Freddy Arévalo fredar@ufm.edu Oscar Acuña oacuna@ufm.edu

# WORKSHEET #3

LEXICAL ANALYSIS

This Worksheet requires submitting documents via email, and there is no presentation but group discussion will be done on submission date. Work is to be submitted in groups of no more than 4 students.

## EXPECTED RESULT

This worksheet is about Cryptography, and requires basic knowledge of functions and Finite State Machines.

The expected documents to be presented for grading are:

1) Text document in PDF format, with the **accurate and complete** mathematical definition of
    a. Encryption FSM
    b. Decryption FSM
    c. Encryption function
    d. Decryption function
    e. An step by step explanation of a working sample … encryption and decryption.
2) Excel document (and/or source code) demonstrating how your encryption/decryption works on a alphanumeric string of at least 6 positions. On submission date, you will show your working encryption/decryption machine.

## PREPARATION LECTURE

Cryptography is the science of using mathematics to encrypt and decrypt information. Encryption is the process of masking information to make it unreadable without a key approach. Secrecy is to be maintained for confidential communications. Decryption is the process of extracting the original information from the encrypted data.

In this Worksheet secrecy is maintained by using finite state machine, with a function to perform encryption using Gödel, Fibonacci or similar counting method. You may use Recurrence Relations, which are recursive definitions of mathematical functions or sequences.

Therefore, the following lectures are required for successful execution:

1. Schaum's Book Chapter 3
2. Schaum's Book Chapter 13
3. "A Survey on Password Authentication Using Godel Number" by Chakravarthy, Balaji and Pavani (ISSN: 2248-9622) http://www.ijera.com/papers/Vol2_issue3/CL23534538.pdf

4. "Cryptographic Scheme for Digital Signals using Finite State Machines" by Gandhi, Sekhar and Srilakshmi. International Journal of Computer Applications (0975 – 8887). http://shodhganga.inflibnet.ac.in/bitstream/10603/11436/14/pxc3874904.pdf

Individual Preparation Test will be about Functions exercises (Section Solved Problems in Chapter 3), and Group Preparation Test will be about the Finite State Machines Exercises (Section Solved Problems in Chapter 13).

## GRADING

| GRADING CRITERIA | GRADE |
|---|---|
| Preparation Test (Individual and Group) | 4pts |
| A **complete** FSM is defined for encryption, and one for decryption. | 3pts |
| A Gödel, Fibonacci or any other professor approved counting **function** is **completely** defined for encryption within the Encrypting FSM, and one decryption function is **completely** defined within the Decrypting FSM. Both functions are correctly calculated within the Excel (and/or source code). | 5pts |

EXTRA 3pts will be given to the group with the most complex encryption function.

## KEY DATES

- Preparation Test (Individual and group), based on Preparation Lecture, will be done on Oct 5th.
- Groups must be formed by Sep 22nd 5pm, and members e-mailed to Oscar and Freddy. Otherwise, Professor will assign groups.
- Documents need to be submitted via email to Freddy and Oscar, no later than Oct 12th 1pm. Work discussion and demonstration of working functions will be done during class that day.

Start your work as soon as possible, and bring your questions/challenges to discuss with the whole class. Don't leave this until the last day.