**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 2 - Thuật mã Vigenere**

ĐỀ BÀI:

1. Cho k = MAHOA, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = SIHWMMTOCNSTPB
2. Cho k = KHOA, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = DOONRWVOWHBGDLBBKJ
3. Cho k = KEY, N = 26, mã hóa văn bản, dùng thuật mã Vigenere với P = KHOACONGNGHETHONGTIN
4. Cho k = TRUONGDH, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = WRCVBIPVMGBQZ
5. Cho k = BIMAT, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = LPAADJBTUTUFMYWVVS
6. Cho k = SECRET, N = 26, mã hóa văn bản, dùng thuật mã Vigenere với P = HETHONGTHONGTIN
7. Cho k = MONARCHY, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = MBAIEJOCFVBNX
8. Cho k = SECRET, N = 26, mã hóa văn bản, dùng thuật mã Vigenere với P = KHOACONGNGHETHONGTIN
9. Cho k = MONARCHY, N = 26, mã hóa văn bản, dùng thuật mã Vigenere P = ANTOANBAOMATTHONGTIN
10. Cho k = TRUONG, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = LZKINTMYIBTZBE

|  | **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 (Nguyễn Văn Cảnh): Cho k = MAHOA, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = SIHWMMTOCNSTPB**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Trước giải mã | S | I | H | W | M | M | T | O | C | N | S | T | P | B |
| K | M | A | H | O | A | M | A | H | O | A | M | A | H | O |
| Sau giải mã | G | I | A | I | M | A | T | H | O | N | G | T | I | N |

* Vậy **SIHWMMTOCNSTPB** được giải mã thành **GIAIMATHONGTIN**

**Câu 2 (Lê Trung Hiếu): Cho k = KHOA, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = DOONRWVOWHBGDLBBKJ**

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

* Vậy **DOONRWVOWHBGDLBBKJ** được giải mã thành **THANHPHOMANGTENBAC**

**Câu 3 (Bùi Thị Ngân): Cho k = KEY, N = 26, mã hóa văn bản, dùng thuật mã Vigenere với P = KHOACONGNGHETHONGTIN**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Trước mã hóa | K | H | O | A | C | O | N | G | N | G | H | E | T | H | O | N | G | T | I | N |
| K | K | E | Y | K | E | Y | K | E | Y | K | E | Y | K | E | Y | K | E | Y | K | E |
| Sau mã hóa | U | L | M | K | G | M | X | K | L | Q | L | C | D | L | M | X | K | R | S | R |

* Vậy **KHOACONGNGHETHONGTIN** được mã hóa thành **ULMKGMXKLQLCDLMXKRSR**

**Câu 4 (Nguyễn Hữu Toàn): Cho k = TRUONGDH, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = WRCVBIPVMGBQZ**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Trước giải mã | W | R | C | V | B | I | P | V | M | G | B | Q | Z |
| K | T | R | U | O | N | G | D | H | T | R | U | O | N |
| Sau giải mã | D | A | I | H | O | C | M | O | T | P | H | C | M |

* Vậy **WRCVBIPVMGBQZ** được giải mã thành **DAIHOCMOTPHCM**

**Câu 5 (Lê Trí Cường): Cho k = BIMAT, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = LPAADJBTUTUFMYWVVS**

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

* Vậy **LPAADJBTUTUFMYWVVS** được giải mã thành **KHOAKITHUATXAYDUNG**

**Câu 6 (Nguyễn Y Khoa): Cho k = SECRET, N = 26, mã hóa văn bản, dùng thuật mã Vigenere với P = HETHONGTHONGTIN**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Trước mã hóa | H | E | T | H | O | N | G | T | H | O | N | G | T | I | N |
| K | S | E | C | R | E | T | S | E | C | R | E | T | S | E | C |
| Sau mã hóa | Z | I | V | Y | S | G | Y | X | J | F | R | Z | L | M | P |

* Vậy **HETHONGTHONGTIN** được mã hóa thành **ZIVYSGYXJFRZLMP**

**Câu 7 (Trần Thanh Hiệp): Cho k = MONARCHY, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = MBAIEJOCFVBNX**

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

* Vậy **MBAIEJOCFVBNX** được giải mã thành **ANNINHHETHONG**

**Câu 8 (Nguyễn Song Hậu): Cho k = SECRET, N = 26, mã hóa văn bản, dùng thuật mã Vigenere với P = KHOACONGNGHETHONGTIN**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Trước mã hóa | K | H | O | A | C | O | N | G | N | G | H | E | T | H | O | N | G | T | I | N |
| K | S | E | C | R | E | T | S | E | C | R | E | T | S | E | C | R | E | T | S | E |
| Sau mã hóa | C | L | Q | R | G | H | F | K | P | X | L | X | L | L | Q | E | K | M | A | R |

* Vậy **KHOACONGNGHETHONGTIN** được mã hóa thành **CLQRGHFKPXLXLLQEKMAR**

**Câu 9 (Trần Thanh Hiệp): Cho k = MONARCHY, N = 26, mã hóa văn bản, dùng thuật mã Vigenere P = ANTOANBAOMATTHONGTIN**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Trước mã hóa | A | N | T | O | A | N | B | A | O | M | A | T | T | H | O | N | G | T | I | N |
| K | M | O | N | A | R | C | H | Y | M | O | N | A | R | C | H | Y | M | O | N | A |
| Sau mã hóa | M | B | G | O | R | P | I | Y | A | A | N | T | K | J | V | L | S | H | V | N |

* Vậy **ANTOANBAOMATTHONGTIN** được mã hóa thành **MBGORPIYAANTKJVLSHVN**

**Câu 10 (Nguyễn Song Hậu): Cho k = TRUONG, N = 26, giải mã văn bản, dùng thuật mã Vigenere với C = LZKINTMYIBTZBE**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Trước giải mã | L | Z | K | I | N | T | M | Y | I | B | T | Z | B | E |
| K | T | R | U | O | N | G | T | R | U | O | N | G | T | R |
| Sau giải mã | S | I | Q | U | A | N | T | H | O | N | G | T | I | N |

* Vậy **LZKINTMYIBTZBE** được giải mã thành **SIQUANTHONGTIN**