

**TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

**------------------------------------------------**

**KỲ THI KẾT THÚC HỌC PHẦN**

**NĂM HỌC 2021-2022**

**Bài tập lớn môn An toàn và bảo mật hệ thống thông tin**

**Đề số : 05**

|  |  |  |
| --- | --- | --- |
| **Giảng viên hướng dẫn** | **:** | **Nguyễn Văn Hách** |
| **Sinh viên thực hiện** | **:** | Nguyễn Tấn Phát |
| **Mã sinh viên** | **:** | 1911061044 |
| **Lớp** | **:** | ĐH9C5 |
| **Tên học phần** | **: An toàn và bảo mật hệ thống thông tin** | |
| **Khóa học** | **:** | **2019 – 2023** |

***Hà Nội – 2021***

# **LỜI MỞ ĐẦU**

Từ trước công nguyên con người đã phải quan tâm tới việc làm thế nào để đảm bảo an toàn bí mật cho các tài liệu, văn bản quan trọng, đặc biệt là trong lĩnh vực quân sự, ngoại giao. Ngày nay với sự xuất hiện của máy tính, các tài liệu văn bản giấy tờ và các thông tin quan trọng đề được số hóa và xử lý trên máy tính, được truyền đi trong một môi trường mà mặc định là không an toàn. Do đó yêu cầu về việc có một cơ chế, giải pháp để bảo vệ sự an toàn và bí mật của các thông tin nhạy cảm, quan trọng ngày càng trở nên cấp thiết. Mật mã học chính là ngành khoa học đảm bảo cho mục đích này. Khó có thể thấy một ứng dụng Tin học có ích nào lại không sử dụng các thuật toán mã hóa thông tin.

# **CHƯƠNG 1: GIỚI THIỆU.**

1. **Các khái niệm về mật mã.**

* Mật mã là quá trình chuyển đổi các thông tin thông thường thành dạng không đọc trực tiếp được và được gọi là bản mã.
* Giải mật mã là quá trình phục hồi lại văn bản thường từ văn bản mã.
* Trong đó, mật mã là tên gọi chung, nó bao hàm cả quá trình Mật mã hóa và giải mã. Hoạt động của mật mã thông thường được kiểm soát bởi khóa. Khoa là một đoạn thông tin bí mật nào đó cho phép tùy biến cách thức để tạo ra văn bản mã.
* Mật mã là một ngành khoa học chuyên nghiên cứu các phương pháp truyền tin bí mật. Mật mã bao gồm: Lập mã và phá mã.
* **Lập mã**: bao gồm 2 quá trình: mã hóa và giải mã. Các sản phẩm của lĩnh vực này là các hệ mã mật, các hàm băm , các hệ chữ ký điện tử, các cơ chế phân phối, quản lý khóa và các giao thức mật mã.
* **Phá mã:** Nghiên cứu các phương pháp phá mã hoặc tạo mã giá. Sản phẩm lĩnh vực này là các phương pháp phá mã, các phương pháp giả tạo chữ ký, các phương pháp tấn công hàm băm và các giao thức mật mã.
  + Bản rõ - plaintext: Là văn bản thông thường.
  + Bản mã – Ciphertext: Là bản đã được mã hóa và không có thể đọc được.
  + Khóa – key: Dùng khóa để mã hóa và giải mã và khóa được tạo ra bởi thuật toán (Algorithm).

1. **An toàn thông tin bằng mật mã.**

* Cách hiểu truyền thống: giữ bí mật nội dung trao đổi gửi và Nhận trao đổi với nhau trong khi trung gian tìm cách “nghe lén”.
* Thông tin được an toàn, chính là quá trình biến đổi nó thành một dạng mới khó đọc hơn. Viết mật mã có liên quan đến việc mã hóa các thông báo trước khi gửi chúng đi và tiến hành giải mã chúng lúc nhận được.

**CHƯƠNG 2: CÁC PHƯƠNG PHÁP MÃ HÓA CỔ ĐIỂN.**

1. **Phương pháp mã hóa Caesar.**

* Là phương pháp mã hóa đơn giản và sử dụng phương pháp thay thế, do nhà khoa học Julius Caesar.
* Mật mã Caesar liên quan đến việc thay thế mỗi chữ cái trong bảng Alpha.
* Chúng ta gán mặc định các số từ 0 → 25 tương ứng mỗi kí tự trong chữ cái Alpha.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a | b | c | d | e | f | g | h | i | j | k | l | m |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

1. **Bảo mật thông tin với thuật toán Hill.**