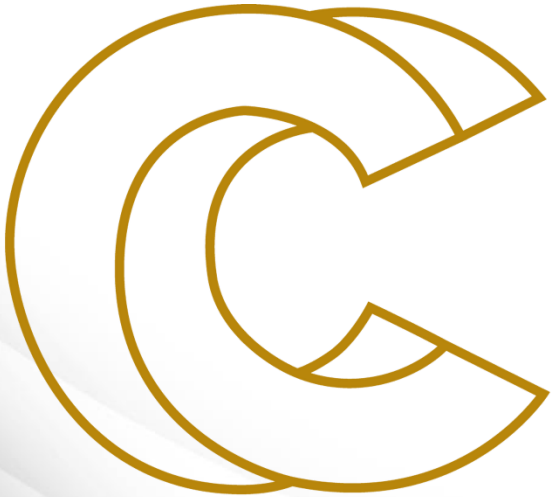


EURO 4SEE

GPU Assisted Brute Force Cryptanalysis of GPRS, GSM, RFID, and TETRA

Cihangir Tezcan, PhD
Graduate School of Informatics, METU, Ankara

ncc@ulakbim.gov.tr

Lesson 2: Introduction to Stream Ciphers

The Unbreakable Cipher

- Generate a very long sequence of ***random*** bits (one-time pad)
- **Encryption:** XOR the plaintext and the one-time pad to get the ciphertext
- **Decryption:** XOR the ciphertext and the one-time pad to get the plaintext

Plaintext	0101011110010 01……
One-time pad	1011110101101 01……
Ciphertext	1110101011111 00……

Lesson 2: Introduction to Stream Ciphers

The Unbreakable Cipher

- Perfect secrecy: Ciphertext provides no information about plaintext.
- Instead of working with bits, one can work on letters or characters.
- Usually printed on a single page with very small letters (hence the name one-time pad).
- **Problems:**
  - Key is too long
  - Key distribution
  - Randomness
- ***Stream ciphers*** try to achieve the one-time pad like security by generating *pseudo-random keystream* from a short key

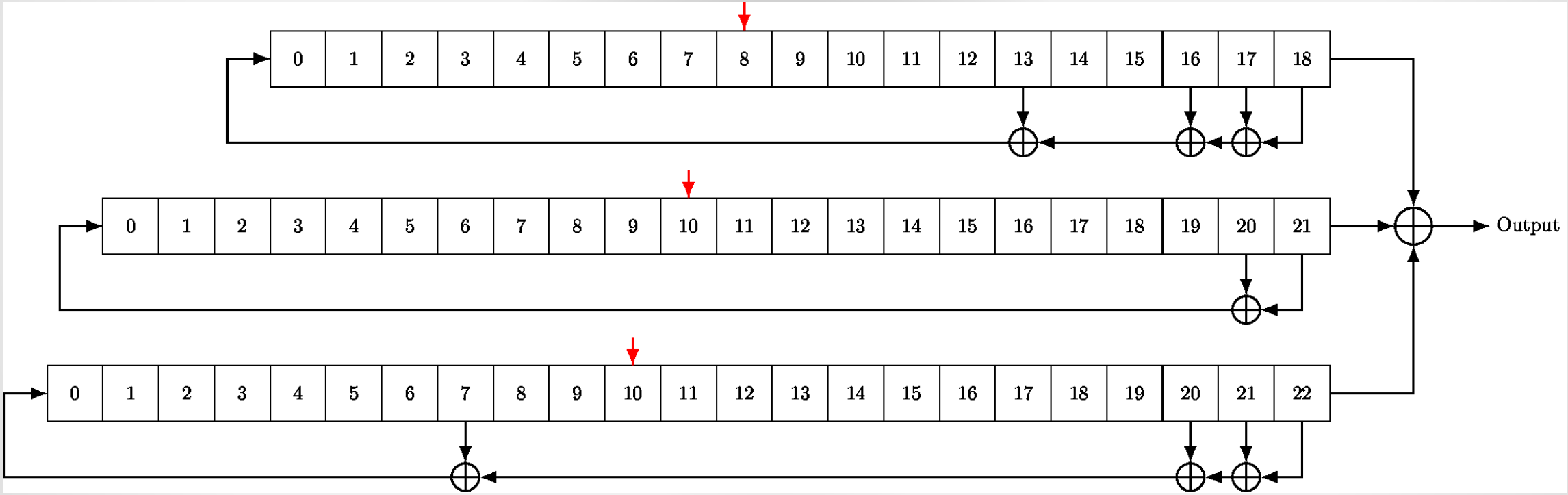
Lesson 2: Introduction to Stream Ciphers

Symmetric Key Cryptography

- Symmetric key cryptosystems are classified as ***block ciphers*** and ***stream ciphers***:
  - ***Block Ciphers*** operate on large blocks of plaintext data with a fixed transformation
  - ***Stream Ciphers*** operate on individual plaintext digits with a time varying transformation
- Contrary to a block cipher, a stream cipher has a (sort of) memory (the internal state) as it processes the plaintext.

Lesson 2: Introduction to Stream Ciphers

Example: A5/1 Stream Cipher (2G Standard)



Next lecture

KASUMI Block Cipher

- KASUMI block cipher is a 3G encryption standard
- Its modified version A5/3 is used in 2G communications

EURO 4SEE

Thanks!

Co-funded by
the European Union

EuroHPC
Joint Undertaking

This project has received funding from the European High-Performance Computing Joint Undertaking (JU) under grant agreement No 101191697. The JU receives support from the Digital Europe Programme and Germany, Türkiye, Republic of North Macedonia, Montenegro, Serbia, Bosnia and Herzegovina.