

## **LAB 6 – HÀM BĂM**

**Author: Trần Quý Nam**

**Date: 04/4/2025**

**Bài 1.** Tham khảo mã nguồn trên links slides bài giảng để cài đặt chương trình C++ thực hiện mã hóa hàm băm MD5 và thực hiện các chức năng:

- Chương trình nhận vào chuỗi ký tự bất kỳ từ người dùng và in ra mã băm MD5 tương ứng (dưới dạng hex)
- Cho phép người dùng nhập 2 chuỗi. Tính MD5 của cả hai chuỗi. So sánh và in ra kết quả: "Giống nhau" hoặc "Khác nhau"

**Bài 2.** Sử dụng thư viện MD5 có sẵn trong thư viện OpenSSL của C++ hoặc thư viện Python trên links các slides bài giảng để cài đặt chương trình có các chức năng:

- Lưu trữ các mật khẩu dưới dạng MD5 trong file. Khi người dùng nhập mật khẩu trên giao diện hoặc command line để đăng nhập, chương trình sẽ: tính hash mật khẩu nhập vào bằng MD5. So sánh với mã lưu trong file. Thông báo đăng nhập thành công/thất bại.
- Đọc một file (ví dụ: .txt, .jpg) và tính mã MD5 của toàn bộ nội dung. Cho phép người dùng nhập mã MD5 gốc để đối chiếu. Thông báo "File đã bị thay đổi" nếu khác nhau.

**Bài 3.** Sử dụng thư viện SHA 512 (với Python dùng hashlib.sha512 và với C++ dùng thư viện OpenSSL hoặc Crypto++) để lập chương trình thực hiện các chức năng:

- Tính SHA-512 của một chuỗi đầu vào bất kỳ (chương trình nhận một chuỗi từ người dùng qua cin hoặc input). Tính SHA-512 hash và in ra dưới dạng hex.
- Nhập hai chuỗi từ người dùng. Tính SHA-512 của cả hai chuỗi. So sánh mã hash → In ra "Giống nhau" hoặc "Khác nhau".
- Đọc nội dung một file (file.txt). Tính SHA-512 hash của toàn bộ nội dung file. Cho phép người dùng nhập vào một chuỗi hash (gốc). So sánh và thông báo file đã bị thay đổi hay chưa.

-----