Systems Programming

Assignment 1

Write a program that implements the A5 stream cipher algorithm(C source code given in the book **Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C,** writer: Bruce Schneier) in Intel 80X86 assembly language. **A5** is a stream cipher used to provide over-the-air voice privacy in the GSM cellular telephone standard. C codes of the algorithm can be obtained from photocopy room.

The project will consist of two source files. In one file, the C main function as given in the book will be written. In the other file all assembly routines you implement will be given.

The a5_key, a5_encrypt, a5_decrypt and all other necessary routines must be implemented using the Netwide Assembler.

Together with your source code, submit a report that covers the following:

- short survey about A5 algorithm.
- description of your program as specified in the Software Reports Guide.

Submission deadline: 22 November 2005

- Assignments will be submitted via the Homework Submission System.

Note: Your survey should be written entirely in your own words and all references you use must be appropriately mentioned within the body of the text. You are NOT allowed to do any direct copy-and-paste from any source.