# PROJECT 1

OPTION: 2

GREG DEWS

JEFFERY WALTO

## KEY GEN

- Created a sender public and private key
- Created a receiver public and private key
- Created a symmetric key based off of user input

- Saved all keys to files for use in sender and receiver programs

## SENDER

- Create and initilize the RSA and AES ciphers
- Read in the sender private key and symmetric key
- Prompted the user for a document that would be encrypted
- Hashed the file
- RSA the hashed message
- Append message to hash and encrypt with AES
- Save the message

## RECEIVER

- Create and initialize the RSA and AES ciphers
- Ask the user for the file to decrypt
- Decrypt the file using AES
- Separate the message from hash
- RSA the digital signature
- Hash the message and compare to previous hash value

## QUESTIONS?