Mã hóa đơn bảng

Mã hóa dựa trên mật khẩu

INPUT:

- Bảng chữ cái

- Mật khẩu

- Giá trị cần mã hóa

OUTPUT:

- Kết quả mã hóa

VD:

Bảng chữ cái: a, d, h, k, i, o, p, g

Mật khẩu: abc

Giá trị cần mã: di hoc vui (10 ký tự)

**Mã hóa:**

B1: Sinh mật khẩu lặp lại sao cho độ dài mật khẩu bằng độ dài của giá trị cần mã

Mật khẩu mới = abcabcabca (10 ký tự)

B2: Tạo bảng tra từ bảng chữ cái

BT[4,2] = p; BT[6,5] = k

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| a | d | h | k | i | o | p | g |
| d | h | k | i | o | p | g | a |
| h | k | i | o | p | g | a | d |
| k | i | o | p | g | a | d | h |
| i | o | p | g | a | d | h | k |
| o | p | g | a | d | h | k | i |
| p | g | a | d | h | k | i | o |
| g | a | d | h | k | i | o | p |

for(int i = 0; i < BCC.Length; i++)

for(int j = 0; j < BCC.Length; j++)

BT[i,j] = BCC[(i + j)%BCC.Length];

B3: Tra bảng để mã hóa

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| d | i | \_ | h | o | c | \_ | v | u | i |
| a | b | c | a | b | c | a | b | c | a |
| **g** | **i** | **\_** | **p** | **o** | **c** | **\_** | **v** | **u** | **i** |

Với mỗi ký tự cần mã hóa, ta tìm vào bảng ở dòng có ký tự của cột đầu tiên trùng với giá trị cần mã hóa, tìm trên dòng đó ký tự trùng với giá trị mật khẩu, nếu có thì lấy về ký tự ở dòng đầu tiên trên cột tìm được. Giá trị tìm được chính là kết quả mã hóa của ký tự. Nếu không tìm thấy thì để nguyên không mã hóa.

**Giải mã**

B1: Sinh mật khẩu … như Mã hóa

B2: Sinh bảng tra … như Mã hóa

B3: Tra bảng để giải mã

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **g** | **i** | **\_** | **p** | **o** | **c** | **\_** | **v** | **u** | **i** |
| **a** | **b** | **c** | **a** | **b** | **c** | **a** | **b** | **c** | **a** |
| **d** | **i** | **\_** | **h** | **o** | **c** | **\_** | **v** | **u** | **i** |

Tương tự như Mã hóa (dùng giá trị cần giải mã và mật khẩu để tra)

ỨNG DỤNG:

Mã hóa đơn bảng chỉ **mã hóa ký tự**

**Làm thế nào để sử dụng thuật toán này mã hóa được tệp tin bất kỳ?**

Để thực hiện được

B1: **Chuyển tệp tin thành ký tự**

*B1.1: Đọc tệp tin thành mảng byte*

*B1.2: Chuyển mảng byte thành chuỗi* Base64

B2: **Mã hóa**

B3: Lưu kết quả thành tệp tin