**AN TOÀN HỆ THỐNG THÔNG TIN**

**Nhóm 2**

**Thành viên nhóm:** + Trần Thanh Hiệp – 2151050469

+ Bùi Thị Ngân – 2151050271

+ Lê Trí Cường – 2151053007

+ Lê Trung Hiếu – 2151050128

+ Nguyễn Song Hậu – 2151050123

+ Nguyễn Văn Cảnh – 2151053005

+ Nguyễn Hữu Toàn – 2151050462

+ Nguyễn Y Khoa – 2151500202

**Bài tập thuật mã 3 - Thuật mã Vigenere & Playfair**

ĐỀ BÀI:

1. Cho k = CITY, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = VPTLJXAMOWGEOW
2. Cho k = CITY, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = FIEYVVZYPPHY
3. Cho k = CITY, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = VPTLJXAMEIGRJW
4. Cho k = CITY, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = VPTLJXAMJWTNJCHLILH
5. Cho k = MONARCHY, N = 26, mã hóa văn bản, dùng thuật mã Playfair với P = ANTOANBAOMATTHONGTIN
6. Cho k = MONARCHY, N = 26, giải mã văn bản, dùng thuật mã Playfair với C = FDNRSREBBFOYEFPRRA
7. Cho k = MONARCHY, N = 26, giải mã văn bản, dùng thuật mã Playfair với C = FDNRYQNRGAEWSKOYMH
8. Cho k = MONARCHY, N = 26, giải mã văn bản, dùng thuật mã Playfair với C = FDNRABBCWMKYRACZYQ
9. Cho k = KEY, N = 26, giải mã văn bản, dùng thuật mã Playfair với C = BCNBAJOZDVXKOMKFJONA
10. Cho k = KEY, N = 26, giải mã văn bản, dùng thuật mã Playfair với C = SNGSCFJONSYNBGJH

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

BÀI GIẢI:

**Câu 1: Cho k = CITY, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = VPTLJXAMOWGEOW**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Trước giải mã | V | P | T | L | J | X | A | M | O | W | G | E | O | W |
| K | C | I | T | Y | C | I | T | Y | C | I | T | Y | C | I |
| Sau giải mã | T | H | A | N | H | P | H | O | M | O | N | G | M | O |

* Vậy **VPTLJXAMOWGEOW** được giải mã thành **THANHPHOMONGMO**

**Câu 2: Cho k = CITY, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = FIEYVVZYPPHY**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Trước giải mã | F | I | E | Y | V | V | Z | Y | P | P | H | Y |
| K | C | I | T | Y | C | I | T | Y | C | I | T | Y |
| Sau giải mã | D | A | L | A | T | N | G | A | N | H | O | A |

* Vậy **FIEYVVZYPPHY** được giải mã thành **DALATNGANHOA**

**Câu 3: Cho k = CITY, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = VPTLJXAMEIGRJW**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Trước giải mã | V | P | T | L | J | X | A | M | E | I | G | R | J | W |
| K | C | I | T | Y | C | I | T | Y | C | I | T | Y | C | I |
| Sau giải mã | T | H | A | N | H | P | H | O | C | A | N | T | H | O |

* Vậy **VPTLJXAMEIGRJW** được giải mã thành **THANHPHOCANTHO**

**Câu 4: Cho k = CITY, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = VPTLJXAMJWTNJCHLILH**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Trước giải mã | V | P | T | L | J | X | A | M | J | W | T | N | J | C | H | L | I | L | H |
| K | C | I | T | Y | C | I | T | Y | C | I | T | Y | C | I | T | Y | C | I | T |
| Sau giải mã | T | H | A | N | H | P | H | O | H | O | A | P | H | U | O | N | G | D | O |

* Vậy **VPTLJXAMJWTNJCHLILH** được giải mã thành **THANHPHOHOAPHUONGDO**

**Câu 5: Cho k = MONARCHY, N = 26, mã hóa văn bản, dùng thuật mã Playfair với P = ANTOANBAOMATTHONGTIN**

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

Tách p thành các cặp kí tự và mã hóa:

* AN => RA (Cùng hàng)
* TO => PR (Tạo hình chữ nhật)
* AN => RA (Cùng hàng)
* TH => PD (Tạo hình chữ nhật)
* ON =>NA (Cùng hàng)
* GT =>KQ (Tạo hình chữ nhật)
* IN => GA (Tạo hình chữ nhật)

Vậy mã hóa chuỗi **ANTOANTHONGTIN** thành **RAPRRAPDNAKQGA**

**Câu 6: Cho k = MONARCHY, N = 26, giải mã văn bản, dùng thuật mã Playfair với C = FDNRSREBBFOYEFPRRA**

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

Tách C thành các cặp kí tự và mã hóa:

* FD => KH (Tạo hình chữ nhật)
* NR => OA (Cùng hàng)
* SR => TA (Tạo hình chữ nhật)
* EB => IC (Tạo hình chữ nhật)
* BF => HI (Tạo hình chữ nhật)
* OY => NH (Tạo hình chữ nhật)
* EF => KE (Cùng hàng)
* PR => TO (Tạo hình chữ nhật)
* RA => AN (Cùng hàng)

Vậy giải mã chuỗi **FDNRSREBBFOYEFPRRA** thành **KHOATAICHINHKETOAN**

**Câu 7: Cho k = MONARCHY, N = 26, giải mã văn bản, dùng thuật mã Playfair với C = FDNRYQNRGAEWSKOYMH**

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

Tách C thành các cặp kí tự và mã hóa:

* FD => KH (Tạo hình chữ nhật)
* NR => OA (Cùng hàng)
* YQ => NG (Cùng cột)
* NR => OA (Cùng hàng)
* GA => IN (Tạo hình chữ nhật)
* EW => GU (Tạo hình chữ nhật)
* SK => TI (Tạo hình chữ nhật)
* OY => NH (Tạo hình chữ nhật)
* MH => OC (Tạo hình chữ nhật)

Vậy giải mã chuỗi **FDNRYQNRGAEWSKOYMH** thành **KHOANGOAINGUTINHOC**

**Câu 8: Cho k = MONARCHY, N = 26, giải mã văn bản, dùng thuật mã Playfair với C = FDNRABBCWMKYRACZYQ**

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

Tách C thành các cặp kí tự và mã hóa:

* FD => KH (Tạo hình chữ nhật)
* NR => OA (Cùng hàng)
* AB => XA (Cùng cột)
* BC => YD (Cùng hàng)
* WM => UN (Tạo hình chữ nhật)
* KY => GD (Tạo hình chữ nhật)
* RA => AN (Cùng hàng)
* CZ => DU (Tạo hình chữ nhật)
* YQ => NG (Cùng cột)

Vậy giải mã chuỗi **FDNRABBCWMKYRACZYQ** thành **KHOAXAYDUNGDANDUNG**

**Câu 9: Cho k = KEY, N = 26, giải mã văn bản, dùng thuật mã Playfair với C = BCNBAJOZDVXKOMKFJONA**

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

Tách C thành các cặp kí tự và mã hóa:

* BC => KH (Tạo hình chữ nhật)
* NB => OA (Tạo hình chữ nhật)
* AJ => KN (Tạo hình chữ nhật)
* OZ => HT (Cùng cột)
* DV => EQ (Cùng cột)
* XK => UA (Tạo hình chữ nhật)
* OM => NL (Cùng hàng)
* KF => YC (Tạo hình chữ nhật)
* JO => ON (Cùng hàng)
* NA => GX (Cùng cột)

Vậy giải mã chuỗi **BCNBAJOZDVXKOMKFJONA** thành **KHOAKNHTEQUANLYCONGX**

**Câu 10: Cho k = KEY, N = 26, giải mã văn bản, dùng thuật mã Playfair với C = SNGSCFJONSYNBGJH**

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

Tách C thành các cặp kí tự và mã hóa:

* SN => NG (Cùng cột)
* GS => AN (Cùng cột)
* CF => HD (Cùng hàng)
* JO => ON (Cùng hàng)
* NS => GN (Cùng cột)
* YN => AM (Tạo hình chữ nhật)
* BG => AH (Tạo hình chữ nhật)
* JH => OC (Tạo hình chữ nhật)

Vậy giải mã chuỗi **SNGSCFJONSYNBGJH** thành **NGANHDONGNAMAHOC**