Applied Cryptography Project

Authors:

Derek Hopkins
Jacob Nevin
Ethan Conner

Required Python Packages:

Pycryptodome
Tinyec

Statement:

This program was written as a term project for the class COSC 3341(Applied Cryptography). Its goal is to provide a secure communication channel between two people and utilize multiple cryptographic principles and techniques to ensure the confidentiality and integrity of data communications.

Techniques:

- Elliptic Curve Diffie-Hellman is used for session key distribution
- AES-256 in CBC Mode is used for confidentiality
- SHA-256 is used for data integrity

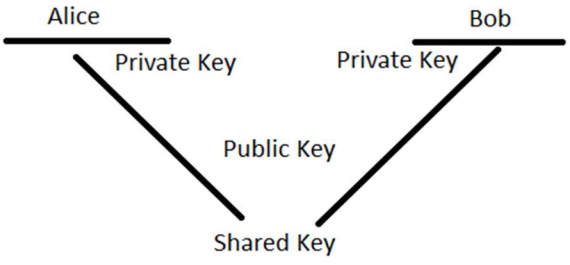
Applied Cryptography Project

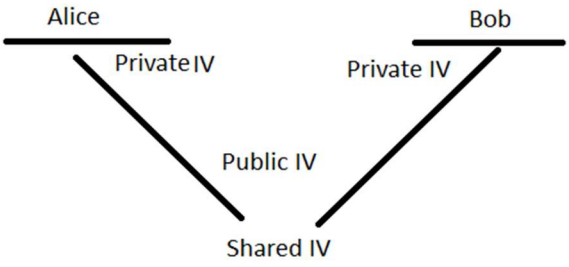
Explanation:

- pTextMsg takes in the plain text message the user wants transmitted
- A session key is generated by use of the ecdhKeyExchange function
- An initial vector is created by initialVectorExchange which will make the initial value harder to intercept
- pTextMsg is passed to hashedPlaintext to has the plain text
- pTextMsg and the session key are passed to the encrypt function to give the encryption dictionary
- The encrypted dictionary is encoded in base64 and stored in cipherText
- The encrypted dictionary and session key are passed to the decrypt function and the result is stored in decryptedCipherText
- decryptedCipherText is fed to the hashMsg function and the unhashed message is stored in hashedDecryption

Key Management/Decryption Visualization:

Key management:





Applied Cryptography Project

Decryption: