BÁO CÁO BÀI TẬP

**Môn học: Mật mã học**

**Kỳ báo cáo: Buổi 02 (Session 02)**

**Tên chủ đề: AES**

*Ngày báo cáo: 28/03/2023*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT219.N22.ATCL

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Nguyễn Trần Anh Đức | 21521964 | 21521964@gm.uit.edu.vn |
| 2 | Nguyễn Hữu Tiến | 21590479 | 21590479@gm.uit.edu.vn |
| 3 | Lê Thanh Duẩn | 19521370 | 19521370@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** | **Người đóng góp** |
| 1 | Chậm lại và suy nghĩ 1 | 100% | Hữu Tiến |
| 2 | Chậm lại và suy nghĩ 2 | 100% | Hữu Tiến |
| 3 | AES vs DES Encryption Benchmark | 100% | Thanh Duẩn |
| 4 | AES vs DES Decryption Benchmark | 100% | Thanh Duẩn |
| 5 | Plaintext support UTF 16 | 100% | Anh Đức |
| 6 | Plaintext manual input | 100% | Anh Đức |
| 7 | Secret Key and IV manual input | 100% | Anh Đức |
| 8 | Use AES with all modes | 100% | Anh Đức |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

**1. AES::DEFAULT\_KEYLENGTH and AES::BLOCKSIZE**

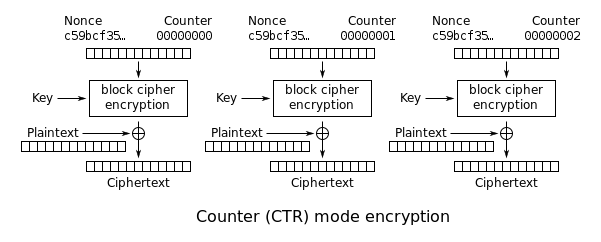
Key length : 16 byte

Block size : 16 byte

**2. CTR Mode :**

The Counter (CTR) mode is a typical block cipher mode of operation using block cipher algorithm. CTR introduces 2 additional input to increase the randomness for ciphertext:

* nonce : random bit and no need to be secret
* counter : the index of the block in the plaintext



The formula for CTR Encryption is :

CTR Mode turn block cipher into stream cipher by generating the next keystream block by encrypting successive values of a counter. Counter can be any function that produces a sequence which is not repetitive.

**3. Bài tập :**

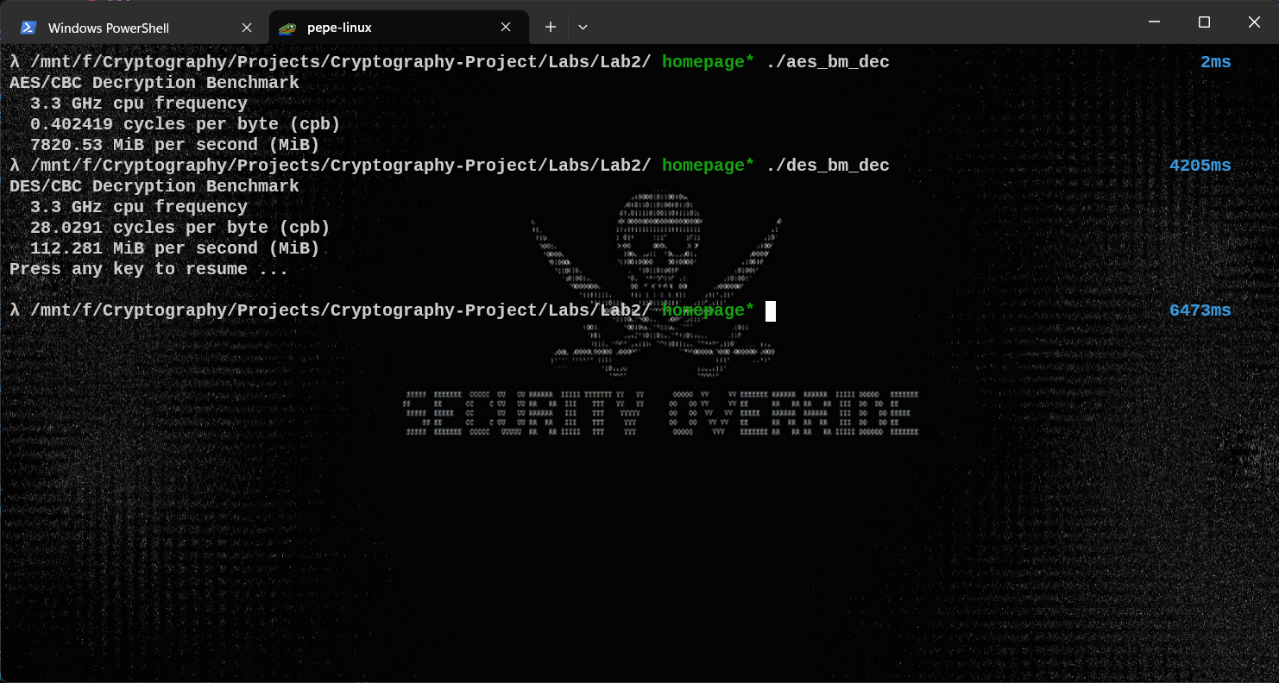
1. **Text

   Description automatically generatedAES vs DES CBC Mode encryption performance comparison:**

|  |  |  |  |
| --- | --- | --- | --- |
| Algorithm | Execution time | Cycles per byte | MiB per second |
| AES CBC | 6214ms | 1.79023 | 1757.94 |
| DES CBC | 9020ms | 30.4878 | 103.226 |

As we can see, AES is much more faster than DES.

1. **AES vs DES CBC Mode decryption performance comparison:**

****

|  |  |  |  |
| --- | --- | --- | --- |
| Algorithm | Execution time | Cycles per byte | MiB per second |
| AES CBC | 4205ms | 0.402419 | 7820.53 |
| DES CBC | 6473 | 28.0291 | 112.281 |

AES decryption process is signficantly faster than DES.

1. **Plaintext support UTF16, manual input Key , IV and plaintext from user**

Text

Description automatically generated

1. **Use AES with all modes**

**Text

Description automatically generated**Script is attached to report.

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)