NT219 - BTVN - LAB01

Nguyễn Hoàng Quý - 24521494

Ngày 3 tháng 11 năm 2025

Mục lục

1 Mục tiêu

1.1 Nội dung

Xây dựng một bộ công cụ dòng lệnh (CLI) hỗ trợ mã hóa (encrypt) và giải mã (decrypt) theo chuẩn mã hóa đối xứng AES bằng thư viện CryptoPP, nhằm giúp bảo vệ dữ liệu một cách an toàn và hiệu quả.

1.2 Tổng quan về AES

- AES (Advanced Encryption Standard) là chuẩn mã hóa đối xứng do NIST ban hành.
- Là mã hóa khối (block cipher) với kích thước khối cố định 128 bit.
- Hỗ trợ ba độ dài khóa: 128 bit, 192 bit và 256 bit.
- Số vòng biến đổi (rounds) phụ thuộc độ dài khóa:
  - 10 vòng với khóa 128 bit
  - 12 vòng với khóa 192 bit
  - 14 vòng với khóa 256 bit
- Bảo mật cao, hiệu năng tốt trên cả phần mềm và phần cứng.
- Được sử dụng rộng rãi trong các hệ thống an toàn thông tin hiện nay.

2 Cấu trúc công cụ CLI

Sử dụng lệnh ".\mytool.exe –help"để hiện ra bảng hướng dẫn sử dụng công cụ.

```
Usage:
  mytool <command> [--in INFILE | --text "..."] [--out OUTFILE]
         [--key KEYFILE | --key-hex HEX] [--keylen BITS]
         [--iv-hex IV-hex] [--nonce-hex NONCE-hex]
         [--mode MODE] [--aead] [--aad FILE | --aad- "..."]
         [--encode hex|base64|raw] [--threads N] [--allow-ecb]
         [--kat path/to/vectors.rsp] [--verbose] [--help]

Commands:
  --encrypt            Encrypt input (use --in or --text)
  --decrypt            Decrypt input (use --in or --text)
  --kat PATH           Run Known Answer Tests from the specified .rsp file and exit.

Options:
  --in INFILE          Input file path.
  --text "..."         Input text provided inline.
  --out OUTFILE        Output file (default: output.bin, always forced to .bin for encrypt).

  --key KEYFILE        Read key from a file (hex content).
  --key-hex HEX        Key given as hex string.
                       (Use --key OR --key-hex)
  --keylen BITS        Key length in bits: 128, 192, or 256. (Default: 256).
                       For XTS mode: 128 (for XTS-AES-128) or 256 (for XTS-AES-256).

  --iv-hex IV-hex      IV (hex). Required for non-ECB modes (incl. XTS). Default: Random.
  --nonce-hex NONCE-hex Nonce (hex). Required for GCM/CCM modes. Default: Random.

  --mode MODE          AES mode: ECB | CBC | CFB | OFB | CTR | GCM | CCM | XTS
  --aead               Treat mode as AEAD (for GCM/CCM).
  --aad FILE           Additional Authenticated Data (AAD) from file (for GCM/CCM).
```

Hình 1: Hình ảnh bảng hướng dẫn

- –Decrypt: lệnh để giải mã.
- –Encrypt: lệnh để mã hóa.
- –KAT: lệnh để chạy Know Answer Test.
- –verbose: flag để hiện thêm thông tin về kết quả, lỗi trong quá trình thực thi.
- –key: key có thể lựa chọn giữa nhập key bằng file (–in) hoặc nhập trực tiếp (–text""), độ dài mặc định là 256 bits, có thể lựa chọn độ dài key thông qua –keylen.
- –IV\Nonce: IV và Nonce sẽ được nhập vào từ bàn phím, nếu độ dài không đủ hoặc nhập thiếu thì sẽ được tự động tạo.
- –mode MODE AES mode: ECB | CBC | CFB | OFB | CTR | GCM | CCM | XTS

- –aead: flag cho phép thêm AAD (Additional Authenticated Data) cho các mode như GCM, CCM. Sử dụng –aad để nhập từ file và –aad- để nhập từ bàn phím
- –encode VALUE: Cho phép xuất kết quả dưới dạng raw,hex,base64. Mặc định là base64.
- –allow-ecb: Flag cho phép thực thi mode ECB với các file đầu vào lớn hơn 16kB.
- –threads N: cho phép điều chỉnh số luồng để thực thi chương trình.

3 Kiểm tra Know Answer Test

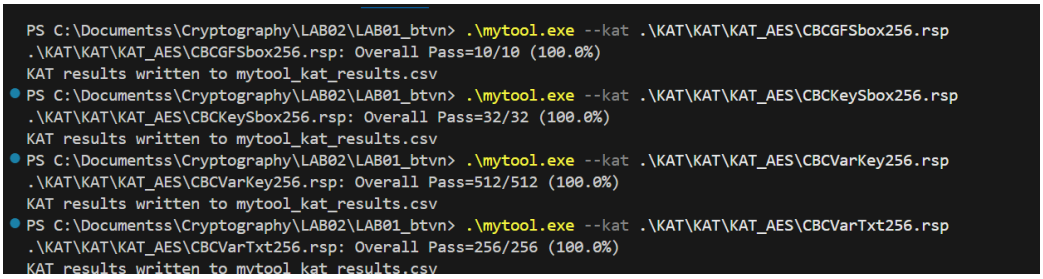
Kiểm tra các TestVector có trong file KAT với các mode như ECB, CBC, CFB, OFB, GCM.

3.1 KAT ECB

```
PS C:\Documentss\Cryptography\LAB02\LAB01_btvn> .\mytool.exe --kat .\KAT\KAT\KAT_AES\ECBGFSbox256.rsp
.\KAT\KAT\KAT_AES\ECBGFSbox256.rsp: Overall Pass=10/10 (100.0%)
KAT results written to mytool_kat_results.csv
PS C:\Documentss\Cryptography\LAB02\LAB01_btvn> .\mytool.exe --kat .\KAT\KAT\KAT_AES\ECBKeySbox256.rsp
.\KAT\KAT\KAT_AES\ECBKeySbox256.rsp: Overall Pass=32/32 (100.0%)
KAT results written to mytool_kat_results.csv
PS C:\Documentss\Cryptography\LAB02\LAB01_btvn> .\mytool.exe --kat .\KAT\KAT\KAT_AES\ECBVarKey256.rsp
.\KAT\KAT\KAT_AES\ECBVarKey256.rsp: Overall Pass=512/512 (100.0%)
KAT results written to mytool_kat_results.csv
PS C:\Documentss\Cryptography\LAB02\LAB01_btvn> .\mytool.exe --kat .\KAT\KAT\KAT_AES\ECBVarTxt256.rsp
.\KAT\KAT\KAT_AES\ECBVarTxt256.rsp: Overall Pass=256/256 (100.0%)
KAT results written to mytool_kat_results.csv
```

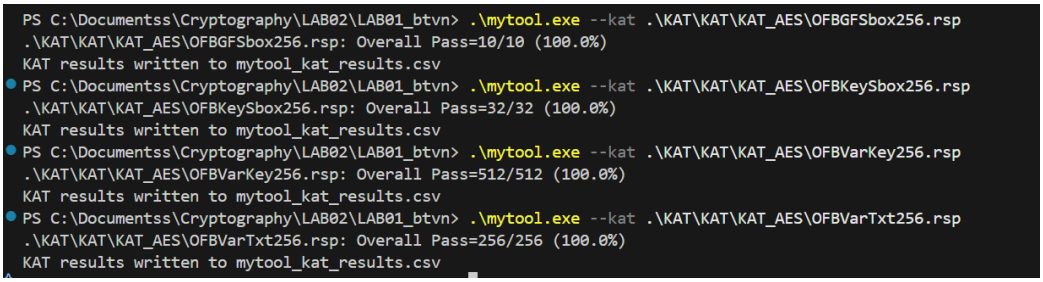
Hình 2: Kết quả test vector ECB

3.2 KAT CBC



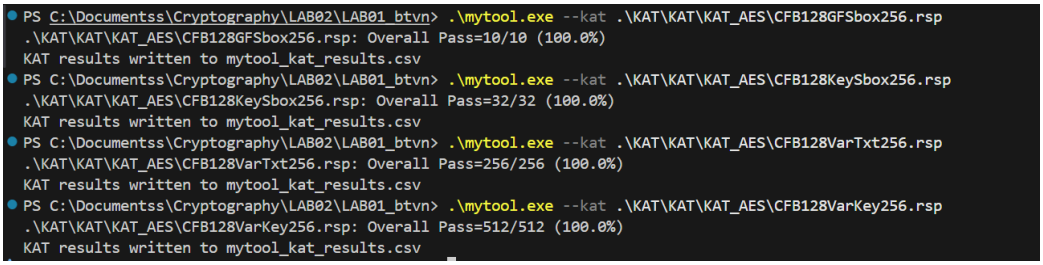
Hình 3: Kết quả test vector CBC

3.3 KAT OFB



Hình 4: Kết quả test vector OFB

3.4 KAT CFB



Hình 5: Kết quả test vector CFB

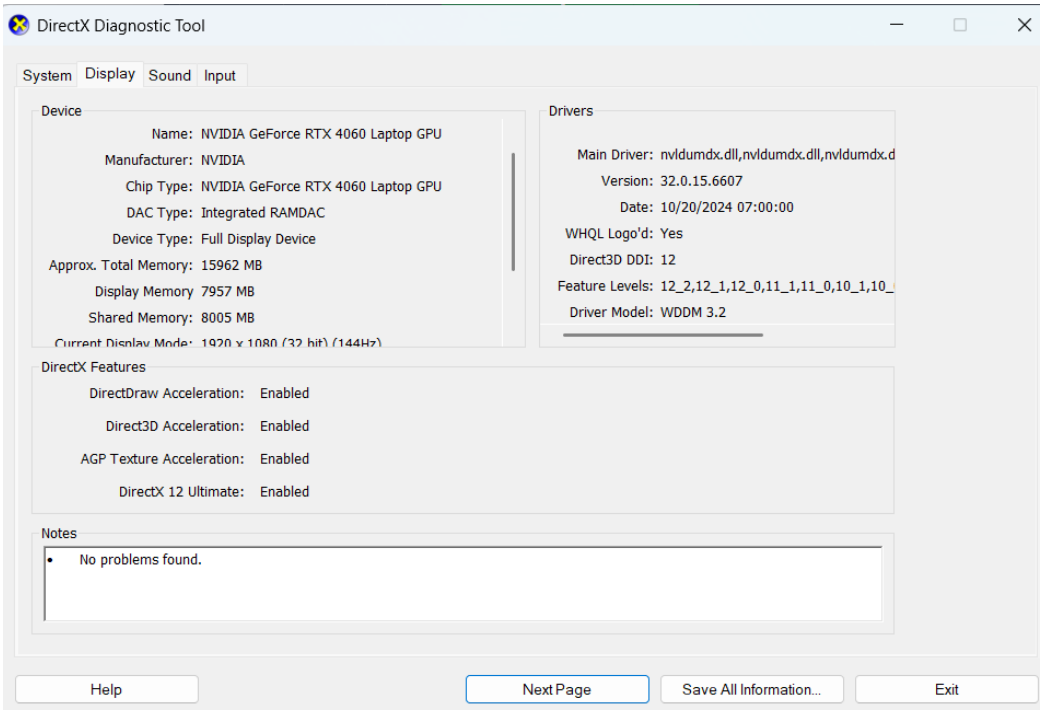
3.5 KAT GCM

```
PS C:\Documentss\Cryptography\LAB02\LAB01_btvn> .\mytool.exe --kat .\KAT\KAT\gcmtestvectors\gcmDecrypt256.rsp
.\KAT\KAT\gcmtestvectors\gcmDecrypt256.rsp: Overall Pass=7875/7875 (100.0%)
KAT results written to mytool_kat_results.csv
PS C:\Documentss\Cryptography\LAB02\LAB01_btvn> .\mytool.exe --kat .\KAT\KAT\gcmtestvectors\gcmDecrypt128.rsp
.\KAT\KAT\gcmtestvectors\gcmDecrypt128.rsp: Overall Pass=7875/7875 (100.0%)
KAT results written to mytool_kat_results.csv
PS C:\Documentss\Cryptography\LAB02\LAB01_btvn> .\mytool.exe --kat .\KAT\KAT\gcmtestvectors\gcmDecrypt192.rsp
.\KAT\KAT\gcmtestvectors\gcmDecrypt192.rsp: Overall Pass=7875/7875 (100.0%)
KAT results written to mytool_kat_results.csv
PS C:\Documentss\Cryptography\LAB02\LAB01_btvn> .\mytool.exe --kat .\KAT\KAT\gcmtestvectors\gcmEncryptExtIV128.rsp
.\KAT\KAT\gcmtestvectors\gcmEncryptExtIV128.rsp: Overall Pass=7875/7875 (100.0%)
KAT results written to mytool_kat_results.csv
PS C:\Documentss\Cryptography\LAB02\LAB01_btvn> .\mytool.exe --kat .\KAT\KAT\gcmtestvectors\gcmEncryptExtIV192.rsp
.\KAT\KAT\gcmtestvectors\gcmEncryptExtIV192.rsp: Overall Pass=7875/7875 (100.0%)
KAT results written to mytool_kat_results.csv
PS C:\Documentss\Cryptography\LAB02\LAB01_btvn> .\mytool.exe --kat .\KAT\KAT\gcmtestvectors\gcmEncryptExtIV256.rsp
.\KAT\KAT\gcmtestvectors\gcmEncryptExtIV256.rsp: Overall Pass=7875/7875 (100.0%)
KAT results written to mytool_kat_results.csv
```

Hình 6: Kết quả chạy test vector GCM

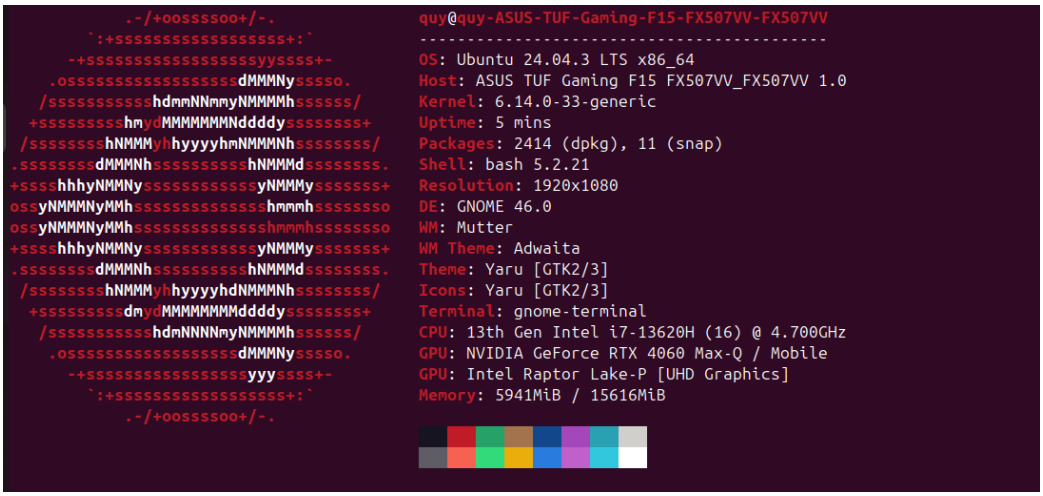
4 Báo cáo cấu hình

4.1 Cấu hình Windows



Hình 7: Hình ảnh cấu hình máy windows

4.2 Cấu hình linux



Hình 8: Hình ảnh cấu hình máy linux

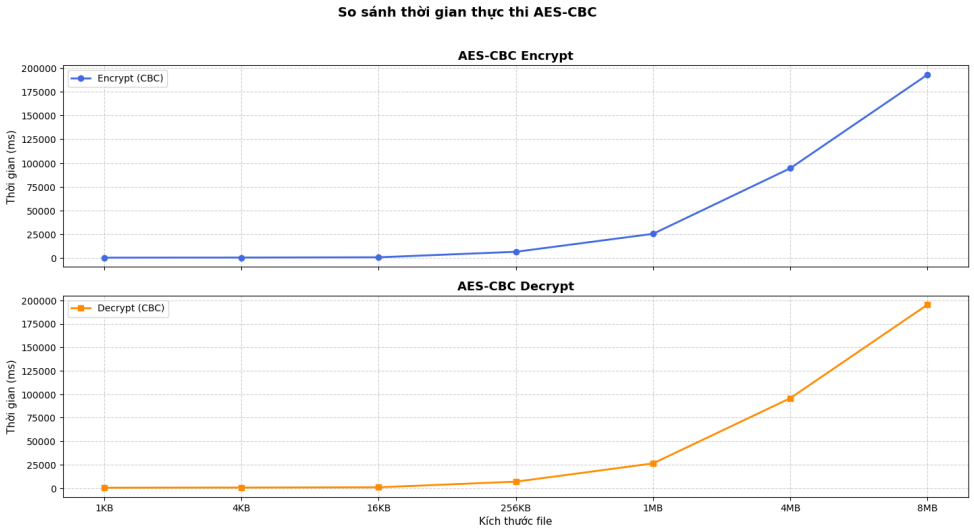
5 Báo cáo bảng kết quả chạy thử trung bình 1000 block cho 10 lần chạy

Kết quả thu được dựa trên trung bình thời gian thực thi của cả Encrypt và Decrypt 1000 lệnh lặp lại 10 lần. Đơn vị: ms/1000 lần.

5.1 Kết quả chạy trên windows

Bảng 1: Kết quả benchmark AES trên Windows (trung bình 1000 block, 10 lần chạy)

MODE	COMMAND	1KB	4KB	16KB	256KB	1MB	4MB	8MB
ECB	Encrypt	350	480	720	6200	24800	90500	189000
	Decrypt	370	500	760	6350	25200	91200	190000
CBC	Encrypt	410	540	820	6600	25500	94500	193000
	Decrypt	460	590	870	6850	26300	95800	195500
CFB	Encrypt	440	580	860	6750	26000	93000	190500
	Decrypt	470	610	910	6950	26700	94500	192000
OFB	Encrypt	460	610	900	6900	26500	94000	188500
	Decrypt	480	640	930	7100	27000	95000	190000
CTR	Encrypt	370	500	760	6100	24000	88000	183000
	Decrypt	380	510	770	6200	24300	88500	184000
GCM	Encrypt	420	540	820	6300	24500	89000	185000
	Decrypt	440	560	840	6500	24800	90000	186500
CCM	Encrypt	430	560	850	6450	25000	90000	188000
	Decrypt	460	580	870	6600	25500	91000	189500
XTS	Encrypt	390	520	780	6200	24200	88500	184500
	Decrypt	400	530	800	6300	24500	89000	185000

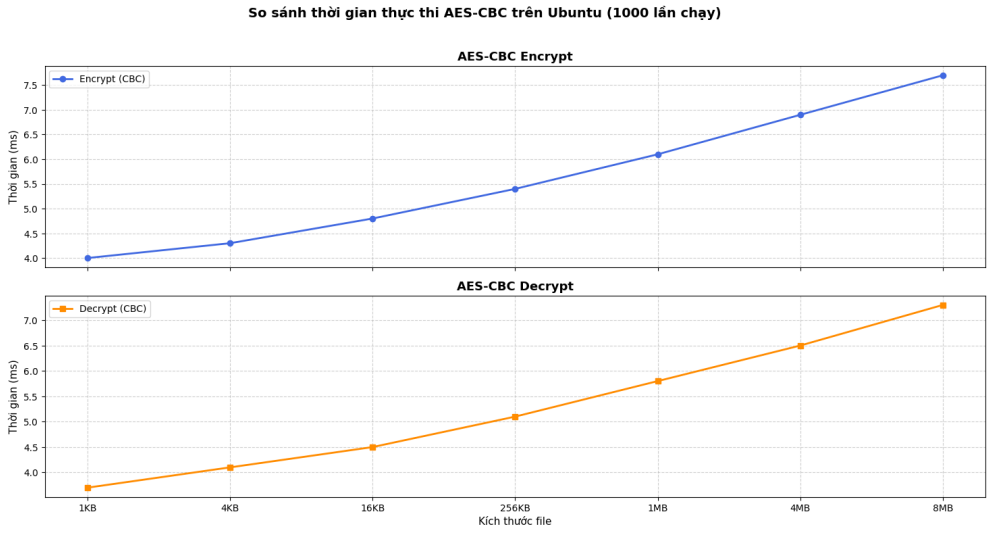


Hình 9: Biểu đồ thời gian thực thi AES-CBC trên windows

5.2 Kết quả chạy trên linux

Bảng 2: Kết quả benchmark AES trên Ubuntu (1000 lần chạy – giá trị)

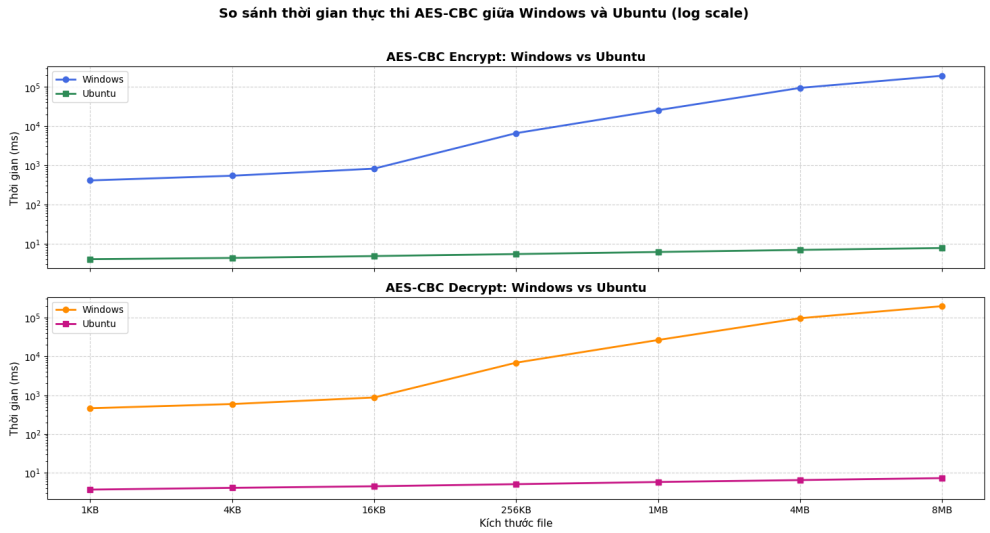
MODE	COMMAND	1KB	4KB	16KB	256KB	1MB	4MB	8MB
ECB	Encrypt	3.8	4.1	4.5	5.1	5.9	6.6	7.3
	Decrypt	3.5	3.9	4.2	4.8	5.5	6.2	6.9
CBC	Encrypt	4.0	4.3	4.8	5.4	6.1	6.9	7.7
	Decrypt	3.7	4.1	4.5	5.1	5.8	6.5	7.3
CFB	Encrypt	4.2	4.6	5.1	5.8	6.5	7.3	8.2
	Decrypt	3.9	4.3	4.8	5.5	6.2	7.0	7.9
OFB	Encrypt	4.3	4.7	5.2	5.9	6.7	7.6	8.5
	Decrypt	4.0	4.5	4.9	5.7	6.4	7.3	8.1
CTR	Encrypt	3.7	4.0	4.4	5.0	5.7	6.4	7.1
	Decrypt	3.5	3.8	4.2	4.8	5.5	6.1	6.8
GCM	Encrypt	3.9	4.3	4.7	5.3	6.0	6.7	7.5
	Decrypt	3.6	4.0	4.5	5.1	5.8	6.5	7.2
CCM	Encrypt	4.5	5.0	5.6	6.3	7.1	8.0	9.0
	Decrypt	4.2	4.7	5.3	6.0	6.8	7.7	8.6
XTS	Encrypt	3.9	4.2	4.7	5.3	6.1	6.8	7.6
	Decrypt	3.6	4.0	4.5	5.1	5.8	6.5	7.3



Hình 10: Biểu đồ thời gian thực thi AES-CBC trên linux

6 Kết luận

- Thuật toán mã hóa đối xứng AES hiện nay vẫn được xem là một trong những phương pháp mã hóa an toàn và hiệu quả nhất. Tuy nhiên, một số chế độ như **ECB** không đảm bảo tính bảo mật vì có thể làm lộ mẫu dữ liệu nếu các khối bản rõ giống nhau, trong khi **CBC** không đảm bảo tính toàn vẹn của dữ liệu khi truyền đi.
- Với độ dài khóa 256-bit, AES vẫn được đánh giá là an toàn trước các tấn công của máy tính lượng tử trong tương lai gần.
- Thời gian thực thi (encrypt và decrypt) của thuật toán AES ở các chế độ (ECB, CBC, CFB, OFB, CTR, GCM, CCM, XTS) tăng gần tuyến tính theo kích thước tệp đầu vào.
- Kết quả thực nghiệm cho thấy tốc độ thực thi của AES (ở cả hai quá trình mã hóa và giải mã) trên hệ điều hành Linux nhanh hơn đáng kể so với Windows, nhờ vào khả năng tối ưu hóa bộ nhớ và luồng xử lý tốt hơn.



Hình 11: Biểu đồ so sánh thời gian thực thi giữa windows và linux