Đại học Quốc gia thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin

5

Lab

Ôn tập

Thực hành môn Mật mã học

Tháng 3/2023

Lưu hành nội bộ

<Nghiêm cấm đăng tải trên internet dưới mọi hình thức>

Mọi góp ý về tài liệu, vui lòng gửi về email inseclab@uit.edu.vn

BEE SECURE
INSECLAB

A. TỔNG QUAN

1. Mục tiêu

- Ôn tập lại các thuật toán và mô hình mật mã học đã thực hành.
- Tìm hiểu, xây dựng lại các mô hình mật mã học
- Ôn tập lại các cuộc tấn công trên các thuật toán này

2. Thời gian thực hành

- Thực hành tại lớp: 5 tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành: tối đa 13 ngày.

B. CHUẨN BỊ MÔI TRƯỜNG

1. Phần mềm visual studio code

2. Hệ điều hành

- Sử dụng cả hệ điều hành linux và window để kiểm tra thuật toán.

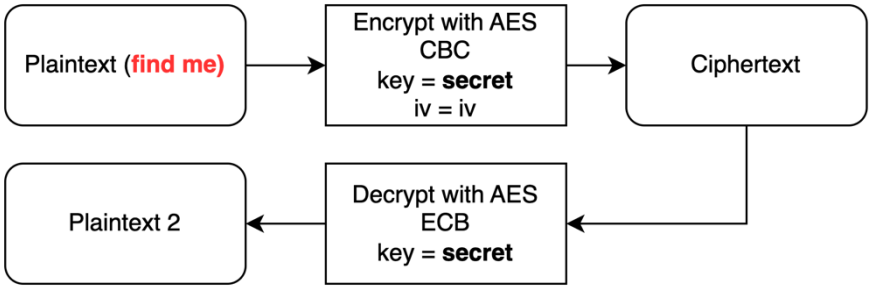
C. CÂU HỎI ÔN TẬP

1. Thuật toán mã hoá DES

- **Bài tập 1: (1đ)** Khoá yếu và nửa yếu trên **DES** là gì, các trường hợp nào có thể xảy ra khoá yếu trên **DES**.
- **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.
- **iv**: VyUR14UQP/0=
- **cipher text:** jtEl85W3Riqjk56bj+7J5YcYhHvzHc6d
- *Kết quả chương trình 50%*
- *Giải thích chi tiết: 50%*

2. Thuật toán mã hoá AES

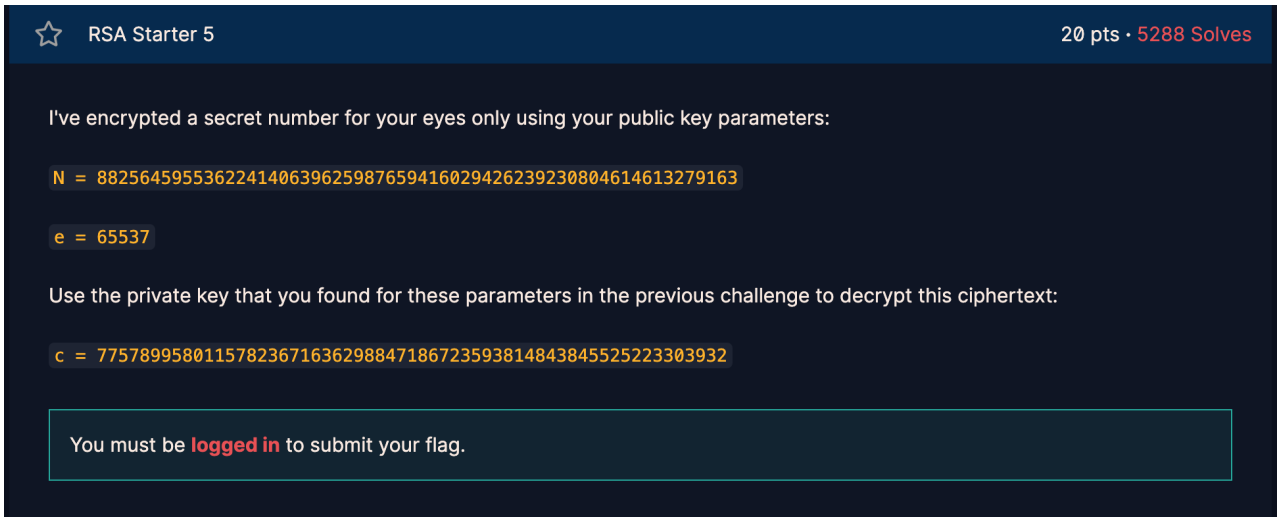
- **Bài tập 3: (1đ)** So sánh sự khác nhau giữa các mode trên AES
- **Bài tập 4: (2đ)** Cho chương trình mã hoá AES bên dưới. Kết quả mã hoá sử dụng AES mode CBC để mã hoá và sử dụng AES mode ECB để giải mã dựa trên cipher của kết quả mã hoá. Hãy tìm ra đoạn mã rõ ban đầu của chương trình



- Cipher text mã hoá bằng **AES_CBC**:
  cipher = MeNQurBA3QKVfCYO34Pbi/ENnjx23hSb0qXkAwbnmWw=
  iv = dkdxdo+eifES0inl0zW/ew==
- Mã rõ giải mã bằng **AES_ECB** (cùng key): decrypt(cipher)
  plaintext 2 = BCIHH+rpqbBXgQnI/hifA16RcM3ZNLUi0D9kC9qG3o4=
- *Kết quả chương trình 50%*
- *Giải thích chi tiết: 50%*

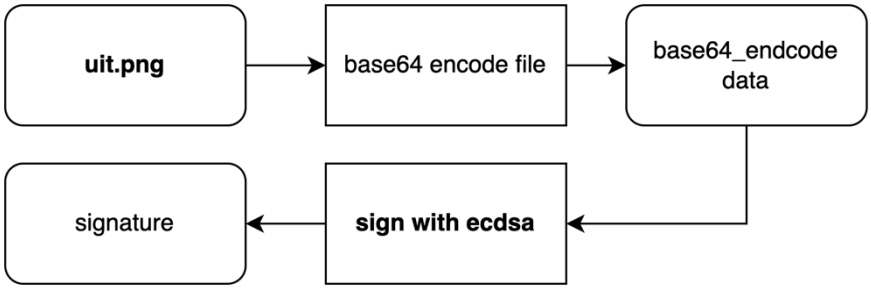
3. Thuật toán mã hoá RSA

- **Bài tập 5: (1đ)** Trong việc sử dụng thuật toán RSA, nếu một số lượng nhỏ các lần mã hóa lặp lại cho kết quả trả về là mã rõ, nguyên nhân có thể là gì.
- **Bài tập 6: (1đ)** Luyện tập sử dụng RSA với các thông số sau.
- Tham khảo challenge tại: https://cryptohack.org/challenges/rsa/
- Kết quả chương trình 50%
- Giải thích chi tiết: 50%



4. Thuật toán mã hoá Elliptic Curve

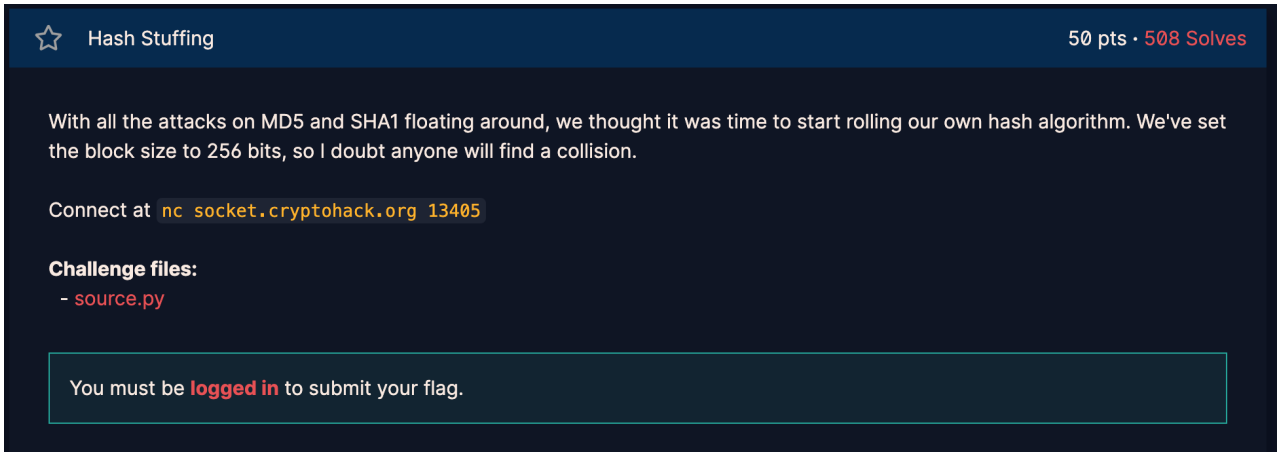
- **Bài tập 7:(2đ)** Cho chương trình mã hoá chữ ký bằng ECC. Hãy viết một chương trình xác thực chữ ký với các signature dưới đây. Kiểm tra signature nào là đúng với tập tin ban đầu.(có 10 signature cần kiểm tra)



- Kết quả chương trình 50%
- Giải thích chi tiết: 50%

5. Hàm băm

- **Bài tập 8:**(1đ) Luyện tập về hàm băm.
- Tham khảo: https://cryptohack.org/challenges/hashes/
- Kết quả chương trình 50%
- Giải thích chi tiết: 50%



D. YÊU CẦU & ĐÁNH GIÁ

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện theo nhóm đã đăng ký.
- Nộp báo cáo kết quả gồm Code, CSDL được export và chi tiết những việc (Report) mà nhóm đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Báo cáo:
  - File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
  - Đặt tên theo định dạng: [Mã lớp]-LabX_MSSV1.
  - Ví dụ: [NT219.K11.ANTN.1]-Lab1_1852xxxx-.
  - Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
  - Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT

Chúc các bạn hoàn thành tốt!