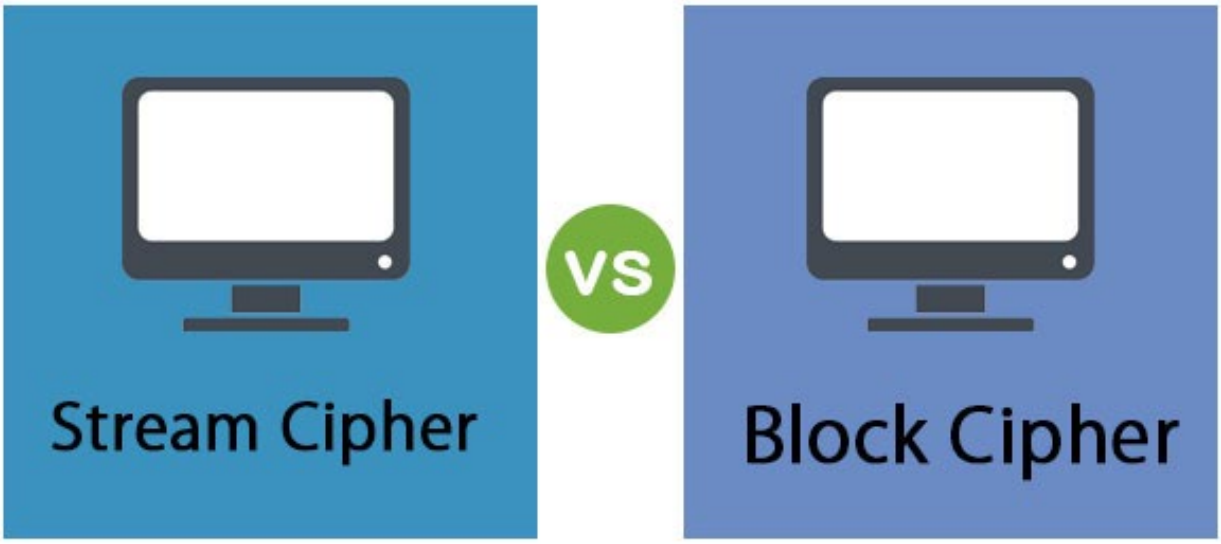
HACETTEPE UNIVERSITY DEPARTMENT OF

COMPUTER ENGINEERING

BBM 456 HOMEWORK 3

Mehmet Taha USTA – 21527472

# Subject: Describe Block Ciphers vs. Stream Ciphers Comparing




The important difference between a block cipher and a stream cipher is that the block cipher encrypts and decrypts a block of the text at a time. On the other hand, stream cipher encrypts and decrypts the text by taking the one byte of the text at a time.

## Block Cipher:

1. Processing or encoding of plain text is done as a fixed length block one by one.A block for example could be 64 or 128 bits in size.

2. The same key is used to encrypt each of the blocks.

3. A pad added to short length blocks.

4. Uses Symmetric Encryption and is NOT used in asymmetric encryption.

5. Confusion factor:The key to the cipher text relationship could be really very complicated.

6. Diffusion factor:output depends on the input in a very complex method.

7. Most block ciphers are based Feistel cipher in structure

8. Looks more line an extremely large substitution and using the idea of product cipher 9. More secure in most cases

10. Usually more complex and slower in operation

11. Examples of Block cipher are:Lucifer/DES,IDEA,RC5,BLOWFISH etc.

## Stream Cipher:

1. Processing or encoding of plain text is done bit by bit.The block size here is simply one bit.
2. A different key is used to encrypt each of the bits.
3. Bits are processed one by one in as in a chain.
4. High speed and low hardware complexity.
5. Key is often combined with an initialization vector.
6. Long period with no repetition.
7. Statistically random.
8. Depends on large key and Large Lineer complexity
9. Equality secure if properly designed
10. Usually very simple and much faster
11. Examples of Stream Cipher are: FISH,RC4,ISAAC,SEALİSNOW, etc