**Bài tập đề số 38**

1. **Mật mã caesar**

Input: EVERYONEHASTHEIRPR

Key: 9

Cách làm: Dịch các chữ cái trong bảng chữ cái sang key đơn vị. Nếu hết bảng thì quay lại chữ cái đầu tiên.

Gốc:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

Mã hóa:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |

=> Output: NENAHXWNQJBCQNRAYA

1. **Mật mã vigenere – lặp khóa**

Input: EVERYONEHASTHEIRPR

Key: THEMORET

Cách làm: lặp khóa đến khi nào độ dài khóa = độ dài input. Sau đó so sánh với bảng để ra kết quả.

=> Key sau khi mã hóa = THEMORETTHEMORETTH

=> Output: XCIDMFRXAHWFVVMKIY

1. **Mật mã vigenere – autokey**

Input: EVERYONEHASTHEIRPR

Key: MANYALIT

Cách làm: Lấy thêm các chữ cái của input để cho vào key để độ dài key = độ dài input. Sau đó so sánh với bảng để ra kết quả.

=> Key sau khi mã hóa: MANYALITEVERYONEHA

Output: QVRPYZVXLVWKFSVVWR

1. **Mã hóa chữ đơn**

Input: EVERYONEHASTHEIRPR

Key: BFEPXVCOHRQDSTUIWGYMJNZKAL

Cách làm: So input với key

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | F | E | P | X | V | C | O | H | R | Q | D | S | T | U | I | W | G | Y | M | J | N | Z | K | A | L |

=> Output: XNXYAUTXOBYMOXHGIG

1. **Mật mã ma trận khóa playfair**

Input: EVERYONEHASTHEIRPR

Key: PENNYWIS

Cách làm: Sử dụng 1 ma trận 5x5, các chữ cái được sắp xếp từ trái qua phải, từ trên xuống dưới.

Graphical user interface, application, Word

Description automatically generated with medium confidence

B1: Tách cặp: EV ER YO NE HA ST HE IR PR

B2: Chuyển: NU WM NQ YN BG IU YF CL WL

=> Output: NUWMNQYNBGIUYFCLWL

1. **Mật mã hoán vị**

Input: EVERYONEHASTHEIRPR

Key: 8

Cách làm: Ghi input dưới dạng 1 chuỗi các đường chéo có độ sau là key. Sau đó đọc lần lượt các hàng.

=>

|  |  |  |
| --- | --- | --- |
| E | H | P |
| V | A | R |
| E | S |  |
| R | T |  |
| Y | H |  |
| O | E |  |
| N | I |  |
| E | R |  |

=> Output: EHPVARESRTYHEONIER

**Bài tập mẫu**

1. **Mật mã caesar**

Input: SAVEFORARAINYDAY

Key: 25

=> Output: RZUDENQZQZHMXCZX

1. **Mật mã vigenere – lặp khóa**

Input: WHENINROMEDO

Key: THETRU

=> Output: POIGZHKVQXUI

1. **Mật mã vigenere – autokey**

Input: BARKINGDOGSS

Key: LIKEFA

=> Output: MIBONNHDFQAF

1. **Mã hóa chữ đơn**

Input: PENNYWISEPOUNDFO

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| K | G | O | X | P | M | U | H | C | A | Y | T | J | Q | W | Z | R | I | V | E | S | F | L | D | N | B |

=> Output: ZPQQNLCVPZWSQXMW

1. **Mật mã ma trận khóa playfair**

Input: STILLWATERSR

Key: SAVEFORA

=> Output: FMKGHZFNACAO

1. **Mật mã hoán vị**

Input: TIMEISMONEYTIMEISM

Key: 5

=> Output: TSYIIMTSMOIMENMIEE