TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN

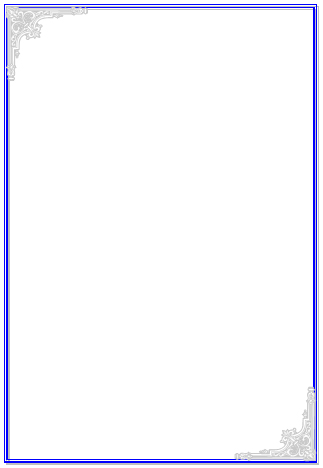
---------------o0o---------------

**AN TOÀN VÀ PHỤC HỒI DỮ LIỆU**



**BÀI TẬP PHÂN CÔNG 01.04**

SINH VIÊN THỰC HIỆN

* Bùi Đăng Tuấn Kiệt - 20127218
* Lê Nguyễn Minh Quang - 20127295

Ngày 18 Tháng 10 Năm 2023

**Đề bài**

Xây dựng chương trình mã hóa & giải mã một file

i. Key mã hóa (password) do người dùng nhập vào được hash thành 1 chuỗi tối thiểu 100bit.

Với yêu cầu này, tụi em sử dụng phương pháp băm bậc 3 (SHA-3), hay còn gọi là SHA-512, tức là sẽ băm chuỗi mật khẩu thành 512 bit

A screenshot of a computer program

Description automatically generated

Ở đây sẽ có 2 file: File để đọc mật khẩu là readpassword.txt và file ghi mật khẩu đã băm là encryptedpassword.txt. Tại câu này, chương trình sẽ đọc mật khẩu từ file và dùng nó để thực hiện quy trình băm thành chuỗi các ký tự. Thủ tục băm sử dụng thư viện hashlib.