modes of operation designed to be used with modern Block Ciphers.

Operation Mode	Description	Type of Result	Data Unit Size
ECB			
CBC			
CFB			
OFB			
CTR			

1.2. What are the advantages and disadvantages of Mode ECB?

2. In a company, all files which are sent on the network are automatically encrypted by using AES-128 in CBC mode. A fixed key is used, and the IV is changed once per day. The network encryption is file-based, so that the IV is used at the beginning of every file. You managed to spy out the fixed AES-128 key, but do not know the recent IV. Today, you were able to eavesdrop two different files, one with unidentified content and one which is known to be an automatically generated temporary file and only contains the value 0xFF. Briefly describe how it is possible to obtain the unknown initialization vector and how you are able to determine the content of the unknown file

3. Besides simple bit errors, the deletion or insertion of a bit yields even more severe effects since the synchronization of blocks is disrupted. In most cases, the decryption of subsequent blocks will be incorrect. A special case is the CFB mode with a feedback width of 1 bit. Show that the synchronization is automatically re-stored after K + 1 steps, where K is the block size of the block cipher.

4.

- Programming

  Complete the file "operationModes.ipynb" related to the implementations of operational modes including ECB, CBC, OFB, CFB, and CTR. In this file, we use AES as our block cipher. For the sake of your convenience, the input string and outputs of functions are processed to make them suitable and compatible for use with the block cipher. This way, all you have to do is to complete the parts in which you're asked to write your codes. However, feel free to change any parts you deem inconsistent with your needs. At the same time, note that the purpose of this exercise is to have you understand and implement the algorithms yourself. Therefore, using built-in implementations of encryption modes does not merit any score. (To open the file you might need to use ipython or jupyter notebooks)

Chapter 6

Euler's Phi Function

5. If p is a prime and a is a positive integer, prove

$$\emptyset\,(p^a) = p^a - p^{a-1}$$

Wilson theorem

6. If p is a prime, prove that

$$\binom{p-1}{k} \equiv (-1)^k \,(mod\ p).$$

Number Theory

7. Prove that any positive integer of the form $6k + 5$ must have a prime factor of the same form.

8. Prove for n a natural number, If $n \geq 2$ then $n^3 - n$ is always divisible by 3.

- Deliverables:

  Put the answer to each of the questions in your answer sheet. For the programming assignment, save your desired changes to the "operationModes.ipynb" file, and put this file along with the "AES.py" file in your answer folder.