DES & AES Encryption

Data Encryption Standard (DES)

DES is a symmetric-key encryption algorithm mainly used for secure transmission of data. It encrypts data in 64-bit blocks with the help of a 56-bit key. In it, 16 rounds of permutations and substitution are performed according to the Feistel structure.

Features:

- **Block Size:** 64 bits
- **Key Length:** 56 bits
- **Structure:** Feistel network
- **Security:** Considered insecure by modern standards due to its small key size, making it vulnerable to brute-force attacks.

Advanced Encryption Standard (AES)

AES is a symmetric-key block cipher developed to replace DES. It encrypts data blocks of 128 bits and supports key lengths of 128, 192, and 256 bits. It uses a substitution-permutation network for encryption and decryption.

Features:

- **Block Size:** 128 bits
- **Key Lengths:** 128, 192, or 256 bits
- **Structure:** Substitution-Permutation network
- **Security:** Highly secure and widely used in modern cryptographic systems.

Python Libraries for DES and AES

Pycryptodome:

- Provides implementations of both DES and AES.
- Easy-to-use methods for encryption and decryption.
- Example: Crypto.Cipher.DES and Crypto.Cipher.AES.

cryptography:

- A robust library for cryptographic operations.
- Supports AES with options for different modes (e.g., CBC, GCM).
- DES is not directly implemented due to its obsolescence, but Triple DES (DES3) is available.

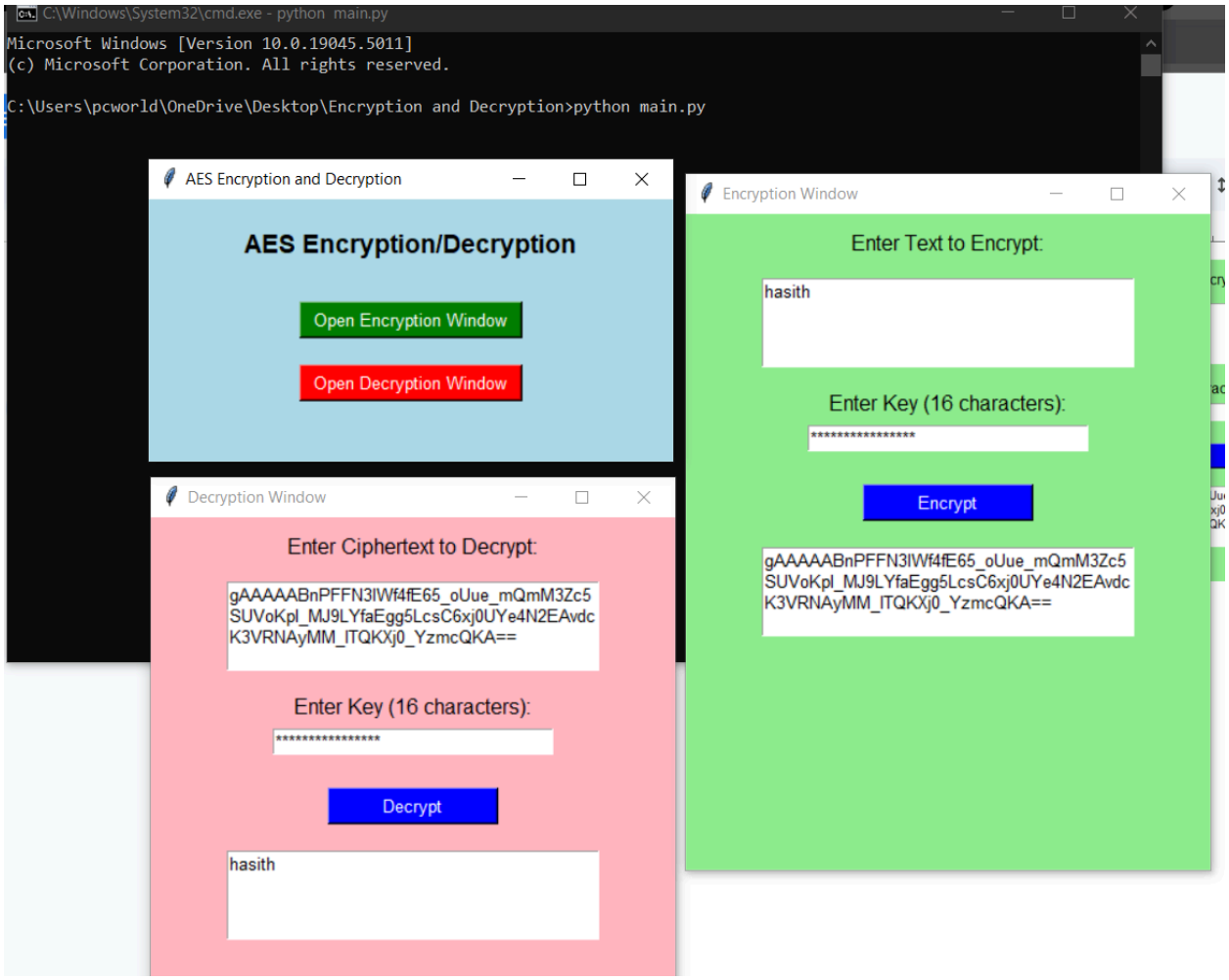
pyCrypto (Deprecated, replaced by pycryptodome):

- Older library for cryptographic tasks; not recommended for new projects.

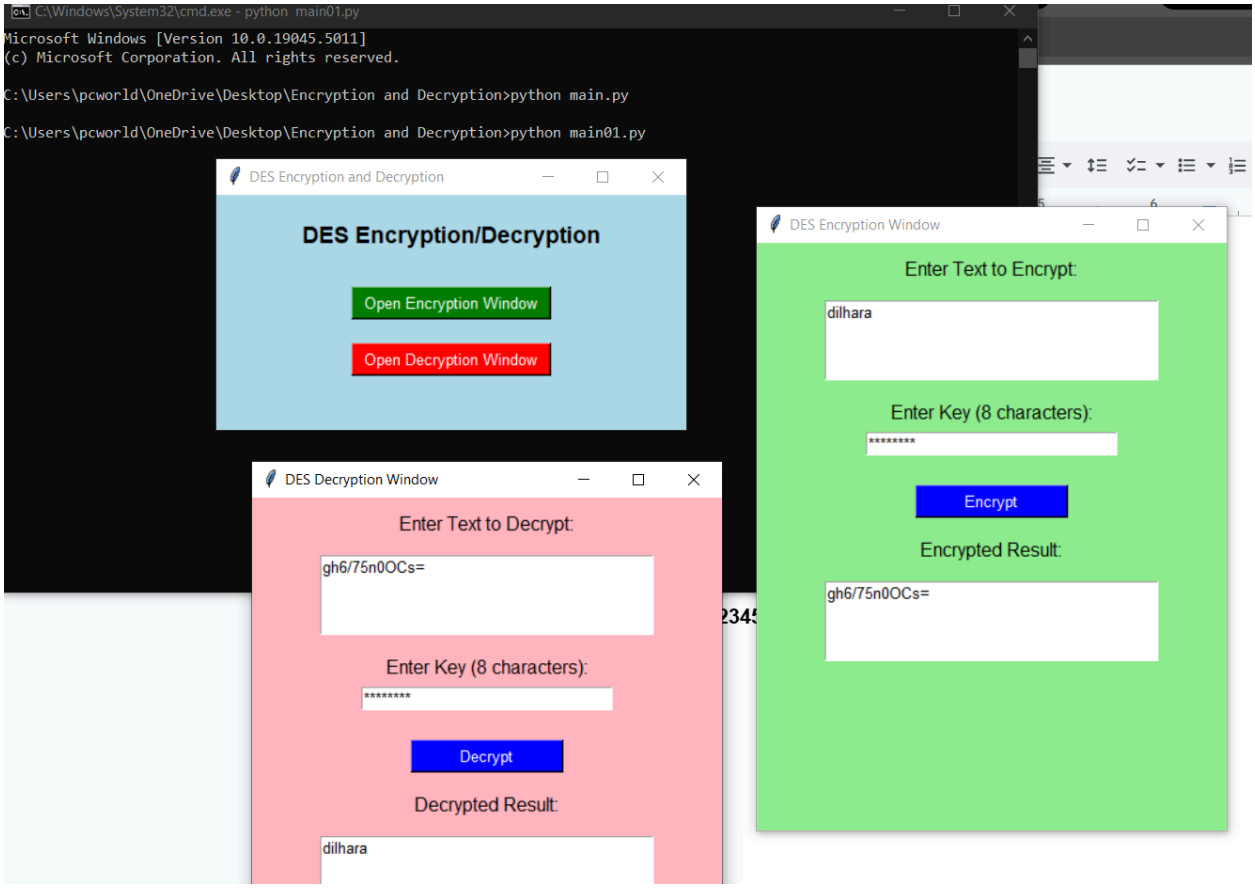
mcrypt:

- Supports both DES and AES but is less commonly used.

AES application key = “1234567812345678”



DES application key = “12345678”


C:\Windows\System32\cmd.exe - python main01.py
Microsoft Windows [Version 10.0.19045.5011]
(c) Microsoft Corporation. All rights reserved.
C:\Users\pcworld\OneDrive\Desktop\Encryption and Decryption>python main.py
C:\Users\pcworld\OneDrive\Desktop\Encryption and Decryption>python main01.py
DES Encryption and Decryption
DES Encryption/Decryption
Open Encryption Window
Open Decryption Window
DES Encryption Window
Enter Text to Encrypt:
dilhara
Enter Key (8 characters):
****
Encrypt
Encrypted Result:
gh6/75n0OCs=
DES Decryption Window
Enter Text to Decrypt:
gh6/75n0OCs=
Enter Key (8 characters):
****
Decrypt
Decrypted Result:
dilhara