Anthony Constantino

HW #8

Safe Encryption

When dealing with cryptography there are many things to be aware of then just than just encrypting text. There are several issues and methodologies that even cryptographers disagree on. There is one issue that can dramatically increase the safety of safe encryption. One of the biggest debates for cryptographers is whether you encrypt the message first and then generate the portion which identifies the sender, or if those two steps should be done in reverse order.

The majority believe that it is better to encrypt the message being sent first then to authenticate it. The reason for doing this is so that on the other end the systems can see that through the authentication the message came from the correct source without even touching the encryption. I personally agree with this consensus because of the dangers that result from forcing the receiving end to do any decryption before verifying the source. If there is any decryption during or before the authentication it can leave several doors open for your security to be hacked.

To explain this, let us analyze the hypothetical situation of the doing those steps in reverse. Let's say the system generates the authentication while it encrypts or generates it before and encrypts the whole thing. The other end would then need to receive the message, decrypt the whole message, and then verify the source because only after the decryption does it have access to that part of the message. This would mean that the computer wouldn't have access to the portion of the message that would trigger the red flag until after all of this had taken place. Let's say that someone hijacked the message and then started testing it against the system, modifying tiny pieces of the message bit by bit. They

would then be able to analyze the error messages and output to figure out where the message ends and authentication begins.

This is the type of situation that must be avoided. If they can figure this out about the message they can slowly start working towards cracking the key that was used to encrypt the message, and leave all sorts of windows open for them to come through and maliciously attack your system or impersonate the messages being sent using your key. In conclusion, to safely encrypt the messages you are going to send to outside sources, it is best practice to encrypt the message then generate the authentication. This will allow for more secure communication for both parties.