CS-7863: Telecommunications Networks

Project 2:
Making and Breaking GSM A5/1 Encryption Ciphers

Overview

GSM is an open-standard that was originally developed by the European Telecommunications Standards Institute (ETSI). This specification defines security requirements for authentication of subscribers and for optional encryption of voice traffic. The name of the encryption cipher chosen by the ETSI for GSM was A5/1. Unfortunately, this cipher was developed behind closed doors and the details of how this cipher works were not originally released to the public. However, security researchers successfully reverse engineered the A5/1 cipher in the 1990s and released the details of the encryption algorithm to the public [1].

1. Briceno, Marc. "A pedagogical implementation of A5/1." http://www. scard. org.

Assignment (Making)

Write your own implementation of the GSM A5/1 cipher using a programming language of your choice (e.g., Python, Java, C). For this assignment I'm looking for a simple proof-of-concept demonstration that shows your ability to manually write an encryption and decryption routine for plain-text messages. Your solution should print out the 64-bit symmetric ciphering key, original message, encrypted message, and decrypted message.

In addition to the lecture material and reading assignments, there are plenty of resources available online to serve as inspiration. Please feel free to use these as you see fit. However, please do not abuse this and copy someone else's code that may be available online. Use this as an opportunity to build your coding skills and gain an appreciation for how LFSR-based stream ciphers work.

Extra Credit Challenge (Breaking)

Decrypt the following message that was encrypted with a 64-bit symmetric key (Kc). What was the value of key (Kc) and the resulting plaint-text message?

Encrypted Message = 0x54686973206973206d7920736563726574206d65737361676521

Hint: Brute force is an acceptable approach. Could this be sped up on a multi-core computing platform (e.g, GPU or FPGA)?

Requirements

The criteria for completion will be a report that at a minimum contains the following information:

- Short write-up of your methodology
- Screen shots of your output and/or test cases
- Please include all original source code in your submission

Grading

This assignment is due by 11:59PM CST on April 1st, 2025. Please submit your report (PDF) and source code to the instructor via email. I'm NOT requiring the paper to be in any particular format. Grading will be gauged based on completion of the requirements above and level of effort.