BÁO CÁO THỰC HÀNH

**Môn học: CRYPTOGRAPHY – Mật mã học**

**Tên chủ đề: BÀI THI THỰC HÀNH**

*GVHD: Tô Trọng Nghĩa*

1. **THÔNG TIN CHUNG:**

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

Lớp: **NT219.N21.ANTT.1**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và tên | MSSV | Email |
| 1 | Lê Đoàn Trà My | 21521149 | 21521149@gm.uit.edu.vn |

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

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Nội dung | Tình trạng | Trang |
| 1 | Thuật toán mã hoá DES | 100% | 2 |
| 2 | Thuật toán mã hoá AES | 50% | 3 |
| 3 | Thuật toán mã hoá RSA | 100% | 3 - 5 |
| 4 | Thuật toán mã hoá Elliptic Curve | 0% | 6 |
| 5 | Hàm băm | 0% | 6 |
| Điểm tự đánh giá | | | **5** |

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

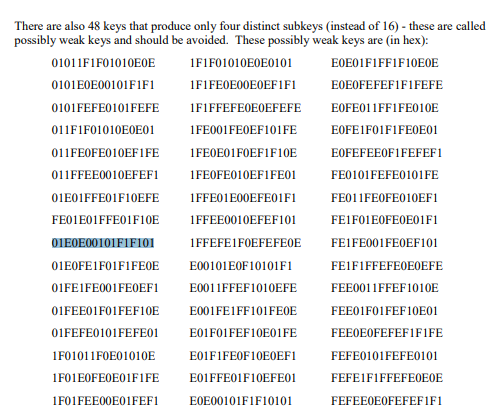
BÁO CÁO CHI TIẾT

1. **Thuật toán mã hoá DES**

**Bài tập 1: (1đ)** Đây có phải là khoá yếu trong DES không, vì sao?

01 E0 E0 01 01 F1 F1 01

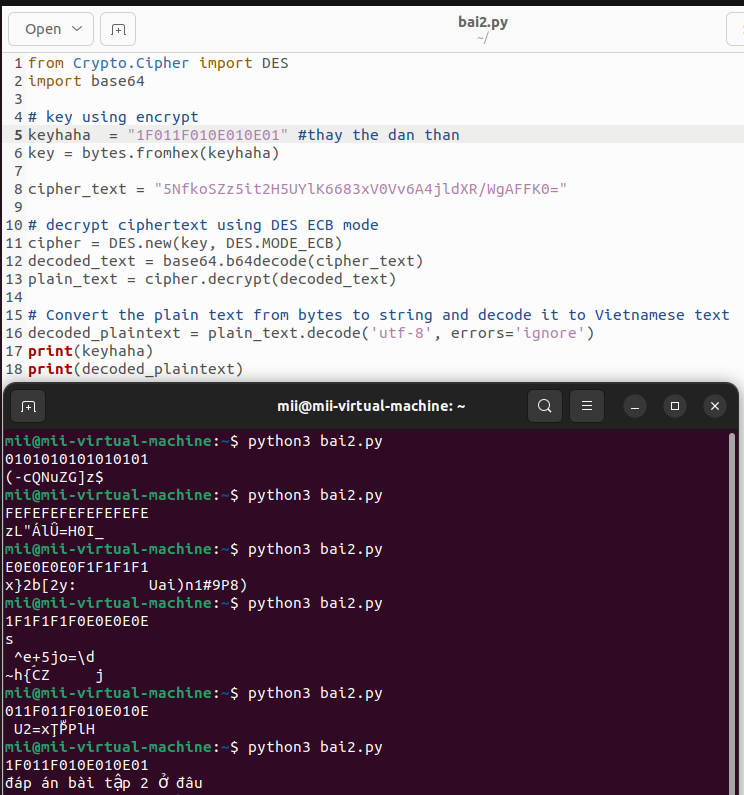
→ Trả lời: Đó là 1 khoá yếu , thay vì tạo ra 16 khoá con thì nó chỉ tạo ra 4 khoá con riêng biệt *(trong bài báo NIST, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher,* [*Special Publication 800-67*](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-67r1.pdf)*, page 14 có liệt kê các khoá có bao gồm khoá này*)



**Bài tập 2: (1đ)** Cho chương trình mã hoá DES bên dưới. Kết quả mã hoá được encode base64. Hãy tìm đoạn mã rõ ban đầu của chương trình. Biết DES mã hoá mode ECB và khoá có liên quan đến khoá yếu và khoá nửa yếu.

▪ cipher text: ***5NfkoSZz5it2H5UYlK6683xV0Vv6A4jldXR/WgAFFK0=***

→ Trả lời: Keyhaha là key em thay thế lần lượt và thử chạy với các key trong mục 3.4.2 Weak Keys ở bài báo được dẫn trong bài tập 1 ([*Special Publication 800-67*](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-67r1.pdf))



1. **Thuật toán mã hoá AES**

**Bài tập 3: (1đ)** Các trường hợp nào nên sử dụng mode CBC, và trường hợp nào nên sử dụng mode OFB trên AES. Cho ví dụ

→ Trả lời:

*- CBC:* Trong CBC, mỗi ciphertext từ khối trước đó được XOR với plaintext của khối hiện tại để trở thành đầu vào cho việc thực thi thuật toán mã hoá với khoá K → Đảm bảo tính toàn vẹn của dữ liệu vì bất kỳ thay đổi nào trong khối bản mã sẽ ảnh hưởng đến tất cả các khối tiếp theo, không thể tiến hành mã hoá song song → ***Xác thực, kiểm tra tính toàn vẹn, general-purpose block-oriented transmission (bảo mật và toàn vẹn dữ liệu đều quan trọng)***

*VD: mã hóa dữ liệu truyền qua Internet, CBC mode có thể được sử dụng để mã hóa email, tệp tin hoặc dữ liệu*

*- OFB:* Giá trị ngõ ra của khối thực thi thuật toán mã hoá (không phải ciphertext) của lần hiện tại sẽ được phản hồi đến ngõ vào của lần mã hoá kế tiếp. OFB xử lý trên một khối dữ liệu với độ dài bit đầy đủ như thuật toán mã hóa quy định chứ không xử lý trên một phần hay một vài bit của khối dữ liệu. → OFB mode không phụ thuộc vào các khối trước đó trong quá trình mã hóa (giảm thiểu tác động của nhiễu lên dữ liệu, lỗi trong một khối không ảnh hưởng khối tiếp theo), nó tạo ra một chuỗi các giá trị ngẫu nhiên (keystream) từ khóa và vector khởi tạo (IV), và sau đó sử dụng keystream này để mã hóa dữ liệu. → ***Truyền định hướng luồng qua kênh nhiễu***

*VD: Truyền qua các kênh nhiễu “ồn ào” như vệ tinh,….*

**Bài tập 4: (2đ)** Cho chương trình mã hoá AES bên dưới. Kết quả mã hoá sử dụng AES mode CBC để mã hoá và sử dụng AES mode ECB để giải mã dựa trên cipher của kết quả mã hoá. Hãy tìm ra đoạn mã rõ ban đầu của chương trình

→ Trả lời:

1. **Thuật toán mã hoá RSA**

**Bài tập 5: (1đ)** Các tham số của public key rsa lần lượt là

▪ e = 6131

▪ n = 10050256277

▪ và ciphertext là 283818407. Hãy tìm lại plaintext ban đầu (ascii). Biết được sau khi mã hoá thêm 1.373.904 lần thì trả lại về kết quả ciphertext 283818407

→ Trả lời:

- Dùng web phân tích n thành tích của 2 số

A screenshot of a computer

Description automatically generated with medium confidence

* Code tính toán tìm flag:

A screenshot of a computer

Description automatically generated

**Bài tập 6: (1đ)** Luyện tập sử dụng RSA với các thông số sau.

▪ Cho N = 578964038403140519872617596733373013666837348169986499204804887 912050378797057695450164018920672745013327547877357092402264601 791345337465611242355171794982951716973311299951268998658630886 339168976856089089879769145078751899048798731997304844829150257 298564573291382656379596401320937889452260564007995242081364864 848132224946702038942698014131530003532769650377734846952516919 116833367491090964761746396895436643171553698164847132256962107 185548977422169817682724411399093713027079573229284842238341024 579335703501691630628449177876328000762436751982386192048748672 577415428756047755050862167352986417326172975758394547185977077 837703929212566806914606819955828372100844345241201164020005851 190153924995788879026250522783939917230773433545466595478867504 920334606546053871869606990229300178395635250354139064211213888 554500675947444101309374037824356224248890282379393782826013313 190632998965514414645159968259532467970224128507462281685494151 668615273495326153093288830897734893232841005421742712406205522 047931835539004055715057632809766161945617915283896442696492778 905485523834949526582988091185972959767326839566052511497483260 863358967110960410160681643249257608396267110763302521503890712 345470239566641296507088535273005677

▪ e = 3

▪ c = 16626984637532017615929028667531146333866135439766441517498 03233991141071198998720881599384967514228675702471322080743 3195460421921875000

▪ Tìm plaintext ban đầu của chương trình

→ Trả lời:

*Ta có:* \* Mã hoá văn bản gốc M:

- Để bảo mật: C = E(M, PU) = Me mod n; Để xác thực: C = E(M, PR) = Md mod n

\* Giải mã bản mã C:

- Để bảo mật: M = D(M, PR) = Cd mod n; Để xác thực: M = D(M, PU) = Ce mod n

Nhận thấy, trong đề bài có: e = 3 rất nhỏ so với n (rất rất lớn) nên khi 1 số mode cho n sẽ bằng chính nó → có thể C = Me

*A screenshot of a computer

Description automatically generated*

1. **Thuật toán mã hoá Elliptic Curve**

**Bài tập 7:(2đ)** Cho chương trình mã hoá chữ ký bằng ECC. Hãy viết một chương trình xác thực chữ ký với các tập tin hình ảnh được cung cấp. Kiểm tra signature đính kèm nào là đúng với tập tin ban đầu.( có 10 signature cần kiểm tra)

▪ ECDSA <ECP, SHA256>

→ Trả lời:

1. **Hàm băm**

**Bài tập 8:(1đ)** Luyện tập về hàm băm.

▪ Tìm giá trị xung đột băm (hash collision) của chương trình trong baitap\_8.py

→ Trả lời:

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