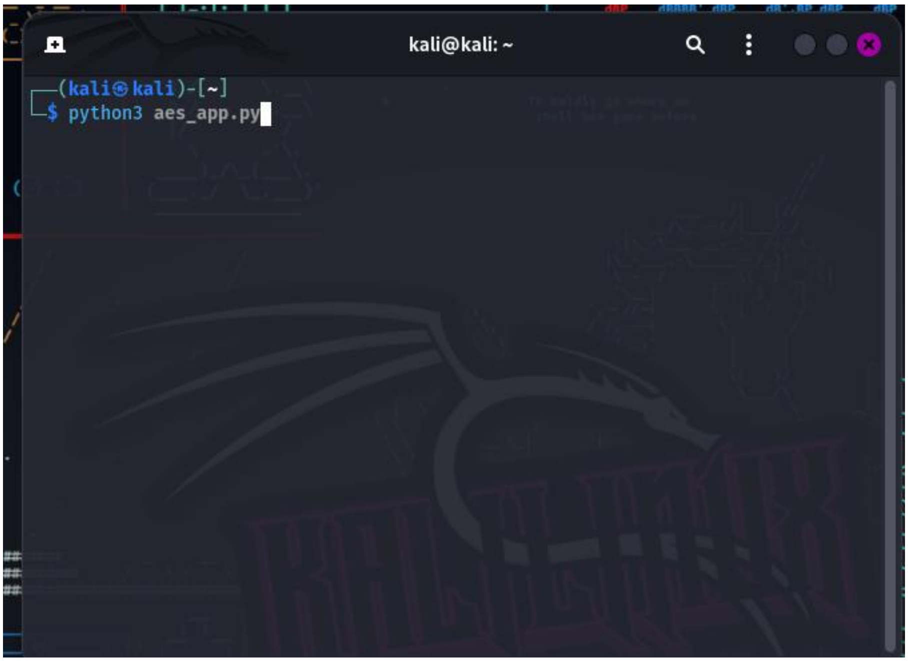
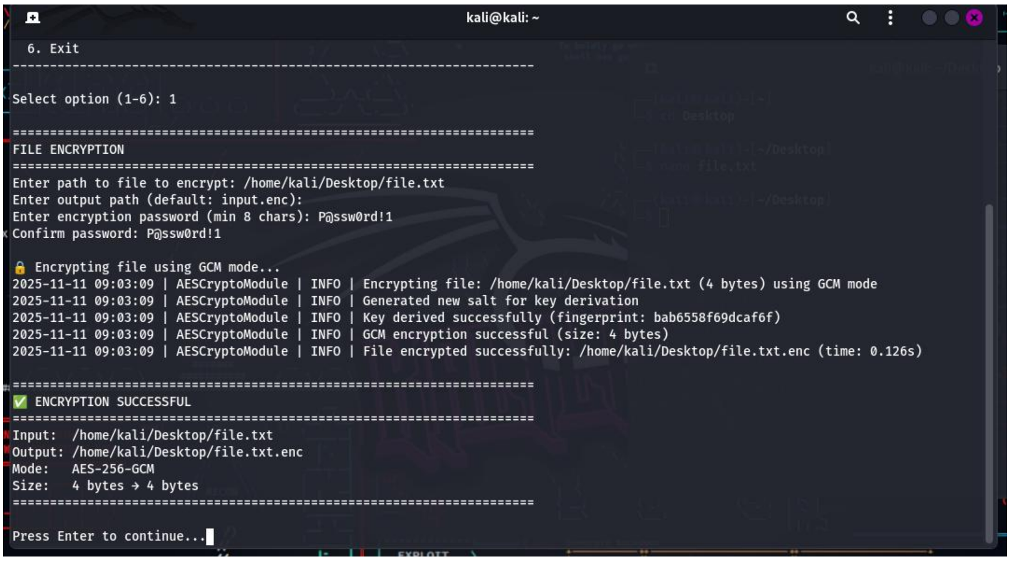
Документація до програми aes_app.py

1) Запуск програми:



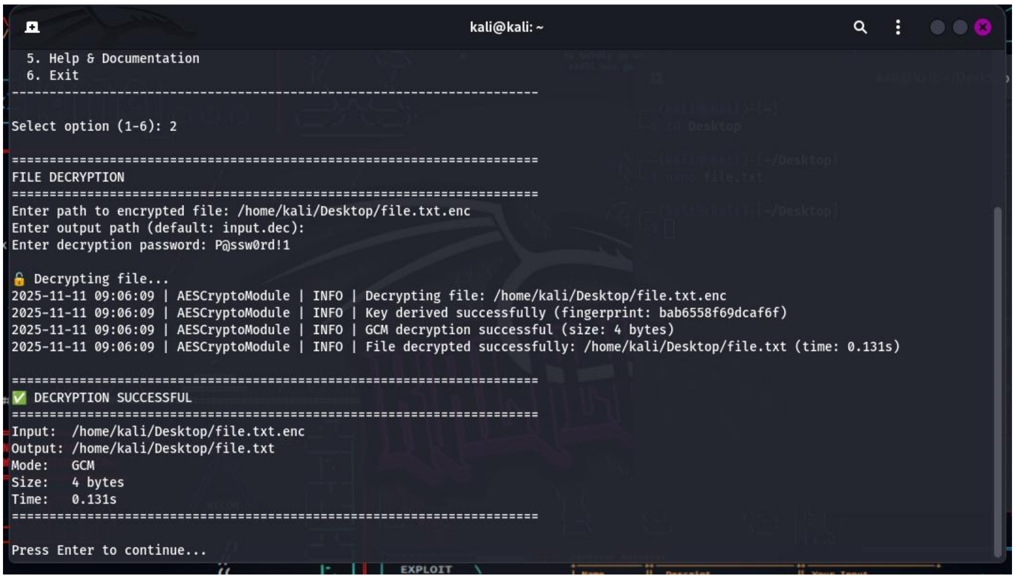
```
┌──(kali㉿kali)-[~]
└─$ python3 aes_app.py
```

2) Шифрування файлу:



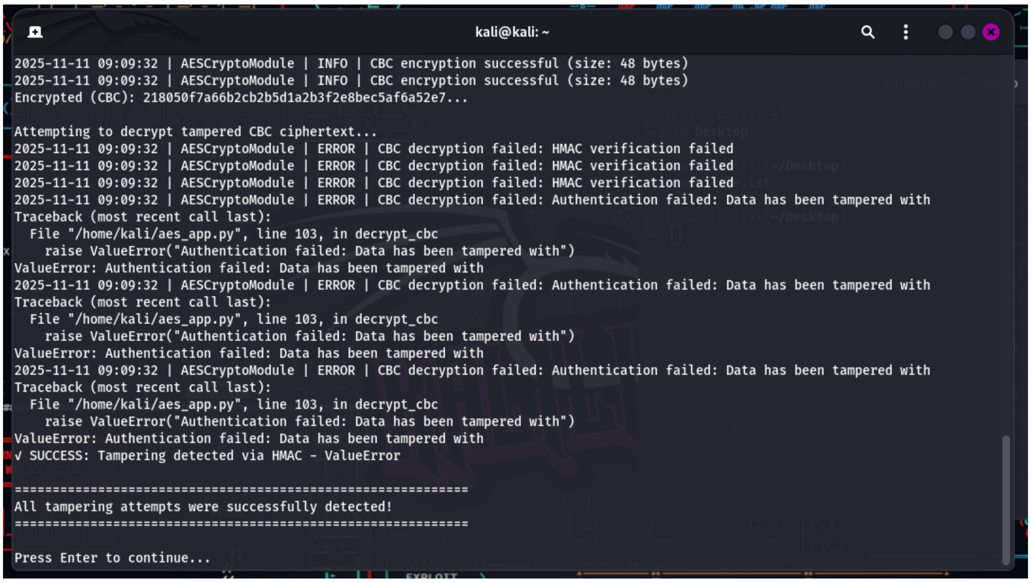
```
  6. Exit
----------------------------------------------------------------------

Select option (1-6): 1

======================================================================
FILE ENCRYPTION
======================================================================
Enter path to file to encrypt: /home/kali/Desktop/file.txt
Enter output path (default: input.enc):
Enter encryption password (min 8 chars): P@ssw0rd!1
Confirm password: P@ssw0rd!1

🔒 Encrypting file using GCM mode...
2025-11-11 09:03:09 | AESCryptoModule | INFO | Encrypting file: /home/kali/Desktop/file.txt (4 bytes) using GCM mode
2025-11-11 09:03:09 | AESCryptoModule | INFO | Generated new salt for key derivation
2025-11-11 09:03:09 | AESCryptoModule | INFO | Key derived successfully (fingerprint: bab6558f69dcaf6f)
2025-11-11 09:03:09 | AESCryptoModule | INFO | GCM encryption successful (size: 4 bytes)
2025-11-11 09:03:09 | AESCryptoModule | INFO | File encrypted successfully: /home/kali/Desktop/file.txt.enc (time: 0.126s)

======================================================================
✅ ENCRYPTION SUCCESSFUL
======================================================================
Input:  /home/kali/Desktop/file.txt
Output: /home/kali/Desktop/file.txt.enc
Mode:   AES-256-GCM
Size:   4 bytes → 4 bytes
======================================================================

Press Enter to continue...
```

3) Дешифрування файлу:



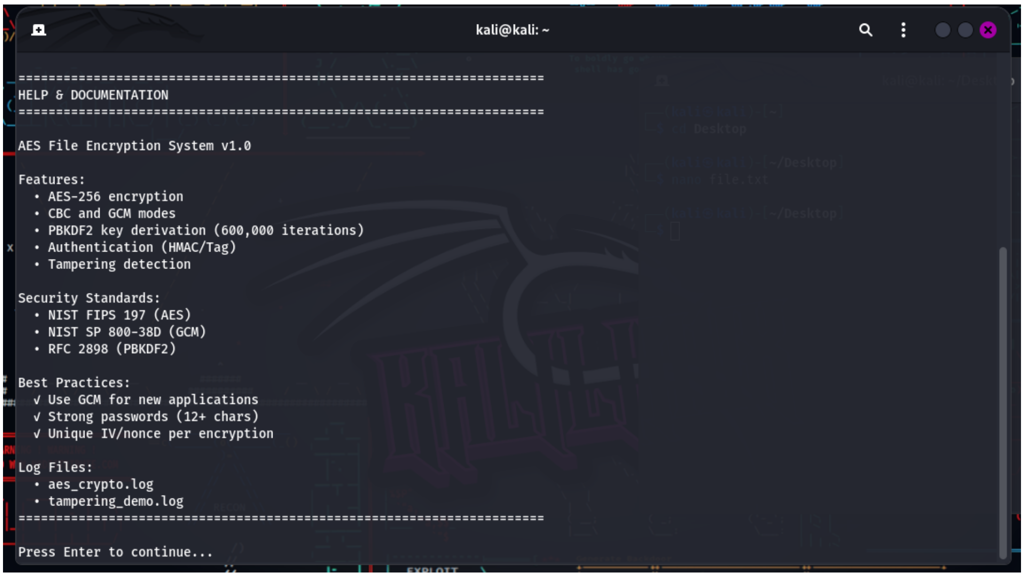
```
  5. Help & Documentation
  6. Exit
----------------------------------------------------------------------

Select option (1-6): 2

======================================================================
FILE DECRYPTION
======================================================================
Enter path to encrypted file: /home/kali/Desktop/file.txt.enc
Enter output path (default: input.dec):
Enter decryption password: P@ssw0rd!1

🔓 Decrypting file...
2025-11-11 09:06:09 | AESCryptoModule | INFO | Decrypting file: /home/kali/Desktop/file.txt.enc
2025-11-11 09:06:09 | AESCryptoModule | INFO | Key derived successfully (fingerprint: bab6558f69dcaf6f)
2025-11-11 09:06:09 | AESCryptoModule | INFO | GCM decryption successful (size: 4 bytes)
2025-11-11 09:06:09 | AESCryptoModule | INFO | File decrypted successfully: /home/kali/Desktop/file.txt (time: 0.131s)

======================================================================
✅ DECRYPTION SUCCESSFUL
======================================================================
Input:  /home/kali/Desktop/file.txt.enc
Output: /home/kali/Desktop/file.txt
Mode:   GCM
Size:   4 bytes
Time:   0.131s
======================================================================

Press Enter to continue...
```

4) Аналіз продуктивності:



```
2025-11-11 09:09:32 | AESCryptoModule | INFO | CBC encryption successful (size: 48 bytes)
2025-11-11 09:09:32 | AESCryptoModule | INFO | CBC encryption successful (size: 48 bytes)
Encrypted (CBC): 218050f7a66b2cb2b5d1a2b3f2e8bec5af6a52e7...

Attempting to decrypt tampered CBC ciphertext...
2025-11-11 09:09:32 | AESCryptoModule | ERROR | CBC decryption failed: HMAC verification failed
2025-11-11 09:09:32 | AESCryptoModule | ERROR | CBC decryption failed: HMAC verification failed
2025-11-11 09:09:32 | AESCryptoModule | ERROR | CBC decryption failed: HMAC verification failed
2025-11-11 09:09:32 | AESCryptoModule | ERROR | CBC decryption failed: Authentication failed: Data has been tampered with
Traceback (most recent call last):
  File "/home/kali/aes_app.py", line 103, in decrypt_cbc
    raise ValueError("Authentication failed: Data has been tampered with")
ValueError: Authentication failed: Data has been tampered with
2025-11-11 09:09:32 | AESCryptoModule | ERROR | CBC decryption failed: Authentication failed: Data has been tampered with
Traceback (most recent call last):
  File "/home/kali/aes_app.py", line 103, in decrypt_cbc
    raise ValueError("Authentication failed: Data has been tampered with")
ValueError: Authentication failed: Data has been tampered with
2025-11-11 09:09:32 | AESCryptoModule | ERROR | CBC decryption failed: Authentication failed: Data has been tampered with
Traceback (most recent call last):
  File "/home/kali/aes_app.py", line 103, in decrypt_cbc
    raise ValueError("Authentication failed: Data has been tampered with")
ValueError: Authentication failed: Data has been tampered with
√ SUCCESS: Tampering detected via HMAC - ValueError

============================================================
All tampering attempts were successfully detected!
============================================================

Press Enter to continue...
```

5) Документація:



```
======================================================================
HELP & DOCUMENTATION
======================================================================

AES File Encryption System v1.0

Features:
  • AES-256 encryption
  • CBC and GCM modes
  • PBKDF2 key derivation (600,000 iterations)
  • Authentication (HMAC/Tag)
  • Tampering detection

Security Standards:
  • NIST FIPS 197 (AES)
  • NIST SP 800-38D (GCM)
  • RFC 2898 (PBKDF2)

Best Practices:
  √ Use GCM for new applications
  √ Strong passwords (12+ chars)
  √ Unique IV/nonce per encryption

Log Files:
  • aes_crypto.log
  • tampering_demo.log
======================================================================

Press Enter to continue...
```