Project 1

Public-key encrypted message and it’s authentic digital digest

Timothy Trusov and Eric Armstrong

What does the program do though?

Sender (X) : E_{Ky+} (E_{Kxy} (H(M)) || M)

Receiver (Y):

1. D_{Ky-} (E_{Ky+} (E_{Kxy} (H(M)) || M))
2. D_{Kxy}(E_{Kxy} (H(M)) and reconstruct M
3. Compare received H(M) with calculated H(M)

Key Generator

This program starts by generating a pair of keys.

The keys are stored in their respective files and the modulus and exponent values are determined.

The symmetric key is also created here and saved to its own file.

The parameters of the modulus and exponent values are then used to create the public and private key for later encryption and decryption.

Sender

- Class retrieves symmetric key and generates final value.
- Asks for file input and generates hash from the file, before continuing it asks to swap the first bit of the hash.
- Hash is encrypted in AES Encryption and written into a file and string variable.
- Key parameters are read from a file and used to generate public Key

Receiver

- RSA Padding and decryption methods are invoked to begin final processing.
- Key Parameters are read from file and used to generate private key
- Then the symmetric key is also generated along with a prompt to input user file for decryption
- The cypher file is retrieved and user file is processed through RSA Decryption
- Compares decrypted hash with calculated one to check authenticity