**Mã cổ điển**

1. **Mật mã Caesar**

Input: M = LOVEISBLINDLOVEI

Key: K = 8

Tìm Output: C =?

Mã hóa:

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

Gán số cho từng chữ cái (Bảng chữ cái)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Chữ | A | B | C | D | E | F | G | H | I | J | K | L | M |
| STT | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Chữ | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| STT | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

C = (M +K) mod 26 ⬄ C = (M +8) mod 26

* Ta có mã M sau mã hóa với:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Input M | L | O | V | E | I | S | B | L | I | N | D | L | O | V | E | I |
| Output C | T | W | D | M | Q | A | J | T | Q | V | L | T | W | D | M | Q |

* Bản mã C: TWDMQAJTQVLTWDMQ

Giải mã:

C = TWDMQAJTQVLTWDMQ

K = 8

M =?

M = (C - K) mod 26 ⬄ M = (C – 8) mod 26

* Ta có mã C sau giải mã như sau:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Output C | T | W | D | M | Q | A | J | T | Q | V | L | T | W | D | M | Q |
| Input M | L | O | V | E | I | S | B | L | I | N | D | L | O | V | E | I |

* Bản mã C: TWDMQAJTQVLTWDMQ

1. **Mật mã Vigenere – Khóa lặp**

Input: M = MONEYMAKESTH

Key: K = NOPAIN

Tìm Output: C =?

Mã hóa:

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

Gán số cho từng chữ cái (Bảng chữ cái)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Chữ | A | B | C | D | E | F | G | H | I | J | K | L | M |
| STT | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Chữ | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| STT | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

nM = 12; nK = 6;

Lặp khóa K: NOPAINNOPAIN

C = (M +K) mod 26

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Input M | M | O | N | E | Y | M | A | K | E | S | T | H |
| Key(loop) | N | O | P | A | I | N | N | O | P | A | I | N |
| Output C | Z | C | C | E | G | Z | N | Y | T | S | B | U |

* Bản mã C = ZCCEGZNYTSBU

Giải mã:

C = ZCCEGZNYTSBU

K = NOPAIN

M =?

Lặp khóa K: NOPAINNOPAIN

M = (C – K) mod 26

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Output C | Z | C | C | E | G | Z | N | Y | T | S | B | U |
| Key(loop) | N | O | P | A | I | N | N | O | P | A | I | N |
| Input M | M | O | N | E | Y | M | A | K | E | S | T | H |

* Bản mã M = MONEYMAKESTH

1. **Mật mã Vigenere - Autokey**

Input: M = MONEYMAKESTH

Key: K = NOPAIN

Tìm Output: C =?

Mã hóa:

(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)

Gán số cho từng chữ cái (Bảng chữ cái)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Chữ | A | B | C | D | E | F | G | H | I | J | K | L | M |
| STT | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Chữ | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| STT | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

nM = 12; nK = 6;

Autokey K: NOPAINMONEYM

C = (M +K) mod 26

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Input M | M | O | N | E | Y | M | A | K | E | S | T | H |
| Key(loop) | N | O | P | A | I | N | M | O | N | E | Y | M |
| Output C | Z | C | C | E | G | Z | M | Y | R | W | R | T |

* Bản mã C: ZCCEGZMYRWRT

Giải mã:

C = ZCCEGZMYRWRT  
K = NOPAIN

M =?

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Output C | Z | C | C | E | G | Z | M | Y | R | W | R | T |
| Key(loop) | N | O | P | A | I | N |  |  |  |  |  |  |
| Input | M | O | N | E | Y | M |  |  |  |  |  |  |

Autokey K: NOPAIN + M: MONEYM (Vì nC = 12; nK = 6 => Điền 6 chữ cái đầu tiên của M nối vào K) = NOPAINMONEYM

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Output C | Z | C | C | E | G | Z | M | Y | R | W | R | T |
| Key(loop) | N | O | P | A | I | N | M | O | N | E | Y | M |
| Input | M | O | N | E | Y | M | A | K | E | S | T | H |

* Bản mã M = MONEYMAKESTH

1. **Mã hóa chữ đơn**

Input: M = THEGRASSAREALWAY

Key: K = HLXQPSVKMZYCDUEGJTNFBAIWOR

Tìm Output: C =?

Mã hóa:

(Cách làm: So input với key)

So sánh bảng chữ cái với Key:

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

C sẽ tương ứng với các ký tự Key theo các ký tự Alphabet bên trên dóng xuống

* C = FKPVTHNNHTPHCIHO

Giải mã:

Output: C = FKPVTHNNHTPHCIHO

Key: K = HLXQPSVKMZYCDUEGJTNFBAIWOR

Input: M =?

So sánh Key với bảng chữ cái:

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

M sẽ tương ứng với các ký tự trong Alphabet theo các ký tự Key bên trên dóng xuống

1. **Mật mã ma trận khóa Playfair**

Input: M = LOVEISBLINDL

Key: K = HONESTY

Tìm Output: C =?

Mã hóa:

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 |

Khóa K thành ma trận sau: (Dồn các key trước rồi dồn các ký tự trong bảng alphabet ngoại trừ các key đã cho xuống dưới lần lượt từ trái sang phải, từ trên xuống dưới)

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

B1: Tách cặp M: LO VE IS BL IN DL

B2: Chuyển theo quy tắc: HM OX EK TQ EG LU

(Quy tắc:

* Nếu 2 chữ giống nhau, tách ra bởi 1 chữ điền thêm thường là X hoặc Q.
* Nếu 2 chữ nằm cùng hàng, thay bởi các chữ bên phải.
* Nếu 2 chữ nằm cùng cột, thay bởi các chữ bên dưới.
* Các trường hợp khác, mỗi chữ cái được thay bởi chữ cái khác cùng hàng, trên cột chữ cái cùng cặp.)
* C = HMOXEKTQEGLU

Giải mã:

C = HMOXEKTQEGLU

K = HONESTY

M =?

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

B1: Tách cặp C: HM OX EK TQ EG LU

B2: Chuyển theo quy tắc: LO VE IS BL IN DL

(Quy tắc:

* Nếu 2 chữ giống nhau, tách ra bởi 1 chữ điền thêm thường là X hoặc Q.
* Nếu 2 chữ nằm cùng hàng, thay bởi các chữ bên trái.
* Nếu 2 chữ nằm cùng cột, thay bởi các chữ bên trên.
* Các trường hợp khác, mỗi chữ cái được thay bởi chữ cái khác cùng hàng, trên cột chữ cái cùng cặp- phải sang trái, dưới lên trên)

1. **Mật mã hoán vị**

Input: M = DONTTROUBLETROUBLE

Key: K = 8

Tìm Output: C =?

Mã hóa:

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

Key: K = 8 = n(Rows)

|  |  |  |
| --- | --- | --- |
| D | B | L |
| O | L | E |
| N | E |  |
| T | T |  |
| T | R |  |
| R | O |  |
| O | U |  |
| U | B |  |

(Output sẽ tính từ trái sang phải, từ trên xuống dưới)

* C = DBLOLENETTTRROOUUB

Giải mã:

C = DBLOLENETTTRROOUUB

K = 8

M =?

nC = 18 => Chia thành 3 cột (vì 18/8 = 2 dư 2)

Điền các ký tự từ trái sang phải, từ trên xuống dưới, cột bên ngoài đầy thì sẽ ngắt không tiếp tục thực hiện việc điền tiếp

|  |  |  |
| --- | --- | --- |
| D | B | L |
| O | L | E |
| N | E |  |
| T | T |  |
| T | R |  |
| R | O |  |
| O | U |  |
| U | B |  |