BÁO CÁO THỰC HÀNH

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

**Tên chủ đề: CRYPTOHACK**

*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 | Introduction | 3 bài | 2 - 3 |
| 2 | General | 4 bài | 4 |
| 3 | RSA | 3 bài | 5 - 7 |
| 4 | Symmetric ciphers | 2 bài | 7 - 8 |
| 5 | Mathematics | 2 bài | 8 - 9 |
| Điểm tự đánh giá | | |  |

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

BÁO CÁO CHI TIẾT

1. **Introduction**1.1. Finding flags:

Đây là bài khởi đầu, theo hướng dẫn chỉ cần copy dán  vào ô kết quả.

A screenshot of a computer

Description automatically generated with medium confidence

* 1. Great Snakes:

Chạy file great\_snakes.py được cung cấp trên trang web để thu được flag:

A screenshot of a computer

Description automatically generated with medium confidence

Kết quả thu được:

A screenshot of a computer

Description automatically generated

* 1. Network Attacks:

Sửa từ clothes trong code cũ thành flag theo yêu cầu của đề bài và tiến hành thực thi file, thu được flag:

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated with medium confidence**

1. **GENERAL**
   1. ASCII

- Sử dụng chr() trong python để chạy và lấy flag

**A screenshot of a computer

Description automatically generated**

* 1. Hex

**A screenshot of a computer

Description automatically generated**

* 1. Base64

**A screenshot of a computer program

Description automatically generated with low confidence**

* 1. Bytes and Integer

**A screenshot of a computer

Description automatically generated**

1. **RSA**

3.1. Inferius Prime

- Dùng web phân tích n thành tích của 2 số

A screenshot of a computer

Description automatically generated with medium confidence

A screen shot of a computer

Description automatically generated with medium confidence

3.2. Monoprime

- Kết quả kiểm tra số n là 1 số nguyên tố, phi = n -1

A screenshot of a computer

Description automatically generated with low confidence- Code tương tự câu trên

A screenshot of a computer

Description automatically generated with medium confidence

3.3. Square eyes

- Kết quả kiểm tra n = bình phương của một số

A screenshot of a computer

Description automatically generated

**A screenshot of a computer

Description automatically generated with medium confidence**

1. **SYMMETRIC CIPHERS**

4.1. Structure of AES

**A screenshot of a computer program

Description automatically generated with medium confidence**

4.2. Round Keys

**A screenshot of a computer program

Description automatically generated with medium confidence**

- Kết quả (bỏ các dấu [] ‘’ , đi ta sẽ được flag): crypto{r0undk3y}

1. **MATHEMATICS**

5.1. Vector

- Dùng sagemath để tính toán

**A picture containing text, screenshot, font, line

Description automatically generated**

- Kết quả bằng = 9

5.2. What’s a Lattice?

- Sử dụng web matrixcalc.org để tính toán định thức det

**A screenshot of a computer

Description automatically generated**

* Kết quả: 255

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