ĐỒ ÁN  
\* BẢO MẬT

# Công dụng chính của bcrypt:

**🔒 1. Bảo vệ mật khẩu người dùng**

* bcrypt chuyển đổi mật khẩu từ dạng dễ đọc (plaintext) → thành **chuỗi mã hóa không thể đọc được**.
* Ví dụ: "123456" → $2b$10$wNqUbc...vnKZcOeM/sZ6j.

👉 Điều này có nghĩa: nếu database bị lộ, hacker **không thể biết mật khẩu thật**.

**⏳ 2. Khó bị tấn công dò mật khẩu (Brute-force)**

* bcrypt được thiết kế để **chạy chậm có chủ ý**, nên hacker **không thể kiểm thử hàng triệu mật khẩu mỗi giây**.
* Bạn có thể chỉnh độ "tốn thời gian" bằng tham số **saltRounds** (số lần lặp, mặc định thường là 10).

**🔁 3. Mỗi lần mã hóa → kết quả khác nhau**

* Khi mã hóa "123456" 2 lần → kết quả **khác nhau hoàn toàn** nhờ **salt ngẫu nhiên**.
* Điều này làm hacker **không thể so sánh** để đoán được người dùng dùng chung mật khẩu.

# 🔐 ****Công dụng của**** encrypt ****trong bảo mật dữ liệu****

A screenshot of a computer

Description automatically generated

## ✅ ****1️⃣ Mã hoá dữ liệu trên đường truyền****

* 🔒 Khi encrypt: true, **toàn bộ dữ liệu** (query, tham số, kết quả trả về) sẽ được **mã hoá** trước khi gửi qua mạng.
* Giúp **ngăn chặn kẻ tấn công nghe lén** (sniffing) hoặc bắt gói tin (MITM — Man In The Middle Attack).

## ✅ ****2️⃣ Đảm bảo tính riêng tư****

* 👀 Nếu không mã hoá, ai bắt được gói tin có thể **đọc toàn bộ query SQL, email, token, thông tin nhạy cảm**.
* Với mã hoá, chỉ **Node.js và SQL Server** mới hiểu được nội dung.

## ✅ ****3️⃣ Bắt buộc khi dùng môi trường production (public network)****

* 🌍 Khi chạy qua Internet (VD: SQL Server không cùng máy với Node.js), **luôn phải bật mã hoá**.
* Một số dịch vụ cloud (Azure SQL, AWS RDS) **bắt buộc phải bật**.

## ✅ ****4️⃣ Bảo vệ dữ liệu khách hàng****

* 💳 Dữ liệu khách hàng (email, địa chỉ, mật khẩu hash, thông tin thanh toán,...) được bảo vệ an toàn ngay cả khi đang truyền.

# 🔐 ****Sử dụng access token và refresh token****

- Bảo mật có thư viện dotenv nhằm không để lộ thông tin nhạy cảm trong code (VD: mật khẩu DB, API key) tất cả các thông tin đó sẽ được lưu vào 1 file env  
+ Thực hiện bằng cách cho các thông tin quan trọng vào file env sau đó dùng thư viện dotenv để đọc   
  
Cấu trúc tổ chức backend  
A screenshot of a computer program

Description automatically generated

- Tiếp tục design giao diện dynamicComponent