EE 453/717: Advanced Computing for Electrical Engineers

Indian Institute of Technology Bombay
Autumn 2010

Assignment 2 : **3 points** **Due date**: August 17, 2010

The A5/1 stream cipher is used to encrypt GSM signals. It consists of three irregularly clocked linear feedback shift registers (LFSRs) whose outputs are combined using three-input one-output XOR function. More details can be found at `http://en.wikipedia.org/wiki/A5/1`. A C implementation of A5/1 can be found at `http://www.scard.org/gsm/a51.html`.

The goal of this assignment is to write a C++ program which will generate keystream bits for A5/1 using **arrays**. Understandably, this will be inefficient compared to the C implementation which uses `unsigned long` to store the state of the LFSR. But the point is to get you to work with arrays. Your implementation should have the following features.

1. A C++ class to represent a LFSR
2. The clocking bit and feedback polynomial of each LFSR should be modifiable.
3. The code which uses the LFSR class should not change if you decide to use the C++ STL class `bitset` `http://www.cplusplus.com/reference/stl/bitset/` instead of arrays, i.e. the internal data representation should be private and accessible only through public interfaces.

The C implementation has a test case which can be used to test your implementation.