IUPUI

Final Project
Python Encryption Tool

Project Manager:

Alex Waclawik, Student of B.S. Computer Science

alwaclaw@iu.edu

Proposal:

My final project will be a basic encryption tool. I will be designing my own encryption method to be used. While it may not be as secure as current industry standards, the purpose of the project will be to demonstrate my understanding of encryption techniques and methods.

The encryption method will be a style of OTP (one-time pad), using an MD5 hash. The user will be able to input a message, consisting of letters and numbers, to be encrypted. An MD5 hash will be taken of the message and along with the user input, converted to binary. The user input will then be compared to the hash via XOR operation, then the hash is appended to the input. The size of the message will be 1024 “bits”, so the remaining message will be randomly generated to bring it up to length. This part will use the random library pseudorandom number generator, as it is only for filler and not encryption. I will also use the hash library, and the string library. Decryption will work the same way, just backwards. An MD5 hash of the decrypted message will be taken and compared to the original hash, determining if the message had been tampered with. All inputs and outputs will be on command line.

Data:

There will be several types of data used in the program. They are as follows:

1. The user input for message to be encrypted/decrypted. Will be stored as a string to make it the proper case, then it will become a list.
2. Most of the variables will all be lists. This is due to them being iterable.
3. Dictionaries will be used for converting to and from binary.

Libraries:

Hashlib Library

Random Library

String Module