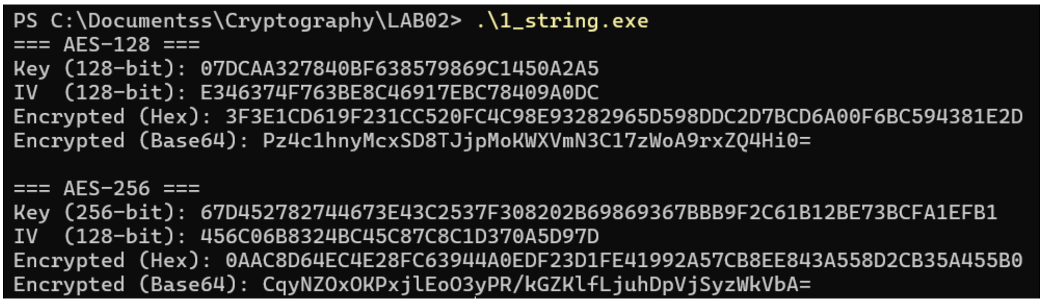
NT219 - BTTL - LAB02

Nguyễn Hoàng Quý - 24521494

Ngày 15 tháng 10 năm 2025

Mục lục

1 string.cpp



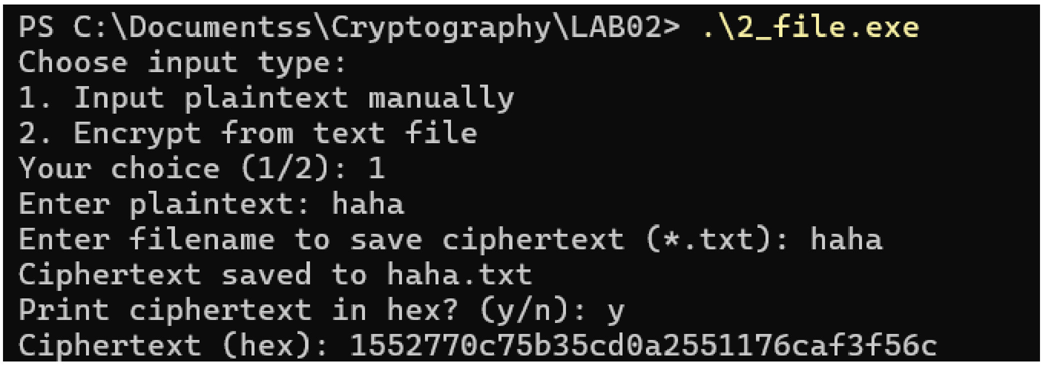
```
PS C:\Documentss\Cryptography\LAB02> .\1_string.exe
=== AES-128 ===
Key (128-bit): 07DCAA327840BF638579869C1450A2A5
IV  (128-bit): E346374F763BE8C46917EBC78409A0DC
Encrypted (Hex): 3F3E1CD619F231CC520FC4C98E93282965D598DDC2D7BCD6A00F6BC594381E2D
Encrypted (Base64): Pz4c1hnyMcxSD8TJjpMoKWXVmN3C17zWoA9rxZQ4Hi0=

=== AES-256 ===
Key (256-bit): 67D452782744673E43C2537F308202B69869367BBB9F2C61B12BE73BCFA1EFB1
IV  (128-bit): 456C06B8324BC45C87C8C1D370A5D97D
Encrypted (Hex): 0AAC8D64EC4E28FC63944A0EDF23D1FE41992A57CB8EE843A558D2CB35A455B0
Encrypted (Base64): CqyNZOxOKPxjlEoO3yPR/kGZKlfLjuhDpVjSyzWkVbA=
```

Hình 1: Kết quả bài string.cpp

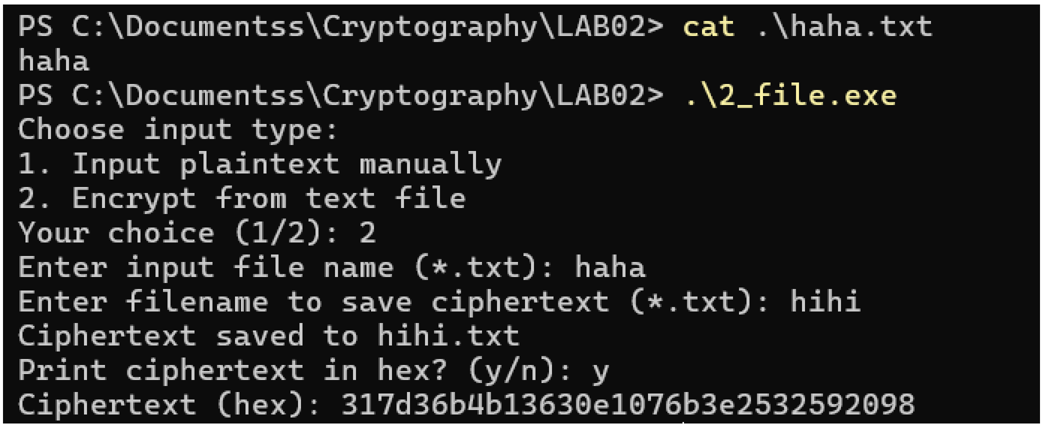
- **Nhận xét:** Ciphertext được in ra dưới dạng chuỗi Hex.

2 file.cpp



```
PS C:\Documentss\Cryptography\LAB02> .\2_file.exe
Choose input type:
1. Input plaintext manually
2. Encrypt from text file
Your choice (1/2): 1
Enter plaintext: haha
Enter filename to save ciphertext (*.txt): haha
Ciphertext saved to haha.txt
Print ciphertext in hex? (y/n): y
Ciphertext (hex): 1552770c75b35cd0a2551176caf3f56c
```

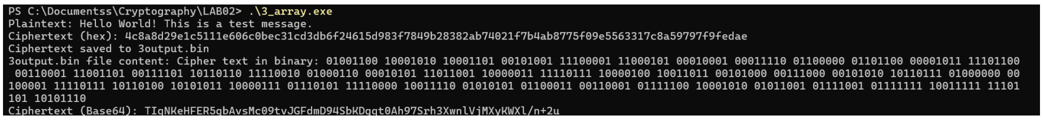
Hình 2: Kết quả nhập plaintext thủ công



```
PS C:\Documentss\Cryptography\LAB02> cat .\haha.txt
haha
PS C:\Documentss\Cryptography\LAB02> .\2_file.exe
Choose input type:
1. Input plaintext manually
2. Encrypt from text file
Your choice (1/2): 2
Enter input file name (*.txt): haha
Enter filename to save ciphertext (*.txt): hihi
Ciphertext saved to hihi.txt
Print ciphertext in hex? (y/n): y
Ciphertext (hex): 317d36b4b13630e1076b3e2532592098
```

Hình 3: Kết quả nhập plaintext từ file

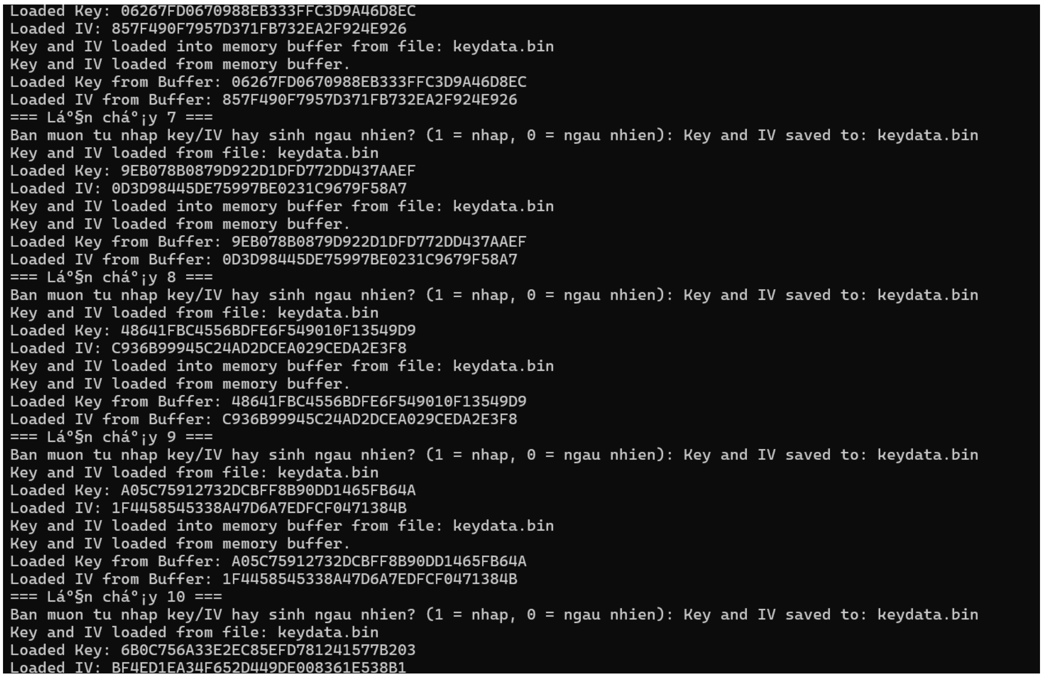
3 array.cpp



```
PS C:\Documentss\Cryptography\LAB02> .\3_array.exe
Plaintext: Hello World! This is a test message.
Ciphertext (hex): 4c8a8d29e1c5111e606c0bec31cd3db6f24615d983f7849b28382ab74021f7b4ab8775f09e5563317c8a59797f9fedae
Ciphertext saved to 3output.bin
3output.bin file content: Cipher text in binary: 01001100 10001010 10001101 00101001 11100001 11000101 00010001 00011110 01100000 01101100 00001011 11101100
 00110001 11001101 00111101 10110110 11110010 01000110 00010101 11011001 10000011 11110111 10000100 10011011 00101000 00111000 00101010 10110111 01000000 00
100001 11110111 10110100 10101011 10000111 01110101 11110000 10011110 01010101 01100011 00110001 01111100 10001010 01011001 01111001 01111111 10011111 11101
101 10101110
Ciphertext (Base64): TIqNKeHFER5gbAvsMc09tvJGFdmD94SbKDgqt0Ah97Srh3XwnlVjMXyKWXl/n+2u
```

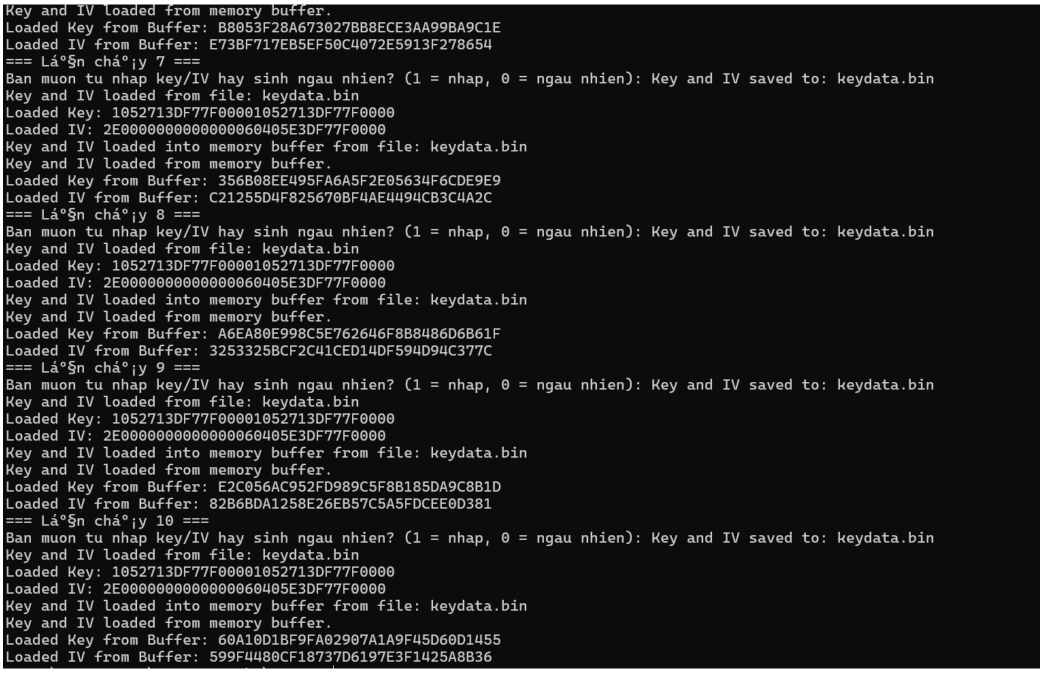
Hình 4: Kết quả chạy array.cpp

4 aeskey.cpp



```
Loaded Key: 06267FD0670988EB333FFC3D9A46D8EC
Loaded IV: 857F490F7957D371FB732EA2F924E926
Key and IV loaded into memory buffer from file: keydata.bin
Key and IV loaded from memory buffer.
Loaded Key from Buffer: 06267FD0670988EB333FFC3D9A46D8EC
Loaded IV from Buffer: 857F490F7957D371FB732EA2F924E926
=== Lá°§n chá°¡y 7 ===
Ban muon tu nhap key/IV hay sinh ngau nhien? (1 = nhap, 0 = ngau nhien): Key and IV saved to: keydata.bin
Key and IV loaded from file: keydata.bin
Loaded Key: 9EB078B0879D922D1DFD772DD437AAEF
Loaded IV: 0D3D98445DE75997BE0231C9679F58A7
Key and IV loaded into memory buffer from file: keydata.bin
Key and IV loaded from memory buffer.
Loaded Key from Buffer: 9EB078B0879D922D1DFD772DD437AAEF
Loaded IV from Buffer: 0D3D98445DE75997BE0231C9679F58A7
=== Lá°§n chá°¡y 8 ===
Ban muon tu nhap key/IV hay sinh ngau nhien? (1 = nhap, 0 = ngau nhien): Key and IV saved to: keydata.bin
Key and IV loaded from file: keydata.bin
Loaded Key: 48641FBC4556BDFE6F549010F13549D9
Loaded IV: C936B99945C24AD2DCEA029CEDA2E3F8
Key and IV loaded into memory buffer from file: keydata.bin
Key and IV loaded from memory buffer.
Loaded Key from Buffer: 48641FBC4556BDFE6F549010F13549D9
Loaded IV from Buffer: C936B99945C24AD2DCEA029CEDA2E3F8
=== Lá°§n chá°¡y 9 ===
Ban muon tu nhap key/IV hay sinh ngau nhien? (1 = nhap, 0 = ngau nhien): Key and IV saved to: keydata.bin
Key and IV loaded from file: keydata.bin
Loaded Key: A05C75912732DCBFF8B90DD1465FB64A
Loaded IV: 1F4458545338A47D6A7EDFCF0471384B
Key and IV loaded into memory buffer from file: keydata.bin
Key and IV loaded from memory buffer.
Loaded Key from Buffer: A05C75912732DCBFF8B90DD1465FB64A
Loaded IV from Buffer: 1F4458545338A47D6A7EDFCF0471384B
=== Lá°§n chá°¡y 10 ===
Ban muon tu nhap key/IV hay sinh ngau nhien? (1 = nhap, 0 = ngau nhien): Key and IV saved to: keydata.bin
Key and IV loaded from file: keydata.bin
Loaded Key: 6B0C756A33E2EC85EFD781241577B203
Loaded IV: BF4ED1EA34F652D449DE008361E538B1
```

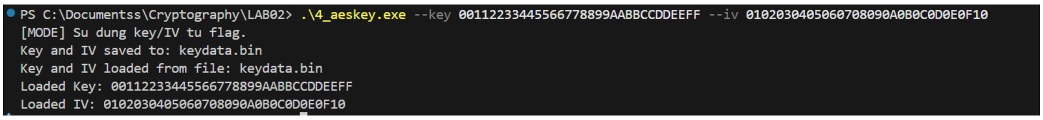
Hình 5: Kết quả chạy 10 lần với bool là false



```
Key and IV loaded from memory buffer.
Loaded Key from Buffer: B8053F28A673027BB8ECE3AA99BA9C1E
Loaded IV from Buffer: E73BF717EB5EF50C4072E5913F278654
=== Lá°§n chá°¡y 7 ===
Ban muon tu nhap key/IV hay sinh ngau nhien? (1 = nhap, 0 = ngau nhien): Key and IV saved to: keydata.bin
Key and IV loaded from file: keydata.bin
Loaded Key: 1052713DF77F00001052713DF77F0000
Loaded IV: 2E000000000000060405E3DF77F0000
Key and IV loaded into memory buffer from file: keydata.bin
Key and IV loaded from memory buffer.
Loaded Key from Buffer: 356B08EE495FA6A5F2E05634F6CDE9E9
Loaded IV from Buffer: C21255D4F825670BF4AE4494CB3C4A2C
=== Lá°§n chá°¡y 8 ===
Ban muon tu nhap key/IV hay sinh ngau nhien? (1 = nhap, 0 = ngau nhien): Key and IV saved to: keydata.bin
Key and IV loaded from file: keydata.bin
Loaded Key: 1052713DF77F00001052713DF77F0000
Loaded IV: 2E000000000000060405E3DF77F0000
Key and IV loaded into memory buffer from file: keydata.bin
Key and IV loaded from memory buffer.
Loaded Key from Buffer: A6EA80E998C5E762646F8B8486D6B61F
Loaded IV from Buffer: 3253325BCF2C41CED14DF594D94C377C
=== Lá°§n chá°¡y 9 ===
Ban muon tu nhap key/IV hay sinh ngau nhien? (1 = nhap, 0 = ngau nhien): Key and IV saved to: keydata.bin
Key and IV loaded from file: keydata.bin
Loaded Key: 1052713DF77F00001052713DF77F0000
Loaded IV: 2E000000000000060405E3DF77F0000
Key and IV loaded into memory buffer from file: keydata.bin
Key and IV loaded from memory buffer.
Loaded Key from Buffer: E2C056AC952FD989C5F8B185DA9C8B1D
Loaded IV from Buffer: 82B6BDA1258E26EB57C5A5FDCEE0D381
=== Lá°§n chá°¡y 10 ===
Ban muon tu nhap key/IV hay sinh ngau nhien? (1 = nhap, 0 = ngau nhien): Key and IV saved to: keydata.bin
Key and IV loaded from file: keydata.bin
Loaded Key: 1052713DF77F00001052713DF77F0000
Loaded IV: 2E000000000000060405E3DF77F0000
Key and IV loaded into memory buffer from file: keydata.bin
Key and IV loaded from memory buffer.
Loaded Key from Buffer: 60A10D1BF9FA02907A1A9F45D60D1455
Loaded IV from Buffer: 599F4480CF18737D6197E3F1425A8B36
```

Hình 6: Kết quả chạy 10 lần với bool là true

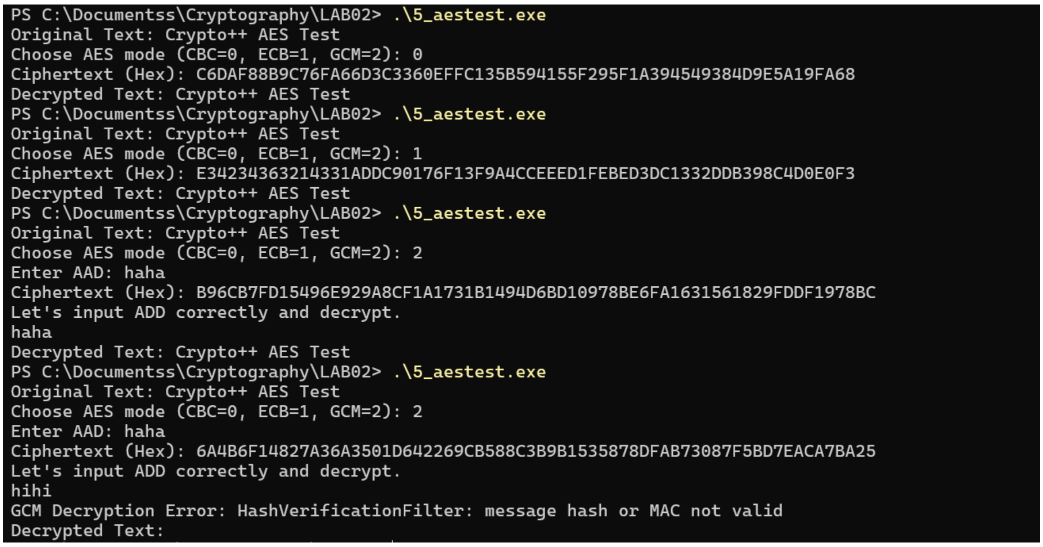
- **Nhận xét:** Nhận thấy IV và KEY trong Buffer khác hoàn toàn so với IV và KEY được tạo ở input.
- **Nguyên nhân:** Do cờ `true` trong hàm `FileSource` có ý nghĩa đọc dữ liệu trong file ngay lập tức, làm cho hàm `PumpUp()` phía sau mất tác dụng dẫn đến sai lệch giữa IV và KEY trong input và buffer.



```
PS C:\Documentss\Cryptography\LAB02> .\4_aeskey.exe --key 00112233445566778899AABBCCDDEEFF --iv 0102030405060708090A0B0C0D0E0F10
[MODE] Su dung key/IV tu flag.
Key and IV saved to: keydata.bin
Key and IV loaded from file: keydata.bin
Loaded Key: 00112233445566778899AABBCCDDEEFF
Loaded IV: 0102030405060708090A0B0C0D0E0F10
```

Hình 7: Kết quả cho phép nhập KEY/IV từ bàn phím dạng hex

5 aestest.cpp

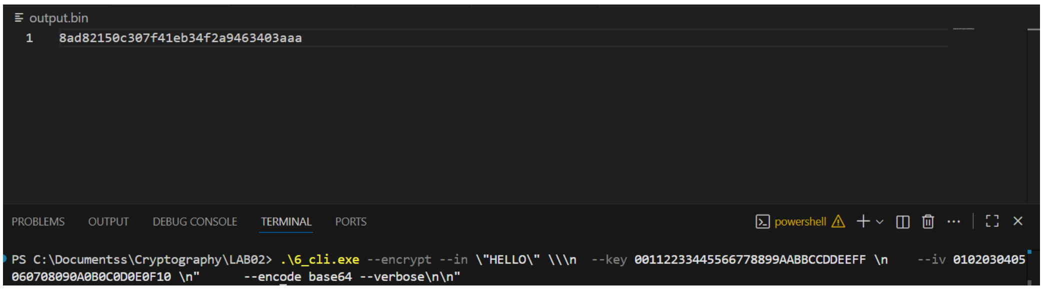


```
PS C:\Documentss\Cryptography\LAB02> .\5_aestest.exe
Original Text: Crypto++ AES Test
Choose AES mode (CBC=0, ECB=1, GCM=2): 0
Ciphertext (Hex): C6DAF88B9C76FA66D3C3360EFFC135B594155F295F1A394549384D9E5A19FA68
Decrypted Text: Crypto++ AES Test
PS C:\Documentss\Cryptography\LAB02> .\5_aestest.exe
Original Text: Crypto++ AES Test
Choose AES mode (CBC=0, ECB=1, GCM=2): 1
Ciphertext (Hex): E34234363214331ADDC90176F13F9A4CCEEED1FEBED3DC1332DDB398C4D0E0F3
Decrypted Text: Crypto++ AES Test
PS C:\Documentss\Cryptography\LAB02> .\5_aestest.exe
Original Text: Crypto++ AES Test
Choose AES mode (CBC=0, ECB=1, GCM=2): 2
Enter AAD: haha
Ciphertext (Hex): B96CB7FD15496E929A8CF1A1731B1494D6BD10978BE6FA1631561829FDDF1978BC
Let's input ADD correctly and decrypt.
haha
Decrypted Text: Crypto++ AES Test
PS C:\Documentss\Cryptography\LAB02> .\5_aestest.exe
Original Text: Crypto++ AES Test
Choose AES mode (CBC=0, ECB=1, GCM=2): 2
Enter AAD: haha
Ciphertext (Hex): 6A4B6F14827A36A3501D642269CB588C3B9B1535878DFAB73087F5BD7EACA7BA25
Let's input ADD correctly and decrypt.
hihi
GCM Decryption Error: HashVerificationFilter: message hash or MAC not valid
Decrypted Text:
```

Hình 8: Kết quả chạy aestest.cpp

- Kết quả đúng như dự kiến, sau khi build `aestest.cpp` thì khi chạy sẽ cho phép chọn giữa 3 mode: ECB, CBC và GCM. Đặc biệt với GCM, yêu cầu nhập AAD trước khi encrypt và decrypt để đảm bảo tính toàn vẹn (integrity) theo ý tưởng của GCM.

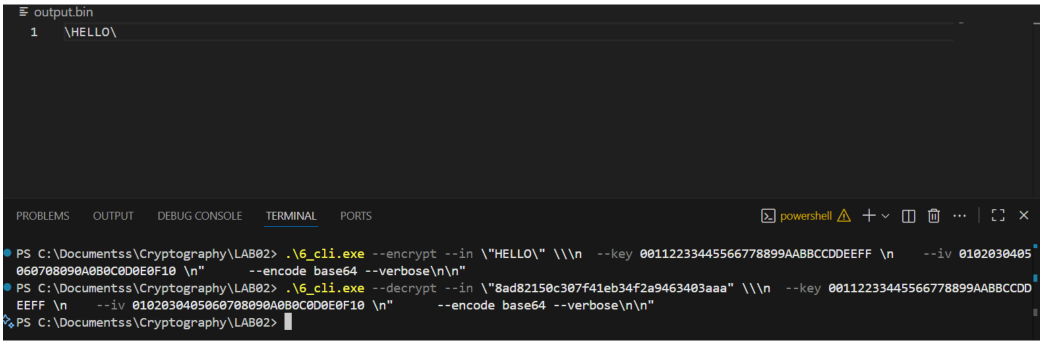
6 cli.cpp



```
8ad82150c307f41eb34f2a9463403aaa
```

```
PS C:\Documentss\Cryptography\LAB02> .\6_cli.exe --encrypt --in \"HELLO\" \\\n  --key 00112233445566778899AABBCCDDEEFF \n    --iv 0102030405
060708090A0B0C0D0E0F10 \n"       --encode base64 --verbose\n\n"
```

Hình 9: Kết quả sau khi encrypt được lưu vào output.bin

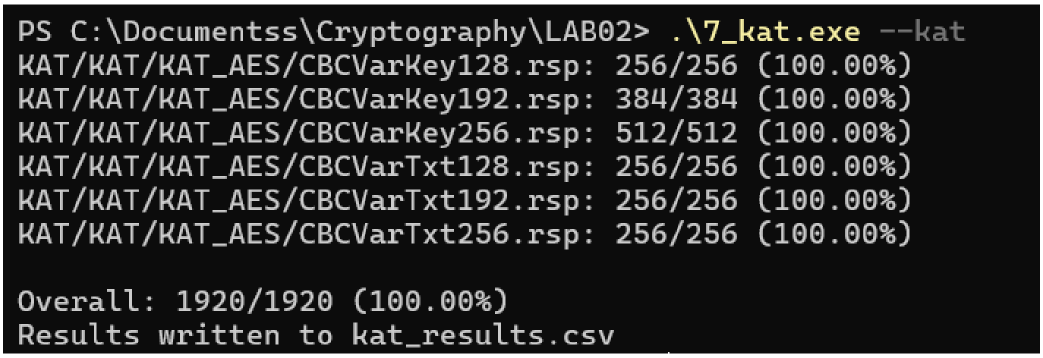


```
\HELLO\
```

```
PS C:\Documentss\Cryptography\LAB02> .\6_cli.exe --encrypt --in \"HELLO\" \\\n  --key 00112233445566778899AABBCCDDEEFF \n    --iv 0102030405
060708090A0B0C0D0E0F10 \n"      --encode base64 --verbose\n\n"
PS C:\Documentss\Cryptography\LAB02> .\6_cli.exe --decrypt --in \"8ad82150c307f41eb34f2a9463403aaa" \\\n  --key 00112233445566778899AABBCCDD
EEFF \n    --iv 0102030405060708090A0B0C0D0E0F10 \n"      --encode base64 --verbose\n\n"
PS C:\Documentss\Cryptography\LAB02> 
```

Hình 10: Kết quả sau khi decrypt được lưu vào output.bin

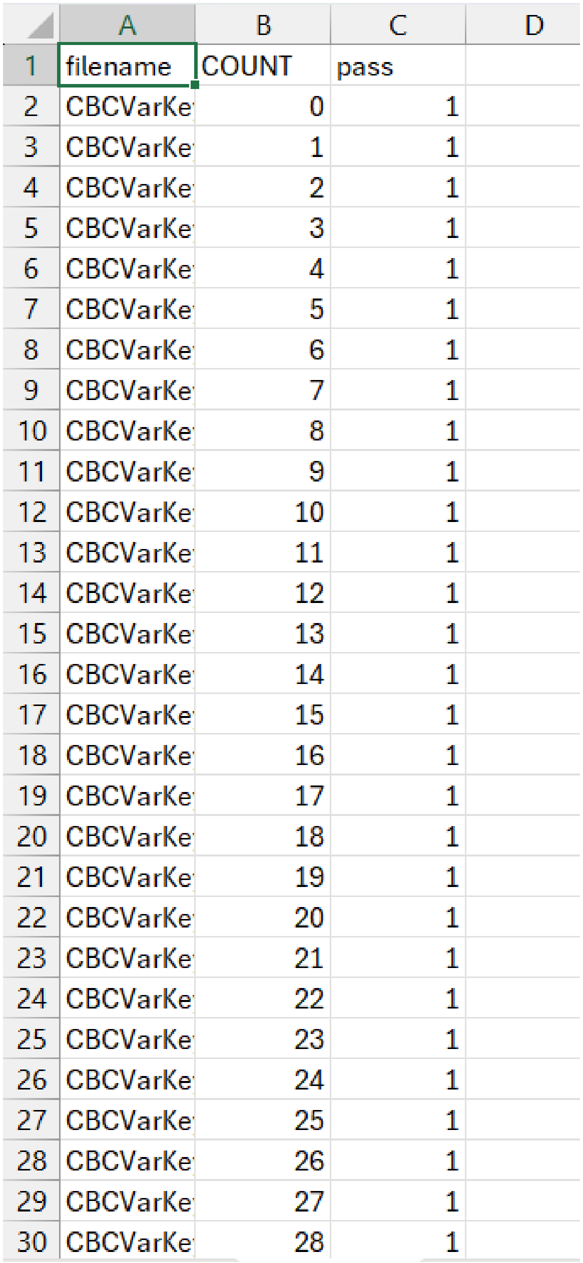
7 kat.cpp



```
PS C:\Documentss\Cryptography\LAB02> .\7_kat.exe --kat
KAT/KAT/KAT_AES/CBCVarKey128.rsp: 256/256 (100.00%)
KAT/KAT/KAT_AES/CBCVarKey192.rsp: 384/384 (100.00%)
KAT/KAT/KAT_AES/CBCVarKey256.rsp: 512/512 (100.00%)
KAT/KAT/KAT_AES/CBCVarTxt128.rsp: 256/256 (100.00%)
KAT/KAT/KAT_AES/CBCVarTxt192.rsp: 256/256 (100.00%)
KAT/KAT/KAT_AES/CBCVarTxt256.rsp: 256/256 (100.00%)

Overall: 1920/1920 (100.00%)
Results written to kat_results.csv
```

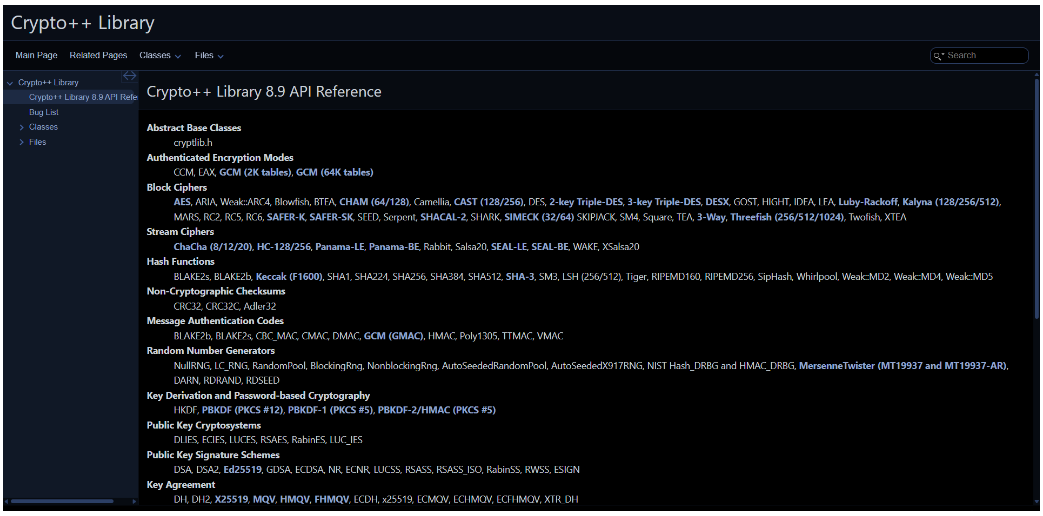
Hình 11: Chạy code KAT.cpp



	A	B	C	D
1	filename	COUNT	pass	
2	CBCVarKe	0	1	
3	CBCVarKe	1	1	
4	CBCVarKe	2	1	
5	CBCVarKe	3	1	
6	CBCVarKe	4	1	
7	CBCVarKe	5	1	
8	CBCVarKe	6	1	
9	CBCVarKe	7	1	
10	CBCVarKe	8	1	
11	CBCVarKe	9	1	
12	CBCVarKe	10	1	
13	CBCVarKe	11	1	
14	CBCVarKe	12	1	
15	CBCVarKe	13	1	
16	CBCVarKe	14	1	
17	CBCVarKe	15	1	
18	CBCVarKe	16	1	
19	CBCVarKe	17	1	
20	CBCVarKe	18	1	
21	CBCVarKe	19	1	
22	CBCVarKe	20	1	
23	CBCVarKe	21	1	
24	CBCVarKe	22	1	
25	CBCVarKe	23	1	
26	CBCVarKe	24	1	
27	CBCVarKe	25	1	
28	CBCVarKe	26	1	
29	CBCVarKe	27	1	
30	CBCVarKe	28	1	

Hình 12: Kết quả sau khi chạy KAT

8 cryptoguides



Crypto++ Library 8.9 API Reference

Abstract Base Classes
cryptlib.h

Authenticated Encryption Modes
CCM, EAX, **GCM (2K tables)**, **GCM (64K tables)**

Block Ciphers
AES, ARIA, Weak::ARC4, Blowfish, BTEA, **CHAM (64/128)**, Camellia, **CAST (128/256)**, DES, **2-key Triple-DES**, **3-key Triple-DES**, **DESX**, GOST, HIGHT, IDEA, LEA, **Luby-Rackoff**, **Kalyna (128/256/512)**, MARS, RC2, RC5, RC6, **SAFER-K**, **SAFER-SK**, SEED, Serpent, **SHACAL-2**, SHARK, **SIMECK (32/64)** SKIPJACK, SM4, Square, TEA, **3-Way**, **Threefish (256/512/1024)**, Twofish, XTEA

Stream Ciphers
ChaCha (8/12/20), **HC-128/256**, **Panama-LE**, **Panama-BE**, Rabbit, Salsa20, **SEAL-LE**, **SEAL-BE**, WAKE, XSalsa20

Hash Functions
BLAKE2s, BLAKE2b, **Keccak (F1600)**, SHA1, SHA224, SHA256, SHA384, SHA512, **SHA-3**, SM3, LSH (256/512), Tiger, RIPEMD160, RIPEMD256, SipHash, Whirlpool, Weak::MD2, Weak::MD4, Weak::MD5

Non-Cryptographic Checksums
CRC32, CRC32C, Adler32

Message Authentication Codes
BLAKE2b, BLAKE2s, CBC_MAC, CMAC, DMAC, **GCM (GMAC)**, HMAC, Poly1305, TTMAC, VMAC

Random Number Generators
NullRNG, LC_RNG, RandomPool, BlockingRng, NonblockingRng, AutoSeededRandomPool, AutoSeededX917RNG, NIST Hash_DRBG and HMAC_DRBG, **MersenneTwister (MT19937 and MT19937-AR)**, DARN, RDRAND, RDSEED

Key Derivation and Password-based Cryptography
HKDF, **PBKDF (PKCS #12)**, **PBKDF-1 (PKCS #5)**, **PBKDF-2/HMAC (PKCS #5)**

Public Key Cryptosystems
DLIES, ECIES, LUCES, RSAES, RabinES, LUC_IES

Public Key Signature Schemes
DSA, DSA2, **Ed25519**, GDSA, ECDSA, NR, ECNR, LUCSS, RSASS, RSASS_ISO, RabinSS, RWSS, ESIGN

Key Agreement
DH, DH2, **X25519**, **MQV**, **HMQV**, **FHMQV**, ECDH, x25519, ECMQV, ECHMQV, ECFHMQV, XTR_DH

Hình 13: Kết quả sau khi tạo cryptoguide bằng doxygen