COSC 3364 – Principles of Cybersecurity

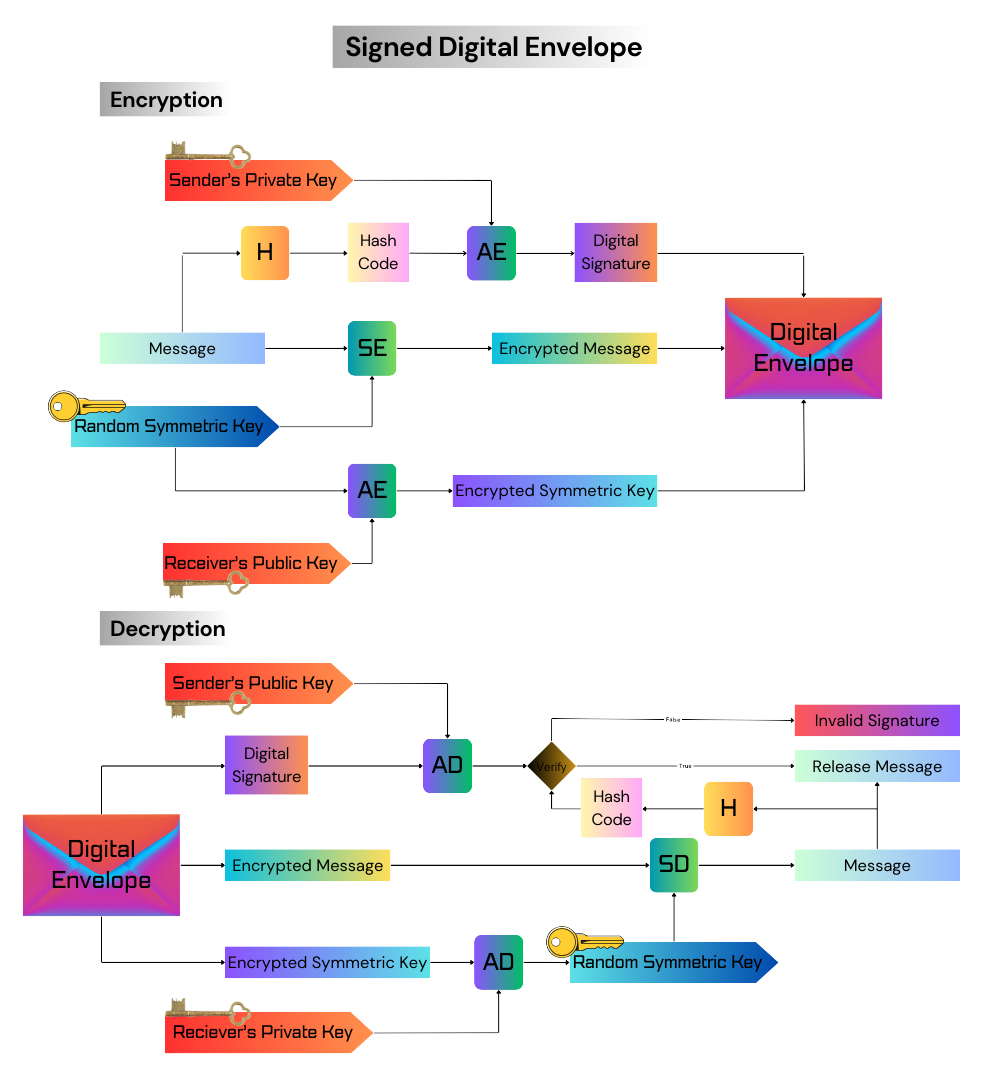
Lab 03

Signed Digital Envelope

Ethan Conner

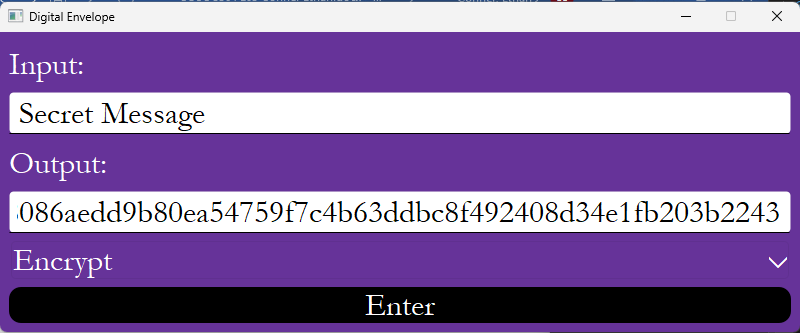
Lab 03

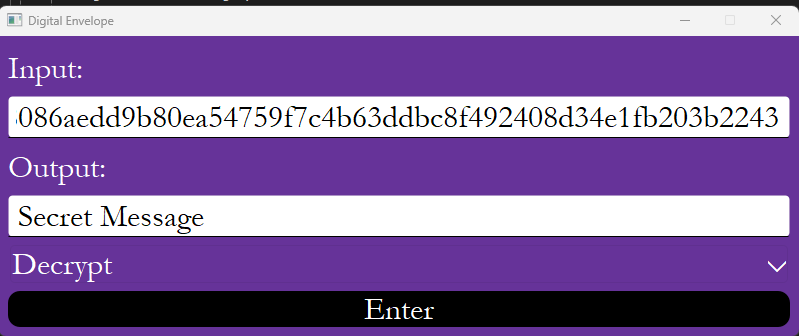
1. Develop a program to generate a signed digital envelope utilizing RSA for the asymmetric encryption of the symmetric key & digital signature, AES in CBC mode for the symmetric encryption of the message, and SHA256 for the hash function.



**ANSWER IN SCREENSHOTS BELOW**

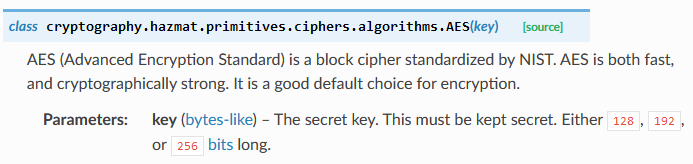
**Output Screenshots**





I attached my .py file to the submission.

AES



A screenshot of a computer code

Description automatically generated

RSA

A screenshot of a computer

Description automatically generated

RSA Encryption

A screenshot of a computer

Description automatically generated

RSA Decryption

A screenshot of a computer

Description automatically generated

RSA Signing

A screenshot of a computer error

Description automatically generated

RSA Verification

A screenshot of a computer program

Description automatically generated

SHA-256

A screenshot of a computer

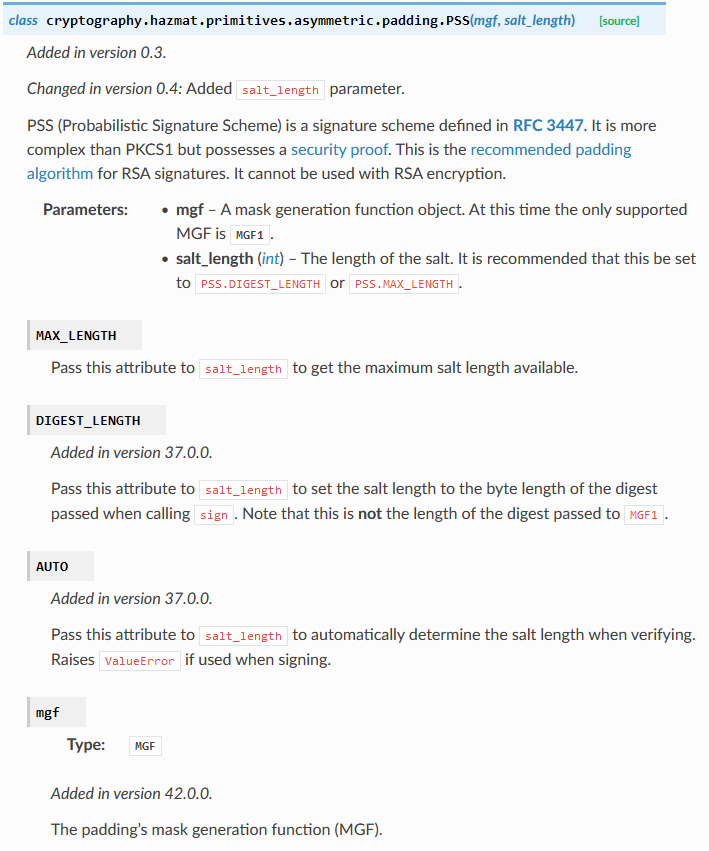
Description automatically generated

CBC

A screenshot of a computer

Description automatically generated

PSS



MGF1

A screenshot of a computer

Description automatically generated

OAEP

A screenshot of a computer

Description automatically generated

PKCS7

A screenshot of a computer

Description automatically generated

InvalidSignature Exception

A screenshot of a computer

Description automatically generated