Cryptography
Lecture five

Stream Cipher(1)

Assis prof. Dr. Saja Jasem Mohammed

Stream cipher

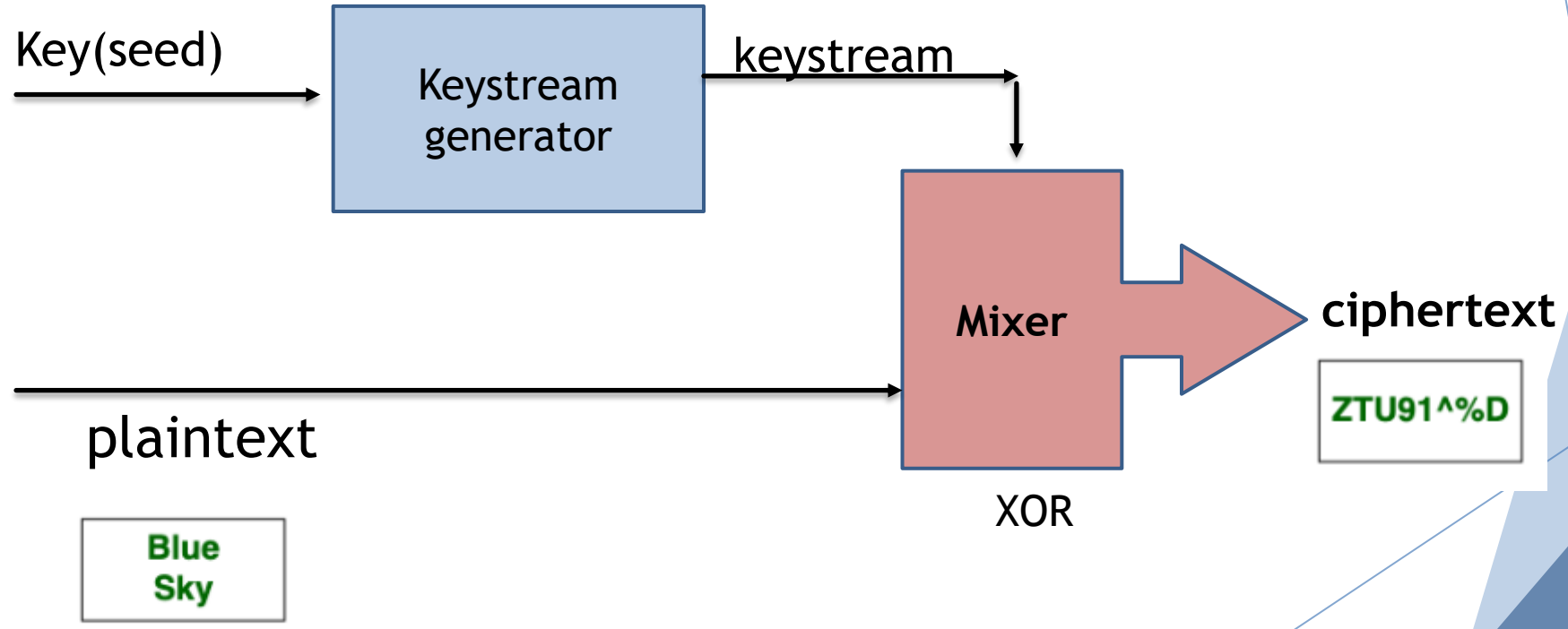
- **Stream ciphers** are a type of the modern encryption algorithm that process an individual **bit, byte, or character of plaintext at a time**.

- Stream ciphers are often **faster than block ciphers** in hardware and **require circuitry that is less complex.**

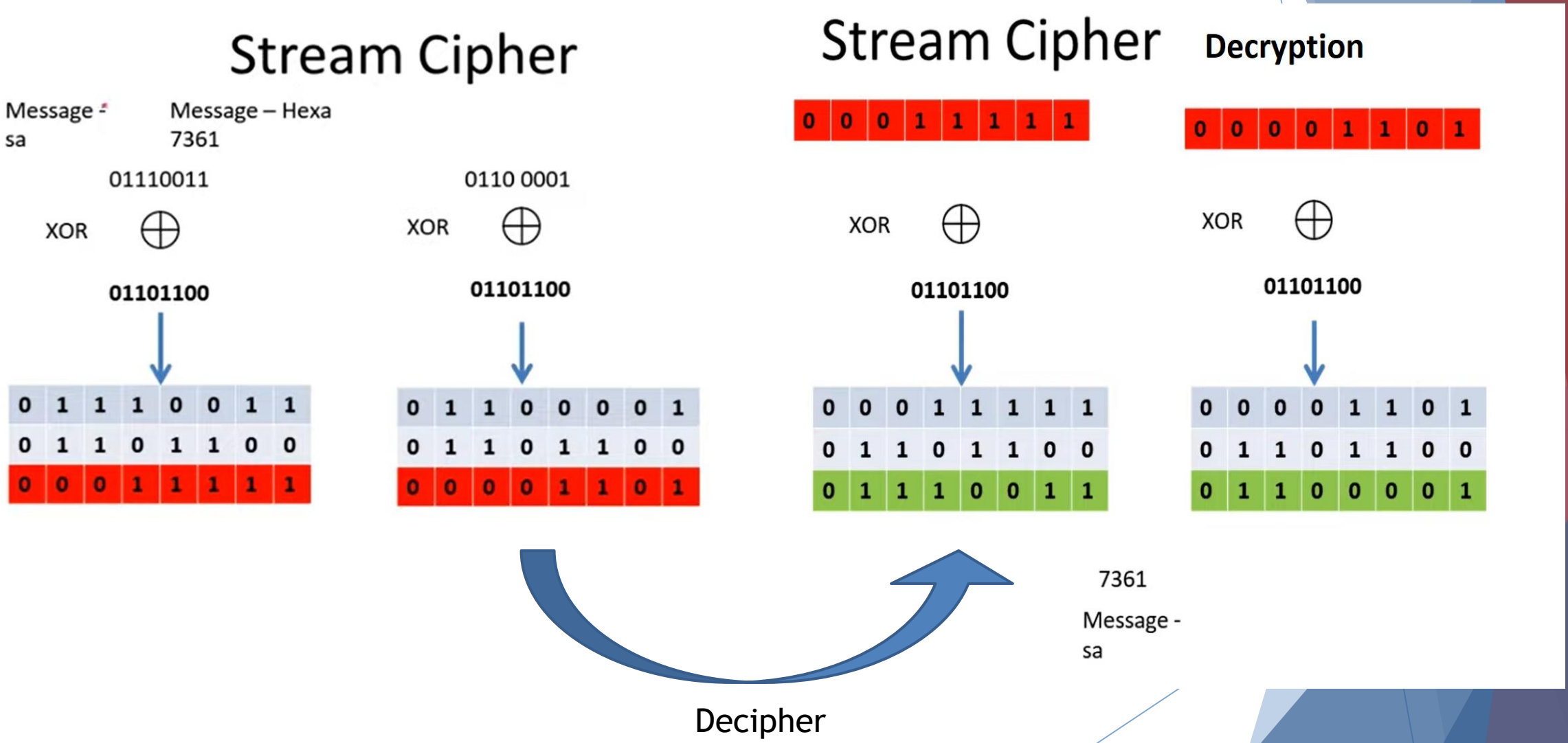
- Stream ciphers are often better for use in situations where we have data of an unknown size or the data is in a continuous stream, such as we might see moving over a network.

Stream cipher components:

- Plaintext
- Keystream generator
- Mixer



Example


Stream Cipher
Message -
sa
Message – Hexa
7361
01110011
XOR
01101100
0 1 1 1 0 0 1 1
0 1 1 0 1 1 0 0
0 0 0 1 1 1 1 1
0110 0001
XOR
01101100
0 1 1 0 0 0 0 1
0 1 1 0 1 1 0 0
0 0 0 0 1 1 0 1
Stream Cipher
0 0 0 1 1 1 1 1
XOR
01101100
0 0 0 1 1 1 1 1
0 1 1 0 1 1 0 0
0 1 1 1 0 0 1 1
Decryption
0 0 0 0 1 1 0 1
XOR
01101100
0 0 0 0 1 1 0 1
0 1 1 0 1 1 0 0
0 1 1 0 0 0 0 1
7361
Message -
sa
Decipher

Benefits of Stream ciphers

- **Speed.** This form of encryption is typically faster than others, including block ciphers.
- **Low complexity.** It's easy to incorporate stream ciphers into modern programs, and developers don't need complex hardware to make it happen.
- **Serial nature.** Some companies deal with messages written in a trickle. With their bit-by-bit processing, stream ciphers allow them to send information when it's ready rather than waiting for everything to be done.
- **Ease of use.** Stream ciphers are symmetrical encryption tools, so companies aren't forced to bother with public and private keys. And mathematical concepts that underlie modern stream ciphers allow computers to determine the proper decryption key to use.
- **Little** or **no error propagation.** It is useful when transmission errors are likely to occur.

FOUR CONDITIONS

The resulting ciphertext will be **impossible to break** if the following four conditions are met:

- 1. The key must be random.
- 2. The key must be at least as long as the plaintext.
- 3. The key must never be reused.
- 4.The key must be kept completely secret by the communicating parties.

- If these condition are met in the key, then the key is called **(one time pad key).**

A pseudorandom number generator (PRNG)

- A **pseudorandom number generator** (**PRNG**) is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers.
- There are two type of random numbers : truly random and pseudorandom
- The PRNG-generated sequence is not truly random, because it is completely determined by an initial value, called the **PRNG's *seed***.
- Seed value must be kept as **secret value**.
-
- **Two criteria can be used to validate that a sequence of numbers is random**:
  - Uniform distribution: the frequency of occurrence of ones and zeros should be approximately equal.
  - Independence: No one subsequence in the sequence can be inferred from the others.