Birzeit University
Faculty of Engineering and Technology
Department of Electrical and Computer Engineering
ENCS4320 - Applied Cryptography (Term 1243)
Task # 1 *(Cryptanalysis of the A5/1 Stream Cipher)* – Due Friday, August 01, 2025

Alice and Bob are communicating over a GSM network, which secures voice and data transmissions using the **A5/1 stream cipher**. To ensure privacy, Alice's phone encrypts her message with A5/1 before sending it over the wireless channel.

Unfortunately for Alice, an attacker — *you!* — is within close proximity. As a result, you were able to **eavesdrop on the beginning of Alice's message**, which is provided to you in the file ***known_plaintext.txt*** (in ASCII). Additionally, you intercepted the **entire encrypted message** (ciphertext), which is available in ***ciphertext.bin*** (in binary).

To assist in your cryptanalysis, you are also given the **initial states of two of the three linear feedback shift registers (LFSRs)** used in the A5/1 cipher — specifically, LFSR **X** and LFSR **Z**. These initial states are provided in the file ***initial_states.txt*** as binary strings. However, the **initial state of LFSR Y (22 bits)** remains unknown.

Write a program in your preferred language (Python is recommended) that performs a cryptanalytic attack to recover the full plaintext message. Your program must:

A) Prompt the user to enter the full paths to the following input files:
   - ***initial_states.txt***: Contains the binary initial states of LFSRs **X** and **Z**.
   - ***known_plaintext.txt***: The known portion of the plaintext message in ASCII.
   - ***ciphertext.bin***: The full encrypted message in binary.

B) Your program should then:
   - **Recover the 22-bit initial state of LFSR Y** using the known plaintext and the corresponding ciphertext. Write the recovered LFSR **Y** state to ***recovered_y_state.txt***.
   - **Decrypt the entire ciphertext** using the generated keystream to obtain the full original plaintext message. Write the full recovered plaintext (in ASCII) to ***recovered_plaintext.txt***.
   - Use progress indicators (e.g., tqdm) to track tested states and remaining candidates.

You are required to submit:

1) Your source code, clearly documented and well-structured.
2) A brief report (maximum 2 pages) that includes:
   - A clear explanation of your cryptanalytic approach and any assumptions or optimizations used.
   - The recovered initial state of LFSR **Y**.
   - The fully recovered plaintext message.

GOOD LUCK