جامعة بيرزيت

BIRZEIT UNIVERSITY

Faculty of Engineering & Technology

Electrical & Computer Engineering Department

ENCS4320, Applied Cryptography

Prepared by:

Mohammed Saada	1221972
Layal Hajji	1220871
Raseel Jafar	1220724

Instructor : Dr.Ahmed Shawahneh

Date: 30th July, 2025

This report outlines a successful cryptanalytic attack on the A5/1 stream cipher, a keystream generator used in GSM mobile communications. By leveraging a known-plaintext attack and partial knowledge of the cipher's internal state, we recovered the unknown initial state of one of the three Linear Feedback Shift Registers (LFSRs) and subsequently decrypted the full intercepted ciphertext. Our approach focused on efficiently narrowing the search space and simulating the A5/1 algorithm to identify the correct internal configuration.

Cryptanalytic Approach

Our cryptanalysis was based on a **known-plaintext attack** combined with **brute-force search** over the unknown initial state of one LFSR. The key insights and steps in our strategy were as follows:

1. **Partial State Knowledge**:
   We were provided with the initial states of two of the three LFSRs: **LFSR X** (19 bits), **LFSR Z** (23 bits), Only **LFSR Y** (22 bits) remained unknown, limiting our search space to $2^{22} \approx 4.2$ million possibilities — a tractable size for exhaustive search.
2. **Keystream Extraction**:
   Given the known plaintext and the corresponding ciphertext, we recovered the first segment of the keystream using bitwise XOR:

   $$\textbf{S[i] = Plaintext[i]} \oplus \textbf{Ciphertext[i]}$$

   This reconstructed keystream allowed us to compare output from simulated LFSRs with the expected output.

3. **A5/1 Cipher Simulation**
   For each candidate initial state of LFSR Y, we simulated the A5/1 keystream generation mechanism:

- **Majority Clocking:** Determined from bits X[8], Y[10], and Z[10].
- **Conditional Stepping:** Each LFSR is clocked only if its control bit matches the majority.
- **Keystream Bit Generation:** Each bit is computed as **KSi = X[18] ⊕ Y[21] ⊕ Z[22]**.

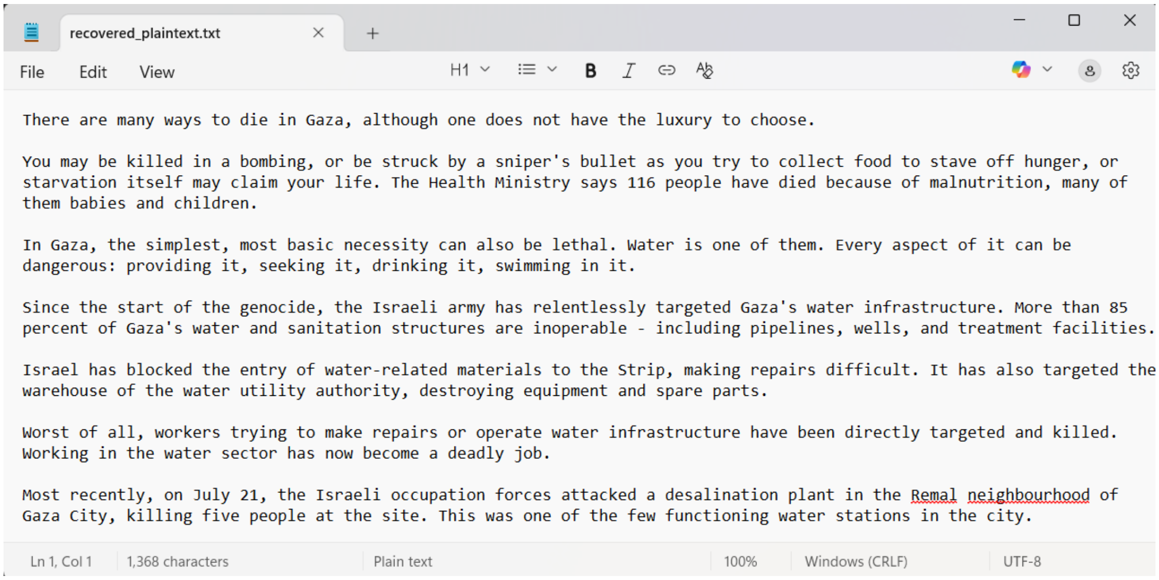
$$\textbf{KSi = X[18]} \oplus \textbf{Y[21]} \oplus \textbf{Z[22]}$$

4. **Search Optimization**

To improve the efficiency of our brute-force search over the 22-bit initial state space of LFSR Y, we applied an early-stopping mechanism during keystream validation. Rather than simulating the full keystream for each candidate Y state, we compared the generated keystream bit-by-bit with the reconstructed known keystream. The simulation starts from the first bit, and as long as the generated bit matches the corresponding known bit, the simulation proceeds. However, the moment a mismatch occurs, we immediately discard the candidate Y state and terminate its simulation. This bit-by-bit verification significantly reduces the computational overhead, as invalid Y states are often rejected early without the need to generate and compare the entire keystream. This optimization proved effective in pruning the search space and accelerating the overall cryptanalytic process.

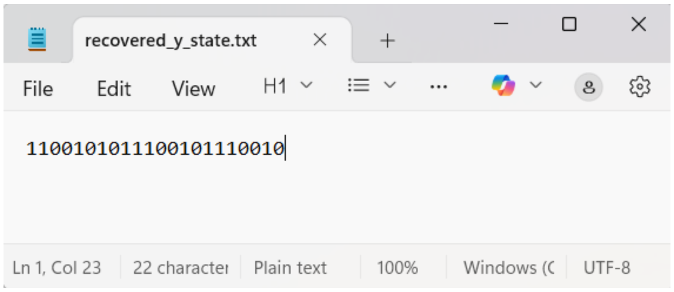
5. **Candidate Validation**:
   The simulation output was compared with the extracted keystream. If the first *n* keystream bits matched, the candidate was accepted as the correct initial state of LFSR Y.

Once the correct Y state was identified, we used the reconstructed A5/1 generator to produce the full keystream and decrypt the entire ciphertext.



```
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.
```

figure 1: recovered_plaintext.txt



```
1100101011100101110010
```

figure 2: recovered_y_state.txt