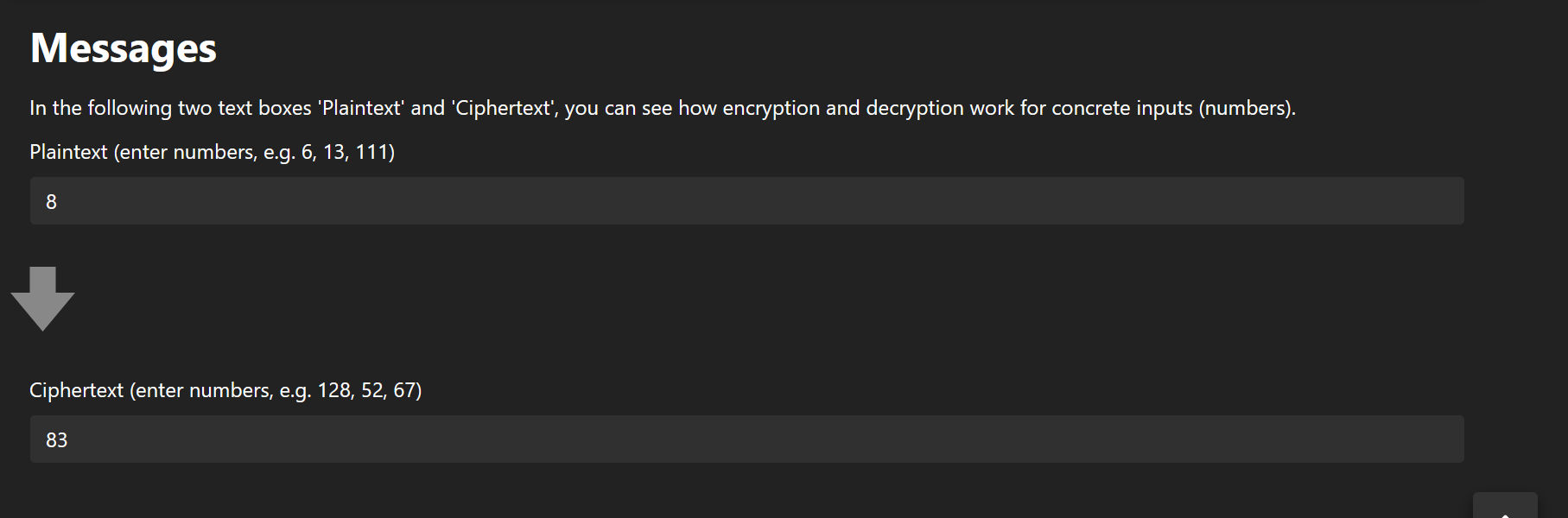
1. **RSA Encryption – Mã hóa bất đối xứng**



Mục tiêu:

Thực hành mã hóa RSA – một thuật toán mật mã bất đối xứng phổ biến, trong đó:

* Khóa công khai (public key) dùng để mã hóa.
* Khóa bí mật (private key) dùng để giải mã.

Công cụ sử dụng:

CrypTool-Online (RSA step-by-step)

Thực hiện:

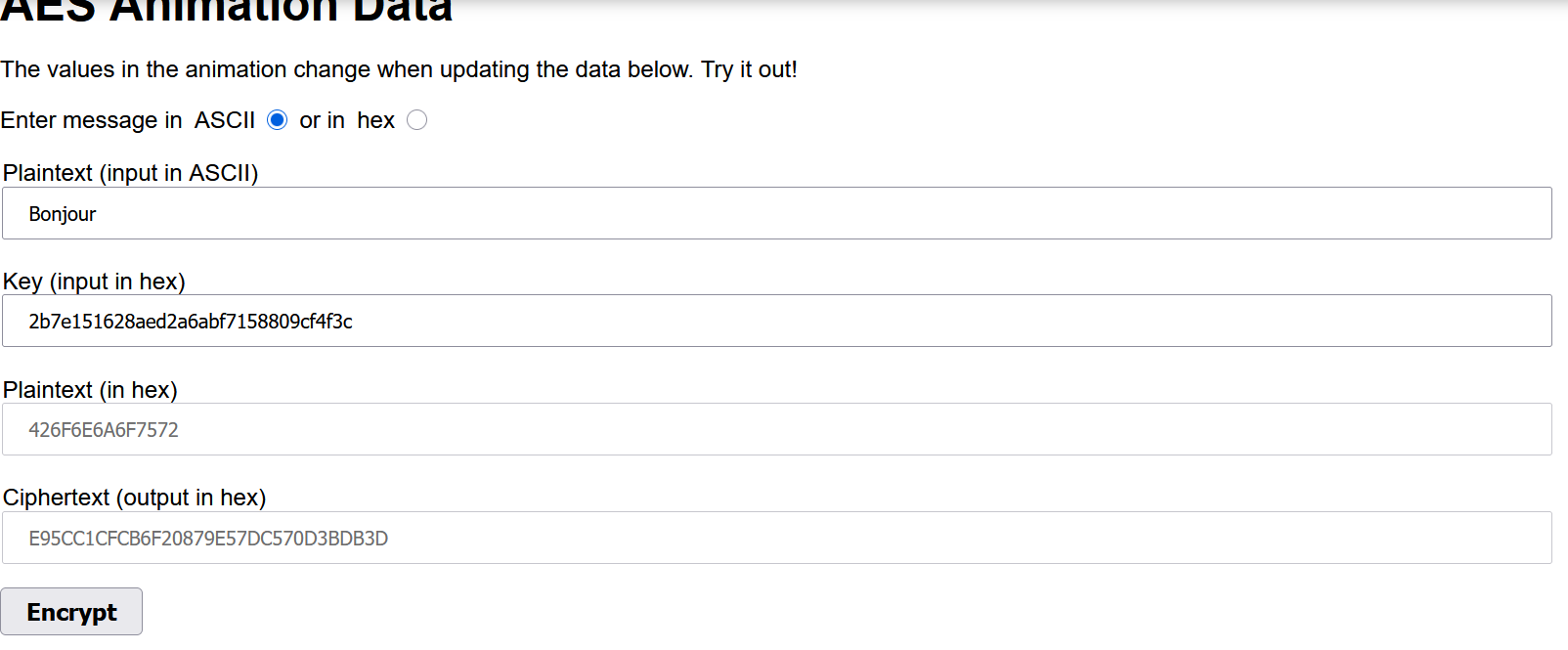
* Thông điệp gốc (Plaintext): 8
* Sau khi mã hóa (Ciphertext): 83

Giá trị 83 là kết quả của quá trình mã hóa số 8 bằng thuật toán RSA với các tham số mặc định được cung cấp bởi công cụ.

Giải thích:

* Công cụ đã sử dụng một cặp khóa RSA gồm e, d và n (không hiển thị chi tiết).
* Thông điệp được chuyển thành số, sau đó áp dụng công thức:

1. **AES Animation (Mã hóa đối xứng).**



#### **Mục tiêu:**

Thực hành thuật toán AES (Advanced Encryption Standard) – một dạng **mã hóa đối xứng** sử dụng cùng một khóa cho mã hóa và giải mã.

#### **Công cụ sử dụng:**

AES Animation (tool trực tuyến mô phỏng trực quan các bước trong AES)

#### **Thực hiện:**

* **Plaintext (ASCII):** Bonjour
* **Plaintext (hex):** 426F6E6A6F7572
* **Khóa (Key - hex):** 2b7e151628aed2a6abf7158809cf4f3c
* **Kết quả mã hóa (Ciphertext - hex):** E95CC1CFCB6F20879E57DC570D3BBD3D

Chuỗi Bonjour được chuyển sang mã hex tương ứng trước khi thực hiện mã hóa với khóa 128-bit. Kết quả là một đoạn ciphertext dài 128-bit, thể hiện dưới dạng hex.

#### **Giải thích:**

* AES sử dụng nhiều vòng lặp (rounds) với các bước như: SubBytes, ShiftRows, MixColumns, AddRoundKey.
* Khóa đầu vào được dùng để tạo ra nhiều **round keys** thông qua quá trình **key expansion**.
* Chuỗi "Bonjour" sau khi được chuyển sang hex đã được mã hóa thành chuỗi không thể đọc được (ciphertext), bảo đảm tính **bảo mật nội dung**.

### ****Mã hóa ASCII (Text Encoding)****

### 

#### **Mục tiêu:**

Chuyển đổi chuỗi ký tự "Bonjour" sang **mã nhị phân ASCII** – đây là bước cơ bản đầu tiên trước khi áp dụng các thuật toán mã hóa như AES hay RSA.

#### **Thực hiện:**

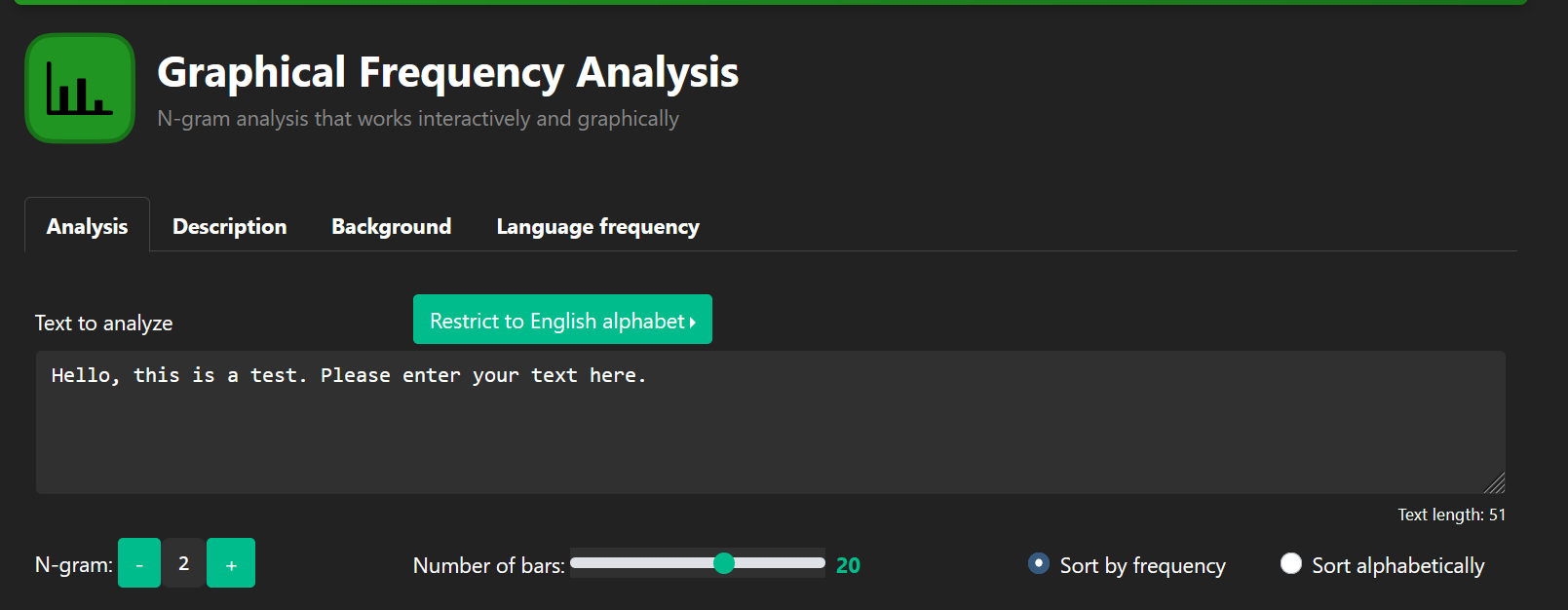
* **Chuỗi đầu vào (Plaintext):** Bonjour
* **Kết quả mã hóa ASCII (dạng nhị phân):**

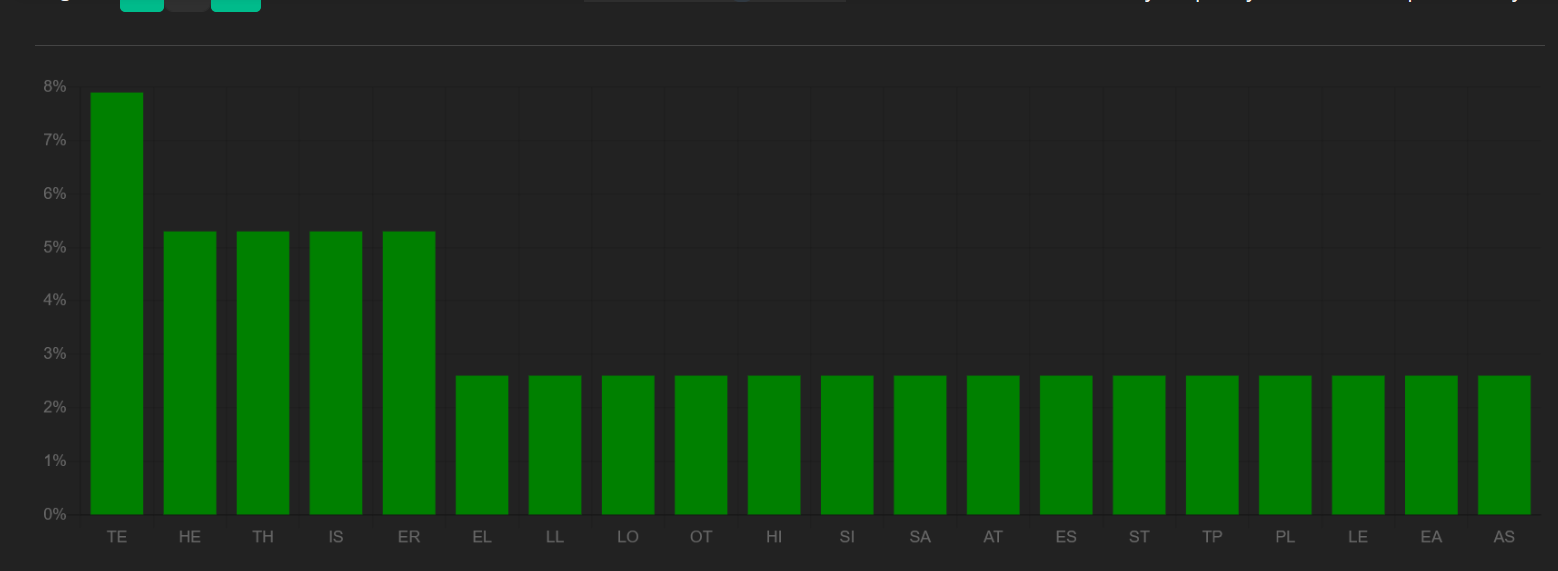
01000010 01101111 01101110 01101010 01101111 01110101 01110010

#### **Giải thích:**

* Mỗi ký tự trong chuỗi "Bonjour" được ánh xạ sang **mã ASCII** 8 bit.
* Ví dụ:
  + B → 01000010
  + o → 01101111
  + n → 01101110
  + …
* Đây là **bước chuẩn hóa dữ liệu** rất quan trọng, để chuỗi có thể xử lý trong môi trường mã hóa nhị phân như AES hay RSA.

## **Frequency Analysis (Phân tích tần suất)**





Hình ảnh thể hiện kết quả của một công cụ phân tích tần suất đồ họa sử dụng **N-gram** (ở đây là bigram - 2 ký tự).

### **Mô tả**:

* Văn bản đầu vào: "Hello, this is a test. Please enter your text here."
* Kết quả là tần suất xuất hiện của các cặp ký tự (bigram) như: TE, HE, TH, IS, ER...

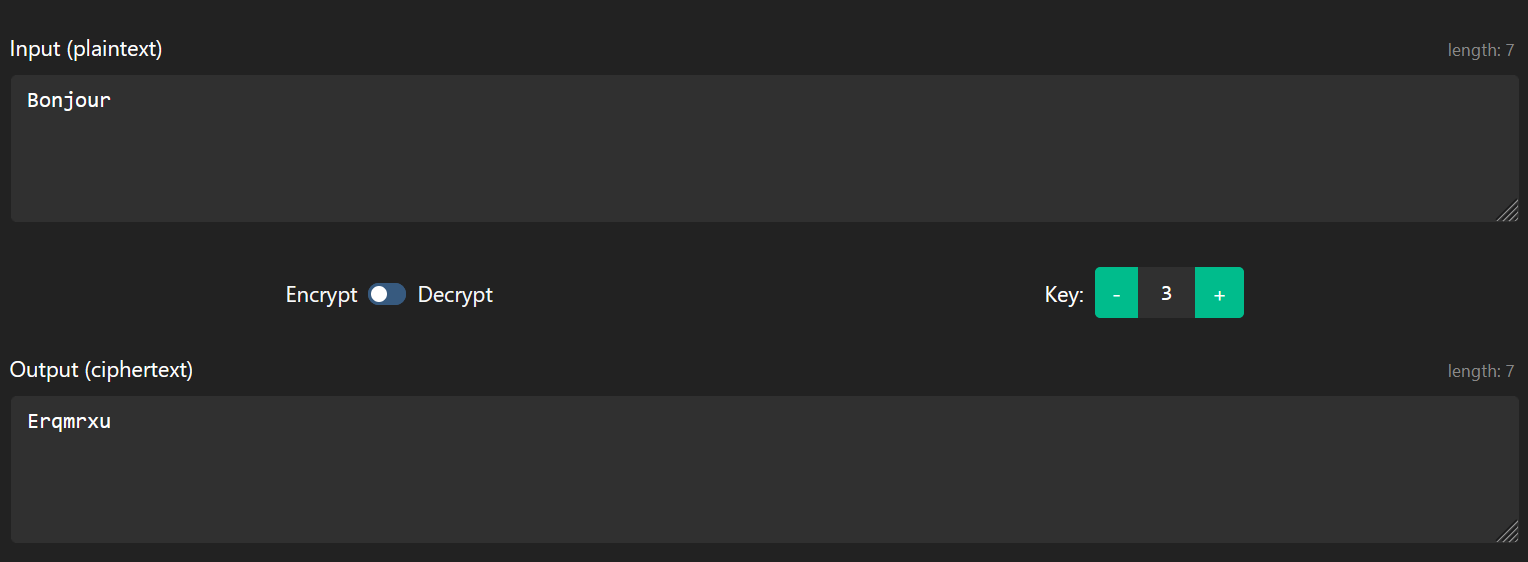
### **Ý nghĩa**:

* Phân tích tần suất là một kỹ thuật thường dùng trong phá mã cổ điển như **mật mã Caesar** hoặc **mật mã monoalphabetic.**
* Các cặp ký tự phổ biến như "TH", "HE", "IN" có thể giúp suy đoán văn bản gốc.

### **Ứng dụng**:

* Phá mã thủ công
* Phân tích ngôn ngữ học
* Phát hiện các mẫu trong dữ liệu

1. **Caesar.**

****

Mục tiêu

Thực hiện mã hóa văn bản sử dụng thuật toán Caesar – một trong những phương pháp mã hóa cổ điển đơn giản nhất.

Cơ sở lý thuyết

Mã hóa Caesar là một dạng mã hóa thay thế trong đó mỗi ký tự trong bản rõ (plaintext) được thay thế bằng một ký tự khác cách nó một số vị trí cố định trong bảng chữ cái.

Công thức mã hóa:

C = (P + k) mod 26

Trong đó:

* C: ký tự sau khi mã hóa
* P: vị trí của ký tự gốc (A = 0, B = 1, ..., Z = 25)
* k: khóa (số bước dịch)
* mod 26: để quay vòng trong bảng chữ cái tiếng Anh

Ví dụ nếu k = 3, thì:

* A → D
* B → E
* Z → C

Thực hiện:

Văn bản: Bonjour

Khóa dịch: 3

Văn bản sau khi mã hóa: Erqmrxu

##### Bảng chuyển từng ký tự:

| **Ký tự gốc** | **Ký tự mã hóa** |
| --- | --- |
| B | E |
| o | r |
| n | q |
| j | m |
| o | r |
| u | x |
| r | u |

### **Nhận xét**

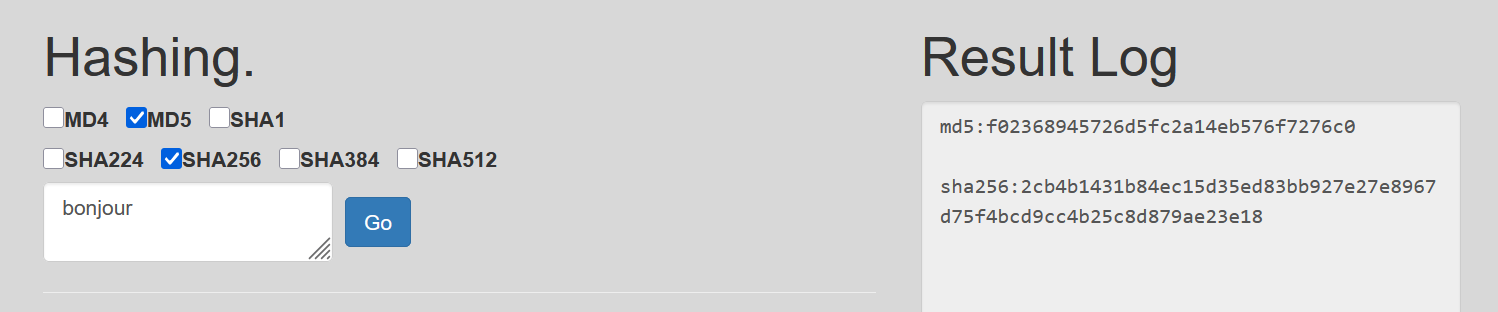
* Phương pháp này đơn giản, dễ cài đặt, nhưng **rất dễ bị phá vỡ** do chỉ có 25 khóa dịch có thể thử.
* Thường chỉ dùng để **minh họa nguyên lý mã hóa** hoặc dùng trong các trò chơi, bài tập giáo dục.
* Mã hóa Caesar không an toàn trong thực tế hiện đại.

### **Ứng dụng thực tế**

* Dạy học về mật mã học cổ điển
* Tạo trò chơi giải mật thư đơn giản
* Giới thiệu khái niệm mã hóa thay thế

**CRYPTO KNIFE.**

- Sử dụng MD5 và SHA256 để băm chuỗi.

****

- Encoding-Base64 (Mã hóa nhị phân):

