Homework 3 (Program)

■ A5/1

A5/1 is a stream cipher used to provide over-the-air communication privacy in the GSM cellular telephone standard. It is one of seven algorithms which were specified for GSM use.

■ Aims

- ✓ You have to implement an A5/1 algorithm to generate a key stream to decrypt an encrypted audio file.
- ✓ The algorithm of A5/1 is based on the following video link:
  http://www.youtube.com/watch?v=LgZAI3DdUA
  [Attention]: The 6 steps of A5/1 in the link are all correct, but the value of one of registers is wrong. So you don't panic if your program's output is totally different from the video.
- ✓ If the encrypted file is larger than 228 bits, you don't need to add the frame counter and re-initialize the three registers again. Instead, you have to just continue generating the key stream until reaching the size of encrypted file. That is, you just have to initialize the three registers once.
  (This part is already included in main.cpp, so you don't worry about this.)

■ Coding Environment

- ✓ **Language:** C/C++
- ✓ **OS:** Linux (You can implement on different OS, but we will check your program on CSCC workstation,linux1.cs.nctu.edu.tw machine. Please make sure your program can perform well on it.)

■ Specification

- ✓ Two files – **hw3.cpp** and **main.cpp** – are published on e3 platform.
- ✓ **hw3.cpp** – you have to implement two functions and rename the file to **<studentID>.cpp (ex: 0123456.cpp)** and upload the file on time.
  - ◆ Read the comments in this file carefully to ensure your implementation of these functions use their arguments correctly.
- ✓ **main.cpp –** you don't have to upload this file.
  - ◆ Modify main.cpp to include <studentID>.cpp to run your A5/1 program.

■ Sample Input & Output

Sample input file and output file, and the test method will be announced in e3 later.

■ Hand in & Deadline

Upload your source code on **e3** before 23:59:59 on **December 29th.**
No late submission.

■ Grading Policies

Pass sample tests – 60%
Pass another tests – 40%
No copying from others (or the Internet), or you will fail in this course.