Assignment (Cyber Secuirty)

Have students write programs to encode and decode text or files in C/Python/Java/JavaScript, etc.

Requirements

• The program uses AES with a 256 bits key to encrypt text (only text is encrypted) and other files (such as PDF, JPG, Doc, etc.).

• IV (Initialization vector) for AES is used as Random.

• Can be decrypted back to the original file (with functions or methods for both encoding and decoding)

• So there will be 1 text file and 1 other file type.

1. The text file will contain the message as student ID and last name. Just take the text in the text file and encode it and make a digital signature with RSA with a key size of 2048 bits (Create a digital signature, use SHA512 and sign with a private key).

2. Other files (such as PDF, JPG, Doc, etc.) must be encoded in the whole file and no digital signature is required.

what to send

1. Source code

2. Video showing encoding and decoding and explaining the principle of the program (no more than 5 minutes)

3. Text Signature

4. Both source files

5. File after encoding (if text file, specify encrypted text)