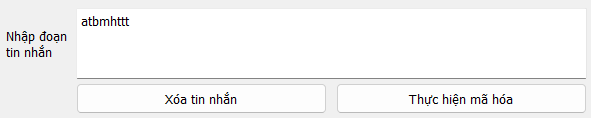
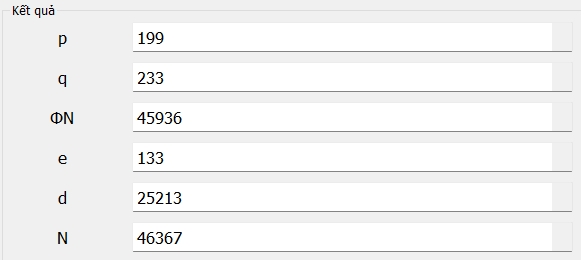
DEMO ỨNG DỤNG MÔ PHỎNG QUÁ TRÌNH MÃ HOÁ TIN NHẮN BẰNG RSA

Đầu tiên ta nhập đoạn tin nhắn cần được mã hoá:



Ở đây, ta nhập đoạn tin nhắn là “atbmhttt”. Sau đó, nhấn vào “Thực hiện mã hoá”.

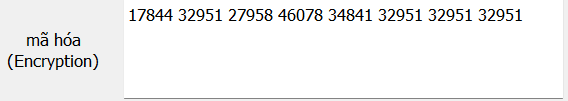


Đoạn code thực hiện lấy ngẫu nhiên các số nguyên tố cho 2 số “q” và “p” có giá trị xấp xỉ nhau, sau đó tính N theo công thức q\*p = N.

Tiếp đến tính bằng công thức (p-1) \* (q-1) = .

Kế đến, thuật toán tìm 1 số nhiên “e” với điều kiện 1 < eA < , gdc (eA, )=1.

Đồng thời thực hiện tìm kiếm “d” theo thuật toán Euclide mở rộng.



Dựa vào bảng ASCII kết hợp với “e” và “N” mà thuật toán cung cấp, chúng ta có được đoạn mã hoá như trên.

Để giải mã đoạn mã trên ta dùng “d” và “N” từ thuật toán, ta giải mã được đoạn tin nhắn ban đầu.

