

VIETNAM NATIONAL UNIVERSITY, HO CHI MINH CITY UNIVERSITY OF  
INFORMATION TECHNOLOGY FACULTY OF COMPUTER NETWORKS AND  
COMMUNICATION



**OFF-CLASS REPORT**

<b>LAB 1</b>
--------------

**Instructor:** PhD. Nguyễn Ngọc Tụ

**Student:** 22521050 – Nguyễn Đặng Quỳnh Như


*Chi tiết các thống kê trong báo cáo xem ở: [task1-2.xlsx](#)*

**1. Hardware resources.**

**a. Windows**

Device specifications		Copy	^
Device name	Warrence		
Processor	11th Gen Intel(R) Core(TM) i5-11400H @ 2.70GHz 2.69 GHz		
Installed RAM	8.00 GB (7.78 GB usable)		
Device ID	04F65534-42EE-48F1-9802-55357BAD4FC7		
Product ID	00356-24559-18106-AAOEM		
System type	64-bit operating system, x64-based processor		
Pen and touch	No pen or touch input is available for this display		

## b. Linux (ubuntu)



# Ubuntu

Device Namewarrence-Nitro-AN515-57

Hardware Model	Acer Nitro AN515-57
Memory	8.0 GiB
Processor	11th Gen Intel® Core™ i5-11400H @ 2.70GHz × 12
Graphics	NV177 / Mesa Intel® UHD Graphics (TGL GT1)
Disk Capacity	512.1 GB

OS Name	Ubuntu 22.04.4 LTS
OS Type	64-bit
GNOME Version	42.9
Windowing System	Wayland
Software Updates	

## 2. Giới thiệu.

Bài báo cáo task 1 bao gồm việc triển khai mã nguồn để thực hiện thuật toán DES và AES bằng ngôn ngữ C++, sử dụng thư viện CryptoPP để hỗ trợ mã hóa và giải mã.

### 3. Thống kê và biểu đồ.

#### a. Thống kê thời gian.

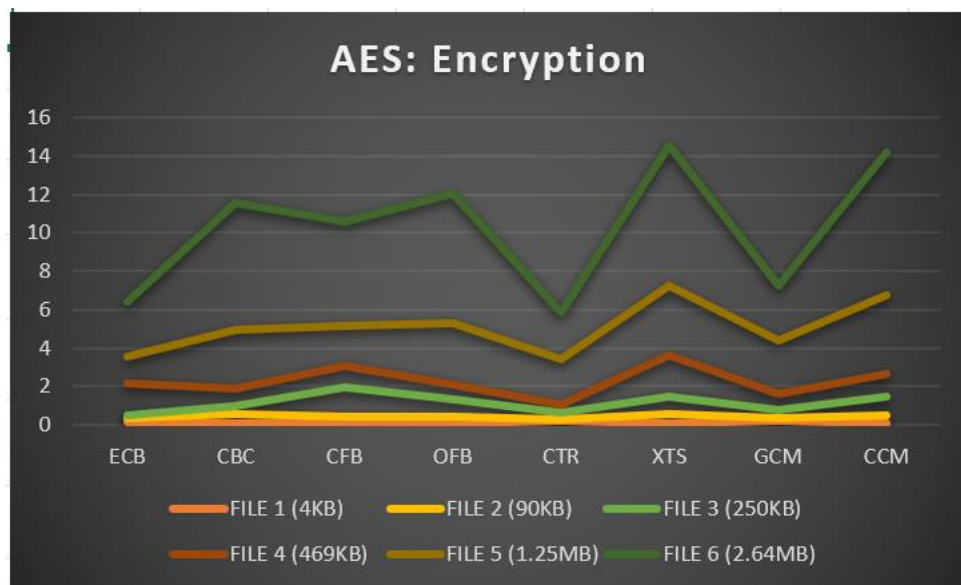
Tiến hành encrypt/decrypt 6 file input với 8 mode.

Chi tiết thống kê: Windows:

#### 3.1 AES

##### Encryption Runtime Estimates (ms)

File Size	ECB	CBC	CFB	OFB	CTR	XTS	GCM	CCM
<b>FILE 1 (4KB)</b>	0.154	0.082	0.116	0.110	0.201	0.108	0.188	0.099
<b>FILE 2 (90KB)</b>	0.344	0.574	0.437	0.446	0.298	0.569	0.361	0.522
<b>FILE 3 (250KB)</b>	0.521	0.994	1.956	1.308	0.622	1.455	0.775	1.449
<b>FILE 4 (469KB)</b>	2.186	1.856	3.062	2.118	1.064	3.595	1.609	2.675
<b>FILE 5 (1.25MB)</b>	3.538	4.971	5.142	5.298	3.387	7.273	4.379	6.729
<b>FILE 6 (2.64MB)</b>	6.419	11.579	10.553	12.061	5.875	14.525	7.273	14.174

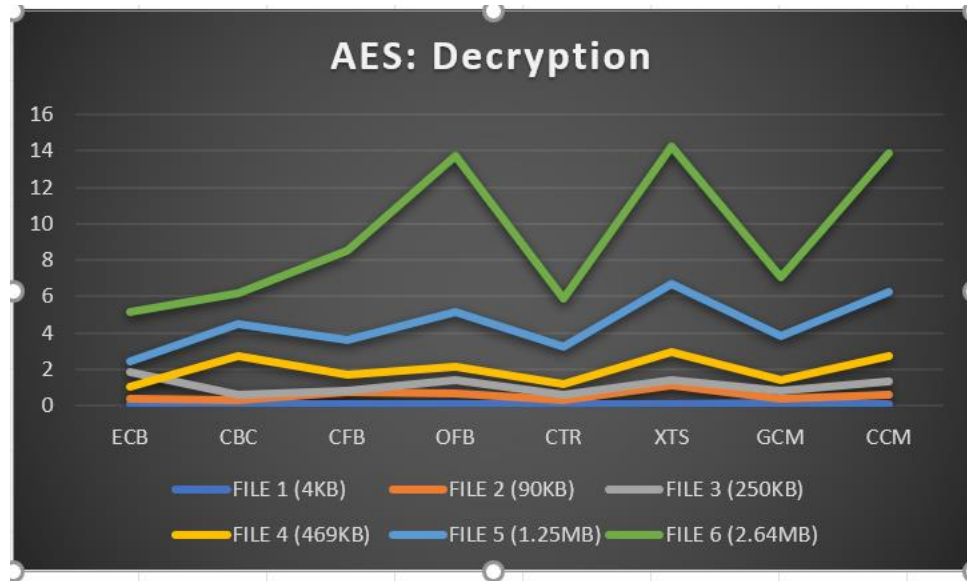


##### Decryption Runtime Estimates (ms):

File Size	ECB	CBC	CFB	OFB	CTR	XTS	GCM	CCM
<b>FILE 1 (4KB)</b>	0.085	0.071	0.071	0.092	0.082	0.093	0.143	0.116
<b>FILE 2 (90KB)</b>	0.360	0.305	0.759	0.633	0.284	1.085	0.398	0.594



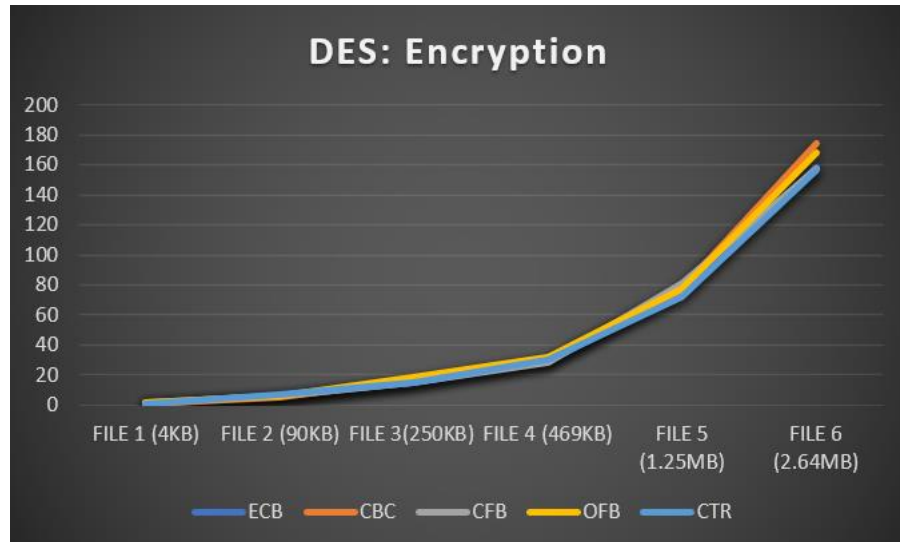
<b>FILE 3(250KB)</b>	1.868	0.620	0.822	1.426	0.603	1.415	0.805	1.317
<b>FILE 4 (469KB)</b>	1.034	2.690	1.694	2.132	1.169	2.965	1.424	2.728
<b>FILE 5 (1.25MB)</b>	2.399	4.455	3.582	5.176	3.215	6.716	3.792	6.264
<b>FILE 6 (2.64MB)</b>	5.125	6.164	8.490	13.696	5.871	14.231	7.083	13.868



### 3.2 DES

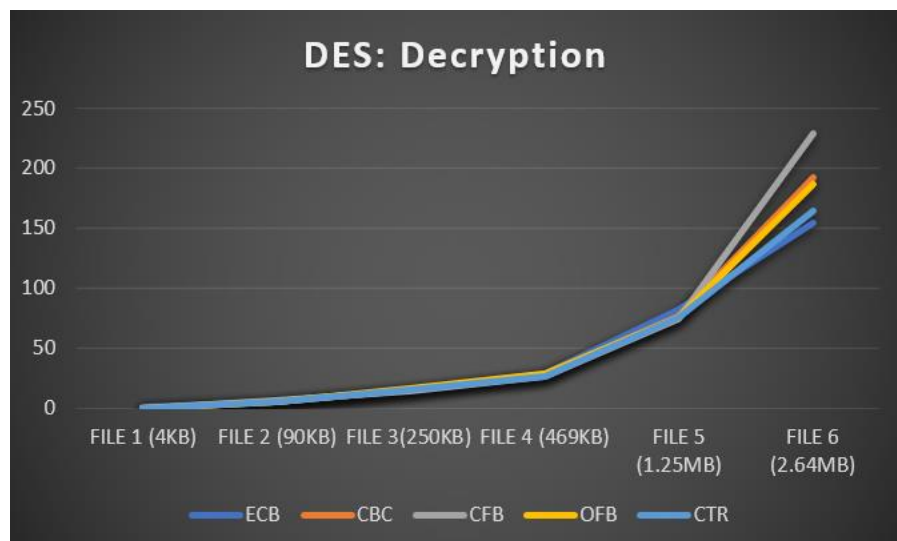
#### Estimated DES Encryption Runtime (ms)

File Size	ECB	CBC	CFB	OFB	CTR
<b>FILE 1 (4KB)</b>	0.504	0.643	1.225	1.579	0.409
<b>FILE 2 (90KB)</b>	6.334	5.435	5.679	6.369	6.901
<b>FILE 3(250KB)</b>	14.701	16.793	15.403	18.910	14.968
<b>FILE 4 (469KB)</b>	29.441	29.791	28.726	31.861	29.808
<b>FILE 5 (1.25MB)</b>	74.425	77.162	80.938	76.910	72.269
<b>FILE 6 (2.64MB)</b>	157.996	174.047	157.644	167.933	156.224



**Estimated DES Decryption Runtime (ms):**

File Size	ECB	CBC	CFB	OFB	CTR
FILE 1 (4KB)	0.417	0.245	0.258	0.285	0.269
FILE 2 (90KB)	5.922	5.372	6.050	5.881	5.114
FILE 3 (250KB)	15.598	15.111	14.683	16.107	15.671
FILE 4 (469KB)	29.275	27.183	27.100	29.068	27.000
FILE 5 (1.25MB)	82.713	77.104	73.875	75.771	75.365
FILE 6 (2.64MB)	154.129	192.754	229.695	186.755	164.059

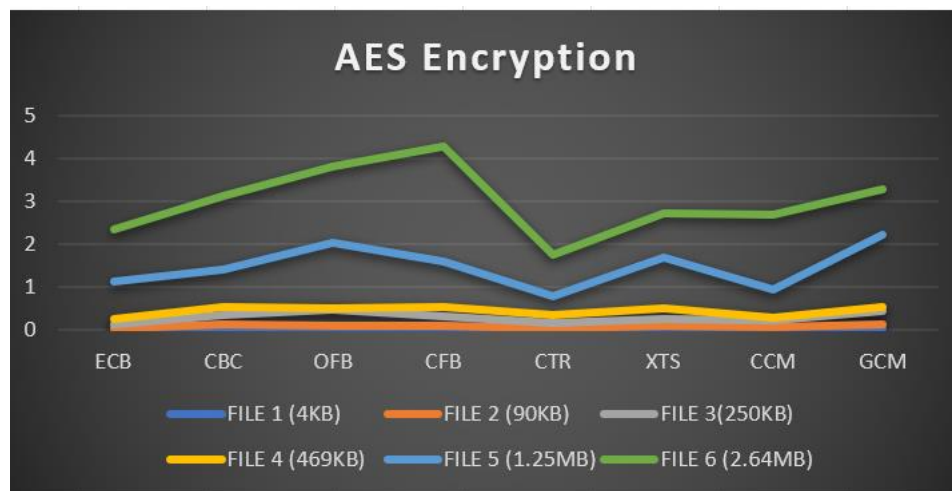


## Chi tiết thông kê: Linux:

### 1. AES

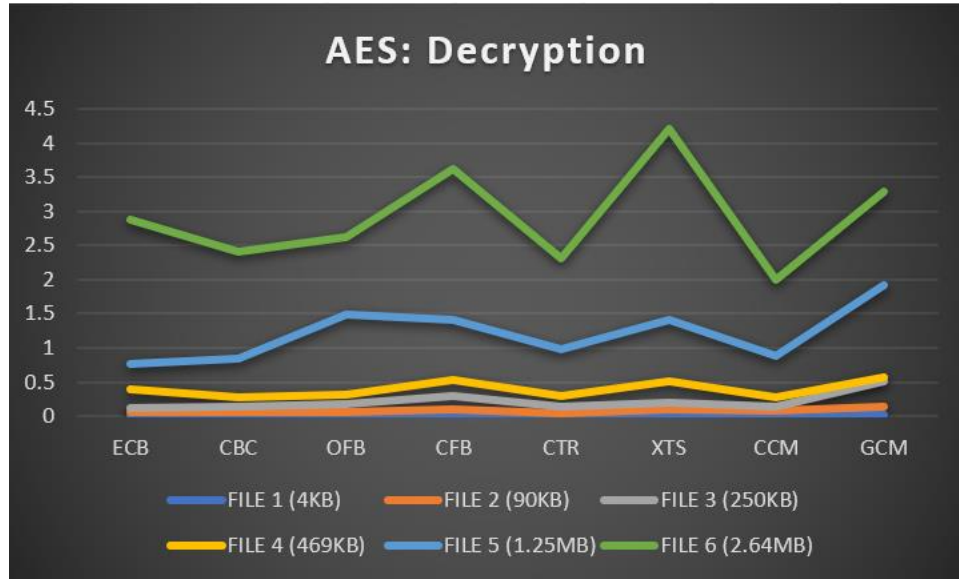
#### Encryption Runtime Estimates:

File Size	ECB	CBC	OFB	CFB	CTR	XTS	CCM	GCM
FILE 1 (4KB)	0.022	0.017	0.023	0.018	0.022	0.022	0.033	0.022
FILE 2 (90KB)	0.045	0.122	0.112	0.100	0.048	0.094	0.056	0.128
FILE 3(250KB)	0.139	0.335	0.473	0.321	0.150	0.254	0.219	0.435
FILE 4 (469KB)	0.261	0.536	0.489	0.548	0.345	0.518	0.293	0.543
FILE 5 (1.25MB)	1.135	1.407	2.037	1.588	0.797	1.682	0.927	2.235
FILE 6 (2.64MB)	2.348	3.112	3.829	4.292	1.748	2.734	2.682	3.270



#### Decryption Runtime Estimates:

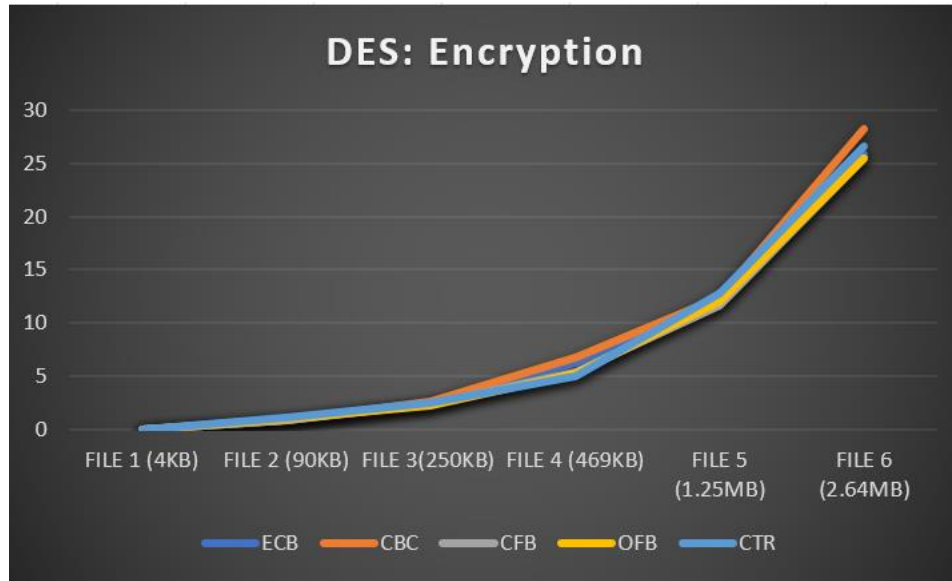
File Size	ECB	CBC	OFB	CFB	CTR	XTS	CCM	GCM
FILE 1 (4KB)	0.015	0.019	0.022	0.023	0.024	0.019	0.025	0.019
FILE 2 (90KB)	0.059	0.070	0.060	0.099	0.045	0.105	0.072	0.131
FILE 3(250KB)	0.123	0.137	0.174	0.298	0.141	0.205	0.143	0.509
FILE 4 (469KB)	0.391	0.282	0.306	0.533	0.292	0.511	0.283	0.566
FILE 5 (1.25MB)	0.768	0.837	1.488	1.419	0.971	1.408	0.879	1.922
FILE 6 (2.64MB)	2.883	2.414	2.614	3.623	2.312	4.212	2.002	3.288



## 2. DES

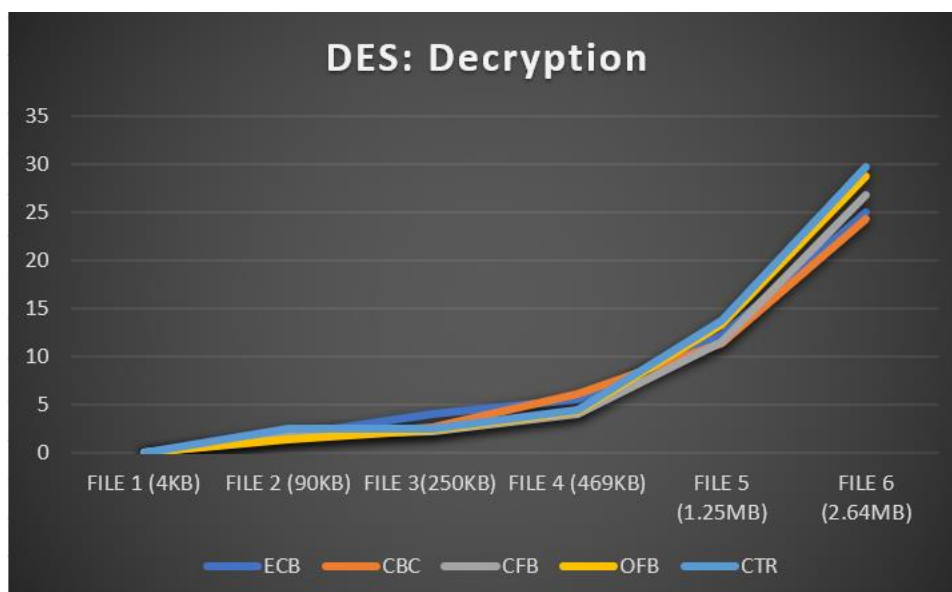
### DES Encryption Runtime Estimates:

File Size	ECB	CBC	CFB	OFB	CTR
<b>FILE 1 (4KB)</b>	0.042	0.038	0.031	0.038	0.033
<b>FILE 2 (90KB)</b>	0.821	0.901	0.824	0.939	1.097
<b>FILE 3(250KB)</b>	2.548	2.608	2.341	2.221	2.443
<b>FILE 4 (469KB)</b>	6.319	6.732	5.341	5.301	5.002
<b>FILE 5 (1.25MB)</b>	11.785	12.384	11.725	12.072	12.848
<b>FILE 6 (2.64MB)</b>	25.864	28.296	25.448	25.490	26.649



### DES Decryption Runtime Estimates:

File Size	ECB	CBC	CFB	OFB	CTR
FILE 1 (4KB)	0.032	0.022	0.023	0.028	0.024
FILE 2 (90KB)	1.745	1.492	1.729	1.402	2.454
FILE 3 (250KB)	4.011	2.607	2.237	2.359	2.435
FILE 4 (469KB)	5.526	6.068	4.068	4.296	4.432
FILE 5 (1.25MB)	12.215	11.356	11.492	13.311	13.777
FILE 6 (2.64MB)	24.955	24.295	26.766	28.768	29.739





### 3. So sánh và phân tích

- ở AES trong windows, CTR có độ mã hóa, giải mã nhanh nhất trong các mode vì chế độ CTR có khả năng song song hóa cao. Không giống như các chế độ khác như CBC (Cipher Block Chaining), nơi mỗi khối phụ thuộc vào khối trước đó, trong chế độ CTR, mỗi khối có thể được mã hóa độc lập. Điều này cho phép nhiều khối được xử lý đồng thời, tận dụng tối đa bộ vi xử lý đa lõi. ECB cũng có thời gian mã hóa, giải mã tương tự CTR
- Ở AES trong windows, XTS VÀ CCM có thời gian mã hóa, giải mã chậm nhất trong các mode. Tuy nhiên ở linux, CFB có thời gian mã hóa lâu nhất và XTS có thời gian giải mã chậm nhất
- AES ở linux chạy nhanh hơn đáng kể so với windows, dễ thấy nhất là ở file 6 (2.64MB). Trong khi ở linux file 6, ở tất cả các mode runtime chưa tới 5 ms, thì file 6 ở windows chạy đến gần 15 ms. Điều này có thể do Linux quản lý tài nguyên và tối ưu hệ thống tốt hơn.
- DES ở windows, thời gian mã hóa và giải mã với các modes ở khoảng 230ms, trong khi ở linux chỉ có khoảng 30ms

Kết quả này cho thấy Linux có hiệu suất mã hóa tốt hơn so với Windows. Việc lựa chọn hệ điều hành và chế độ mã hóa phù hợp là quan trọng để đạt hiệu suất tối ưu trong các ứng dụng yêu cầu mã hóa nhanh chóng