BabyRE:

Đây là file thực thi window 32 bit.

Graphical user interface, text

Description automatically generated

Đầu tiên, chương trình khởi tạo một vùng nhớ 300 bytes, set về zero (dòng 20). Vùng nhớ này được sử dụng để chứa userinput (dòng 31 scanf với %300[^\n]s – nhập vào tối đa 300 kí tự )

Dòng 41 kiểm tra xem độ dài của userinput có lớn hơn 294 hay không. Nếu đúng thì tiếp tục gọi hàm encrypt.

Hàm encrypt: Graphical user interface, text, application, email

Description automatically generated

Ở đây, ta chú ý tới một vùng nhớ đặc biệt là encrypt\_rule. Đây là 1 vùng nhớ đã chứa dữ liệu sẵn (fix cứng, không phải là dump ra lúc chương trình chạy, cũng không phụ thuộc vào user input). Cấu trúc vùng nhớ này là 1 array 122 object, 1 object có kích thước 12byte (3 dword). DWORD thứ nhất chứa option để encrypt, DWORD thứ hai chứa vị trí trên userinput được sử dụng để encrypt. DWORD thứ ba chính là payload để so sánh, nếu