## Thử nghiệm các phương pháp mật mã đã học, thực hiện ký số và xác thực

## Link 1: <https://legacy.cryptool.org/en/cto/>

**Sử dụng Mã hóa bằng RSA (step-by-step):**

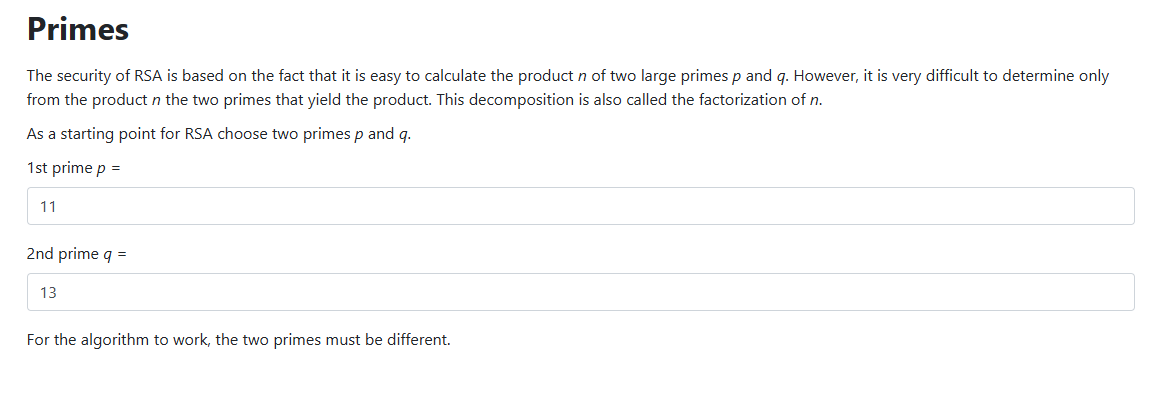
1. Chọn hai số nguyên tố:

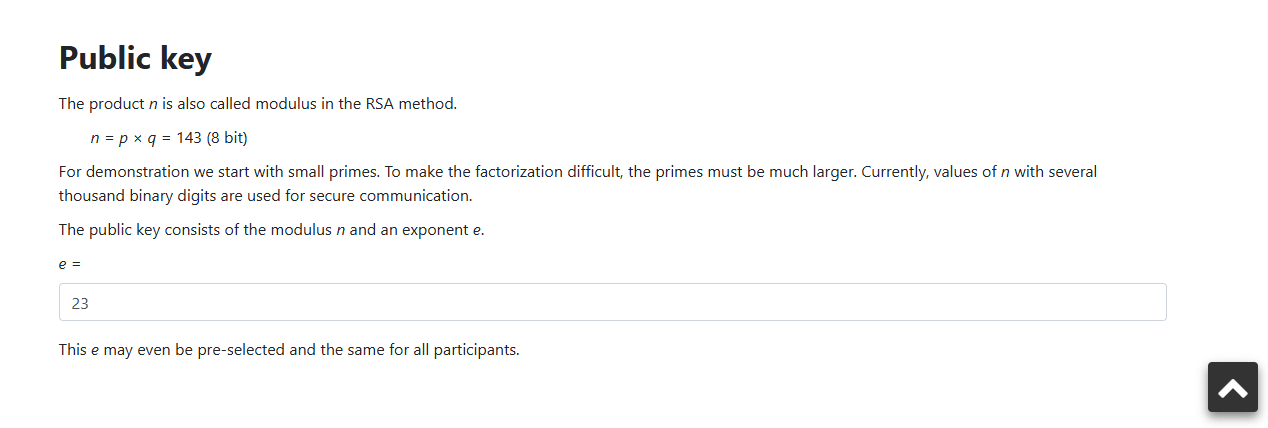
- p = 11

- q = 13

- Tính n = p × q = 143

- Tính φ(n) = (p - 1)(q - 1) = 120





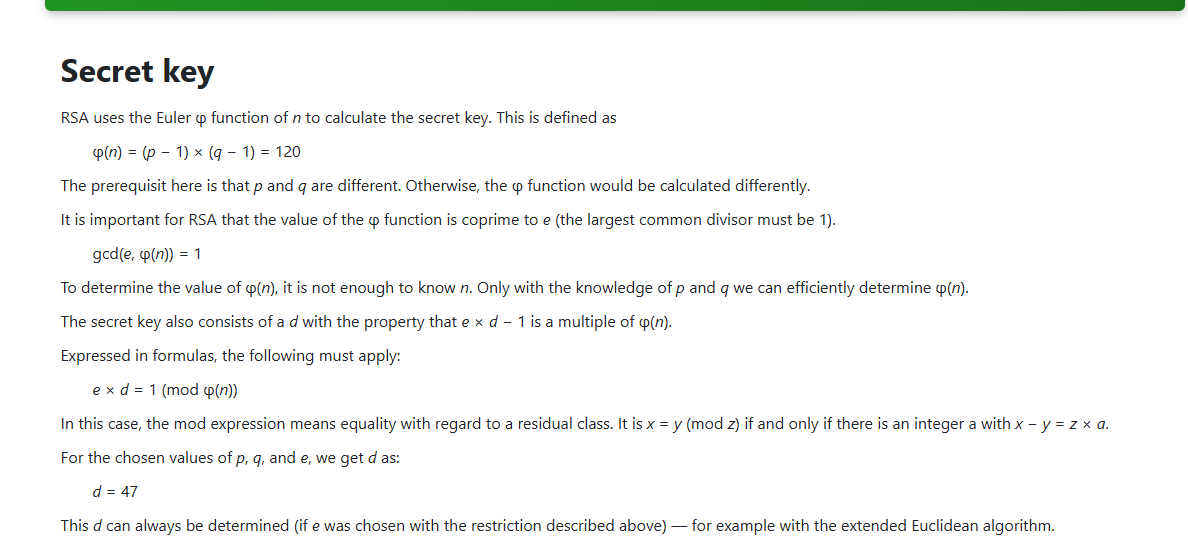
2. Sinh khóa công khai và bí mật:

- Chọn e = 23 (thoả điều kiện gcd(e, φ(n)) = 1)

- Tính d = 47 sao cho (e × d) mod φ(n) = 1

- Public key: (23, 143)

- Private key: (47, 143)



3. Thực hiện ký số:

- Thông điệp (Plaintext): 7

- Chữ ký số = 7^47 mod 143 = 2

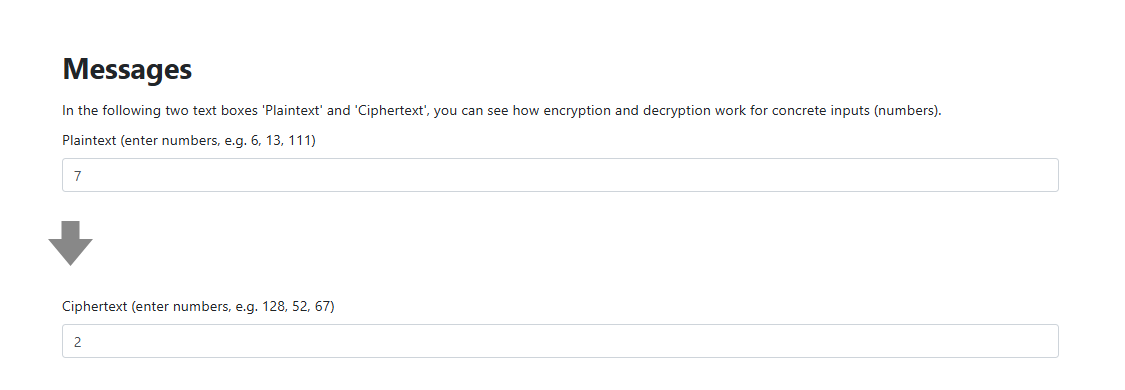


4. Xác thực chữ ký:

- Dùng chữ ký số 2

- Giải mã: 2^23 mod 143 = 7 (trùng với thông điệp gốc)

- ⇒ Xác thực thành công



**Sử dụng Mã hóa bằng Caesar Cipher (Mã hóa dịch chuyển)**

1. Nhập thông điệp cần mã hóa:

- Nội dung: HELLOCRYPTOOL

2. Thiết lập khóa dịch chuyển:

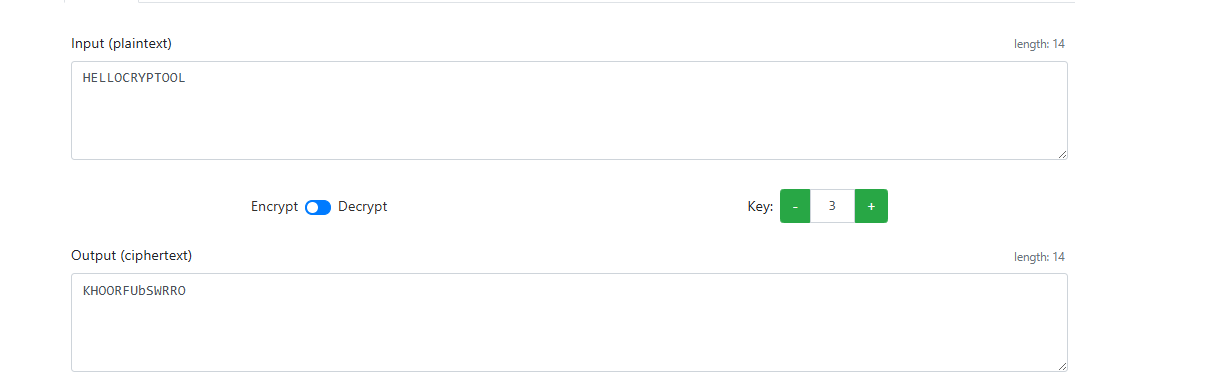
- Key (Shift) = 3

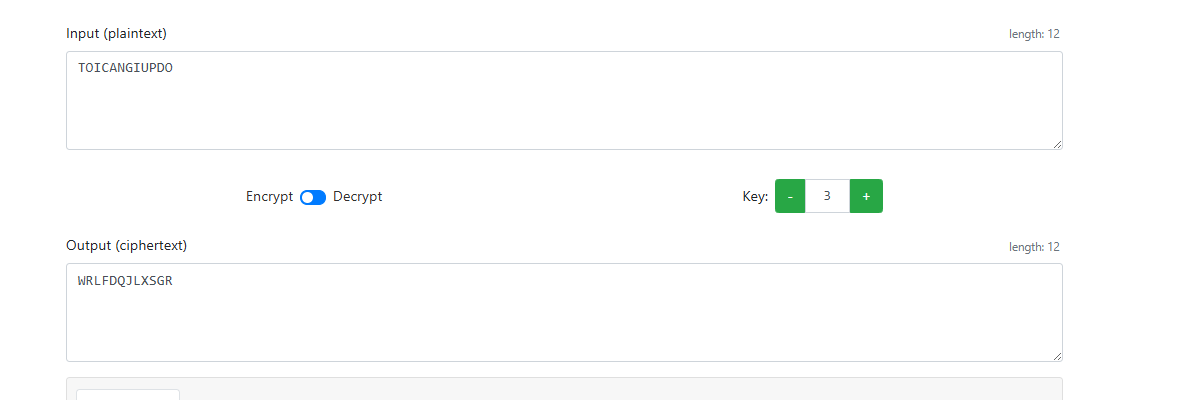
3. Kết quả mã hóa:

- Ciphertext: KHOORFUBSWRRO

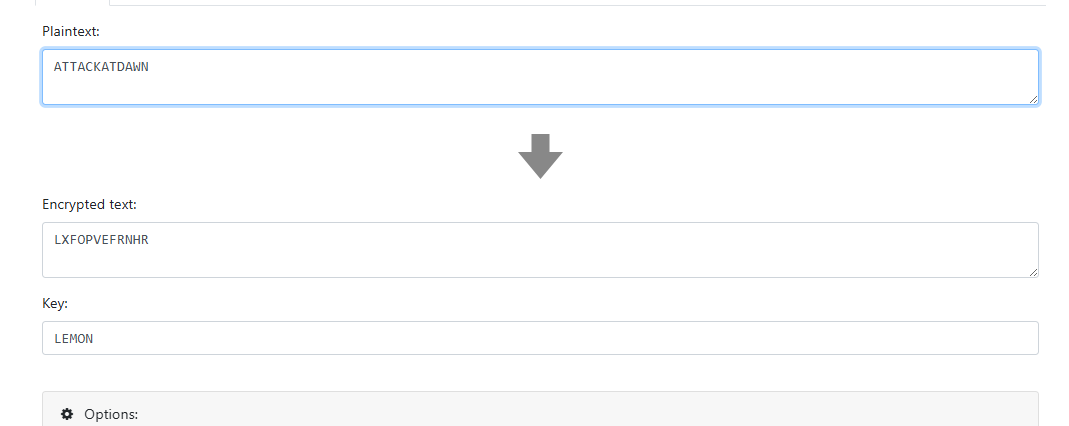
4. Giải mã lại:

- Kết quả giải mã: HELLOCRYPTOOL

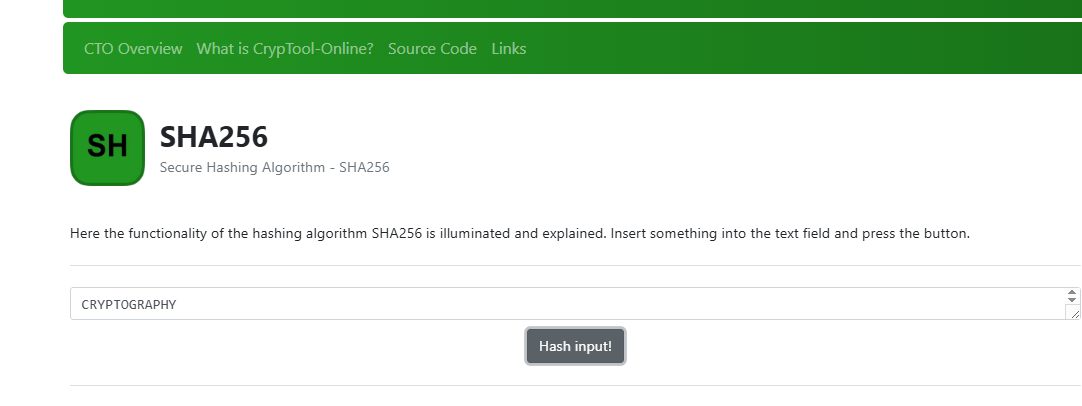


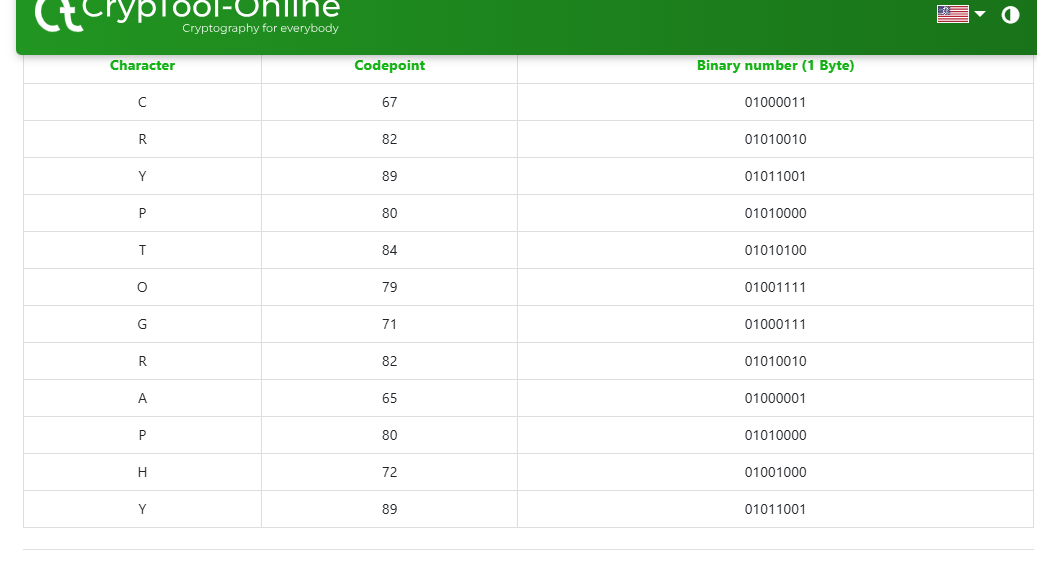


**Sử dụng Mã hóa bằng Vigenère Cipher (Mã hóa nhiều bảng)**



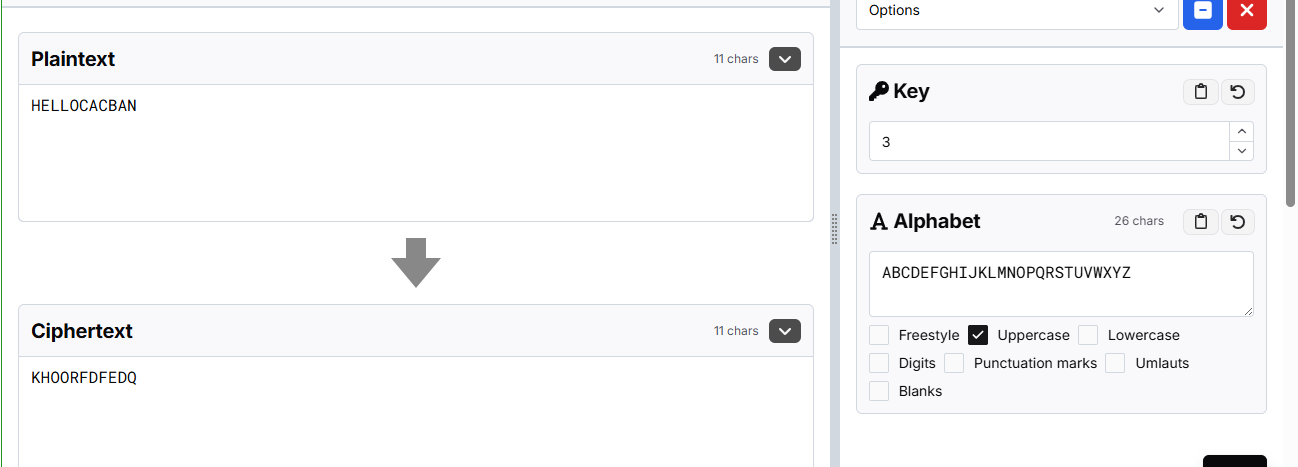
**Sử dụng Hàm băm SHA**

****

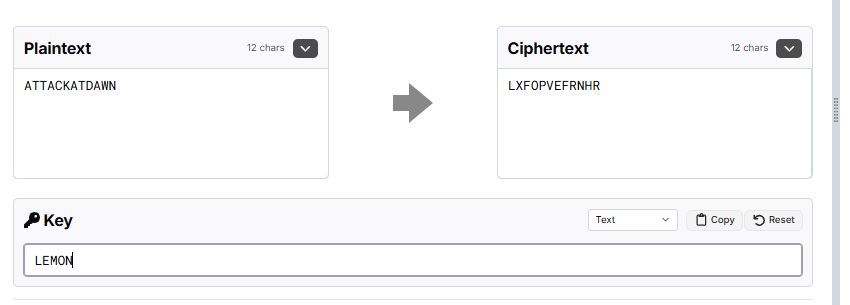
****

**Link 2:**[**https://www.cryptool.org/en/cto/**](https://www.cryptool.org/en/cto/)

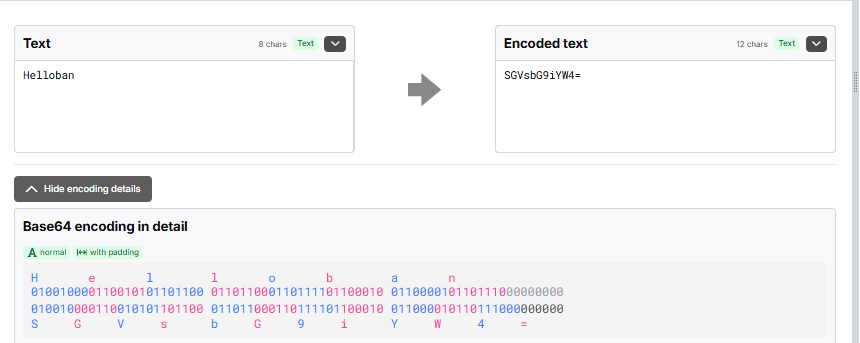
**Sử dụng Mã hóa bằng Caesar Cipher (Mã hóa dịch chuyển)**



**Sử dụng Mã hóa bằng Vigenère Cipher (Mã hóa nhiều bảng)**



**Sử dụng Mã hóa bằng Base64 Encoding**



**Sử dụng mã hóa Bacon (Bacon Cipher)**

