WSU Software Project

Develop an interactive UI / Tutorial for

Advanced Encryption System (AES) / Rijndael Encryption & Decryption

# Requirements / Features:

* Build a GUI for a python-based AES encryption/decryption system (starting from python encryption/decryption algorithm base code – slowAES.py) . This system should allow encryption and decryption for short strings, text files, and data files: from the command line, as well as from the GUI.
* Build a demonstration/Tutorial engine for the AES GUI. This should allow cryptography students to execute step-by-step the encryption & decryption processes, to include the ability to pause, play, and perform step-by-step advancement at the round and sub round level (Byte Substitution; Shift Row; Mix Column; Add Round Key)
  + A nice feature would be to have the ability to click on a character in the plaintext and see what characters it has affected in the (partial) ciphertext as each round proceeds. That way, a student can see how each component of the round (and each round itself) adds entropy to the ciphertext.
* Build an interactive modifier capability that lets cryptography students explore what would happen if certain changes were made to the various components of AES (such as the S-box or the encryption key). The modifier should be interactive/real time/GUI-based. Include as a baseline:
  + Ability to change mode of operation, for example: output feedback mode, cipher feedback mode, cipher block chaining (OFB, CFB, CBC)
  + Ability to change/reorder the values in the S-box
  + Ability to change/reduce the number of rounds in the encryption process (default is 10 rounds)
  + Ability to remove various phases within the rounds (example: substitution and/or mix column)

**Creativity is encouraged here**: especially if you find other things that might make the algorithm less secure or subject to attack

* Add visualizations to help students understand how the encryption/decryption system is working under the hood.
  + Include both the changes happening to the message and the internal variables.
  + Include a visualization of the value of entropy (Relative entropy?) to show how the entropy is changing from the original message to the encrypted version as each round in the encryption occurs. Hint: If two input (plaintext) messages are the same except for 1 character somewhere in the message, how many of the output (ciphertext) bytes get changed? Can you compute & display the relative entropy value that shows how much of the message gets changed by changing 1 character of plaintext?

# Constraints

Your team must work in Python using code provided by Dr. Borghetti (any request for changes to code or language must be approved by Dr. Borghetti)

All source & files must be provided

Instructions must be provided to allow Dr. Borghetti’s students to set your team’s system up on their machine without ‘installing’ anything. If additional items are required for installation (for example – to get graphics), then these will need to be explained and provided.

For educational purposes, we don’t care about the speed of execution of the encryption/decryption – what matters is visibility – thus, minimize and only use libraries or compiled code for the encryption/decryption where absolutely necessary.

# References / Source Code

The windows version of “portable python” that will be used in Dr. Borghetti’s class is included in the set of files. See the readme file for setup details on how to make a portable executable which doesn’t require “installation” on the target machine. This will allow you to set up a coding environment even if you don’t have admin privileges on the target machine. Look at the README file in the directory called “portable python installation”

New to Python? A great reference for learning python is: “Think Python (how to think like a computer scientist) <http://www.greenteapress.com/thinkpython/>

SlowAES.py is the source code for the AES algorithm provided in the set of files. It is located in the directory “slowAES python implementation”

Here is the location of the web page describing the SlowAES implementation of AES in python <https://code.google.com/p/slowaes/>

New to cryptography or AES? Here is some more info on AES :

* Wiki: <http://en.wikipedia.org/wiki/Advanced_Encryption_Standard>
* Online Encryption/decryption demo: <http://aesencryption.net/>
* Gory Details of the AES encryption standard: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
* Still looking for more? For fun: <http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html>