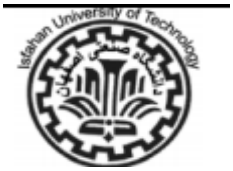

Understanding Cryptography

Homework No.3 **Due Date: 01.01.25**

1.Answer the following questions:
a. What are the advantages and disadvantages of Mode ECB?
b. what is a prime number?
c. what is Euler s totient function?

2. 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			

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)

5. Show that why $\emptyset(n)$ is even for all n>2.

6. If p is a prime, prove that

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

7.1. Using Fermat' s theorem, find 3^{201} mod 11.
7.2. Prove theorem 6.3.2.

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

9. Show that if a,b, n are integers with n| $ab$and gcd(a,n)=1, then n |b.