

1 Phát biểu bài toán

- INPUT:
 - (n, e) : (Khóa công khai)
 - c : (Bản mã)
 - t : (Phần văn bản cố định trong bản rõ)
 - y : (Giới hạn của phần bí mật trong bản rõ)
- OUTPUT:
 - x : (Phần bí mật trong bản rõ)