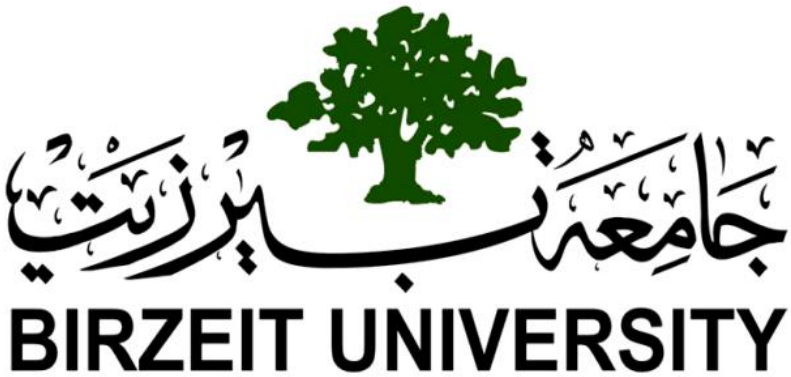

Faculty of Engineering and Technology

Department of Electrical and Computer Engineering

APPLIED CRYPTOGRAPHY

ENCS4320

Task # 1 (Cryptanalysis of the A5/1 Stream Cipher)

Prepared by:

Hala Sabobeh **Number:** 1220322.

Lara Abu Asfour **Number:** 1221484.

Tasneem Shelleh **Number:** 1220439.

Instructor: Dr. Ahmaed Shawahna.

Section: 1

Date: 31/07/2025.

❖ Method Summary

The core idea is to brute-force all possible 22-bit values for **LFSR Y** (a total of 2^{22} = 4,194,304 possibilities), generate the keystream using the known initial states of X and Z, and compare it against the XOR of the ciphertext and known plaintext to find a match.

Steps:

1. The known plaintext is converted to binary bits using (str_to_bits).
2. The ciphertext is read as binary and parsed into a list of bits.
3. A brute-force loop tests each possible Y state:
    - Converts the candidate Y to a 22-bit binary string.
    - Generates the first 24 bits of the keystream using the A5/1 algorithm.
    - XORs the partial keystream with the first 24 bits of the ciphertext.
    - If it matches the corresponding known plaintext bits, the correct Y is found.
4. The full keystream is regenerated using the correct Y.
5. The complete ciphertext is decrypted, and the plaintext is written to recovered_plaintext.txt.

❖ Optimizations

Partial keystream match: We initially used a full bit comparison method to check each candidate Y state, which took around **30 minutes** to find the correct result. Later, we used a **partial keystream match**, comparing only the first 24 bits of the known plaintext and ciphertext. This change reduced the brute-force time drastically down to just **3 minutes**, making the process significantly faster and much more efficient.

Progress tracking: We also used the `tqdm` library to display a live progress bar during brute force. This helped us track how many states were tested and how much time remained, improving the debugging and monitoring experience.

➢ The recovered initial state of LFSR Y.

11001010111001011100 10

➢ The fully recovered plaintext message.

There are many ways to die in Gaza, although one does not have the luxury to choose.

You may be killed in a bombing, or be struck by a sniper's bullet as you try to collect food to stave off hunger, or starvation itself may claim your life. The Health Ministry says 116 people have died because of malnutrition, many of them babies and children.

In Gaza, the simplest, most basic necessity can also be lethal. Water is one of them. Every aspect of it can be dangerous: providing it, seeking it, drinking it, swimming in it.

Since the start of the genocide, the Israeli army has relentlessly targeted Gaza's water infrastructure. More than 85 percent of Gaza's water and sanitation structures are inoperable - including pipelines, wells, and treatment facilities.

Israel has blocked the entry of water-related materials to the Strip, making repairs difficult. It has also targeted the warehouse of the water utility authority, destroying equipment and spare parts.

Worst of all, workers trying to make repairs or operate water infrastructure have been directly targeted and killed. Working in the water sector has now become a deadly job.

Most recently, on July 21, the Israeli occupation forces attacked a desalination plant in the Remal neighbourhood of Gaza City, killing five people at the site. This was one of the few functioning water stations in the city.