**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

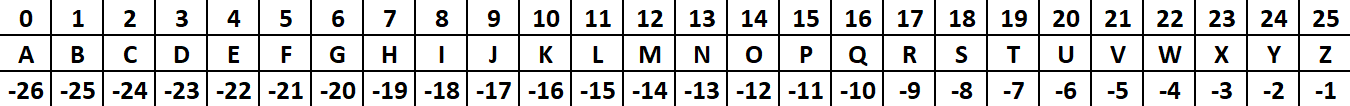
+ Nguyễn Hữu Toàn – 2151050462

+ Nguyễn Y Khoa – 2151500202

**Bài tập thuật mã 1 - Thuật mã Caesar**

ĐỀ BÀI:

1. Cho k = 25, N = 26, mã hóa văn bản, dùng thuật mã Caesar với p = HEDIEUHANH
2. Cho k = 24, N = 26, giải mã văn bản, dùng thuật mã Caesar với C = RGLFMASLEBSLE
3. Cho k = 22, N = 26, giải mã văn bản, dùng thuật mã Caesar với C = WJPKWJDAPDKJCPDKJCPEJ
4. Cho k = 21, N = 26, giải mã văn bản, dùng thuật mã Caesar với C = WVJHVOCZOCJIB
5. Cho k = 19, N = 26, mã hóa văn bản, dùng thuật mã Caesar với p = CONGNGHETHONGTIN
6. Cho k = 25, N = 26, mã hóa văn bản, dùng thuật mã Caesar với p = TRUONGDAIHOCMO
7. Cho k = 24, N = 26, mã hóa văn bản, dùng thuật mã Caesar với p = ANTOANBAOMAT
8. Cho k = 25, N = 26, giải mã văn bản, dùng thuật mã Caesar với C = LZMFLZXSHMG
9. Cho k = 20, N = 26, giải mã văn bản, dùng thuật mã Caesar với C = KOUHNLCGUHA
10. Cho k = 16, N = 26, giải mã văn bản, dùng thuật mã Caesar với C = SEIETKBYUKDQDWSQE



BÀI GIẢI:

Câu 1 (Trần Thanh Hiệp): k = 25, N = 26, p = HEDIEUHANH

|  |  |  |  |
| --- | --- | --- | --- |
| Trước mã hóa | p | C = (p + k) mod N | Sau mã hóa |
| H | 7 | (7 + 25) mod 26 = 6 | G |
| E | 4 | (4 + 25) mod 26 = 3 | D |
| D | 3 | (3 + 25) mod 26 = 2 | C |
| I | 8 | (8 + 25) mod 26 = 7 | H |
| E | 4 | (4 + 25) mod 26 = 3 | D |
| U | 20 | (20 + 25) mod 26 = 19 | T |
| H | 7 | (7 + 25) mod 26 = 6 | G |
| A | 0 | (0 + 25) mod 26 = 25 | Z |
| N | 13 | (13 + 25) mod 26 = 12 | M |
| H | 7 | (7 + 25) mod 26 = 6 | G |

* “HEDIEUHANH” được mã hoá thành “GDCHDTGZMG”

Câu 2 (Trần Thanh Hiệp): k = 24, N = 26, C = RGLFMASLEBSLE

|  |  |  |  |
| --- | --- | --- | --- |
| Trước mã hóa | C | p = (C - k) mod N | Sau mã hóa |
| R | 17 | (17 – 24) mod 26 = 19 | T |
| G | 6 | (6 – 24) mod 26 = 8 | I |
| L | 11 | (11 – 24) mod 26 = 13 | N |
| F | 5 | (5 – 24) mod 26 = 7 | H |
| M | 12 | (12 – 24) mod 26 = 14 | O |
| A | 0 | (0 – 24) mod 26 = 2 | C |
| S | 18 | (18 – 24) mod 26 = 20 | U |
| L | 11 | (11 – 24) mod 26 = 13 | N |
| E | 4 | (4 – 24) mod 26 = 6 | G |
| B | 1 | (1 – 24) mod 26 = 3 | D |
| S | 18 | (18 – 24) mod 26 = 20 | U |
| L | 11 | (11 – 24) mod 26 = 13 | N |
| E | 4 | (4 – 24) mod 26 = 6 | G |

* “RGLFMASLEBSLE” được giải mã thành “TINHOCUNGDUNG”

Câu 3 (Nguyễn Song Hậu): k = 22, N = 26, C = WJPKWJDAPDKJCPDKJCPEJ

|  |  |  |  |
| --- | --- | --- | --- |
| Trước mã hóa | C | p = (C - k) mod N | Sau mã hóa |
| W | 22 | (22 – 22) mod 26 = 0 | A |
| J | 9 | (9 – 22) mod 26 = 13 | N |
| P | 15 | (15 – 22) mod 26 = 19 | T |
| K | 10 | (10 – 22) mod 26 = 14 | O |
| W | 22 | (22 – 22) mod 26 = 0 | A |
| J | 9 | (9 – 22) mod 26 = 13 | N |
| D | 3 | (3 – 22) mod 26 = 7 | H |
| A | 0 | (0 – 22) mod 26 = 4 | E |
| P | 15 | (15 – 22) mod 26 = 19 | T |
| D | 3 | (3 – 22) mod 26 = 7 | H |
| K | 10 | (10 – 22) mod 26 = 14 | O |
| J | 9 | (9 – 22) mod 26 = 13 | N |
| C | 2 | (2 – 22) mod 26 = 6 | G |
| P | 15 | (15 – 22) mod 26 = 19 | T |
| D | 3 | (3 – 22) mod 26 = 7 | H |
| K | 10 | (10 – 22) mod 26 = 14 | O |
| J | 9 | (9 – 22) mod 26 = 13 | N |
| C | 2 | (2 – 22) mod 26 = 6 | G |
| P | 15 | (15 – 22) mod 26 = 19 | T |
| E | 4 | (4 – 22) mod 26 = 8 | I |
| J | 9 | (9 – 22) mod 26 = 13 | N |

* “WJPKWJDAPDKJCPDKJCPEJ” được giải mã thành “ANTOANHETHONGTHONGTIN”

Câu 4 (Nguyễn Song Hậu): k = 21, N = 26, C = WVJHVOCZOCJIB

|  |  |  |  |
| --- | --- | --- | --- |
| Trước mã hóa | C | p = (C - k) mod N | Sau mã hóa |
| W | 22 | (22 – 21) mod 26 = 1 | B |
| V | 21 | (21 – 21) mod 26 = 0 | A |
| J | 9 | (9 – 21) mod 26 = 14 | O |
| H | 7 | (7 – 21) mod 26 = 12 | M |
| V | 21 | (21 – 21) mod 26 = 0 | A |
| O | 14 | (14 – 21) mod 26 = 19 | T |
| C | 2 | (2 – 21) mod 26 = 7 | H |
| Z | 25 | (25 – 21) mod 26 = 4 | E |
| O | 14 | (14 – 21) mod 26 = 19 | T |
| C | 2 | (2 – 21) mod 26 = 7 | H |
| J | 9 | (9 – 21) mod 26 = 14 | O |
| I | 8 | (8 – 21) mod 26 = 13 | N |
| B | 1 | (1 – 21) mod 26 = 6 | G |

* “WVJHVOCZOCJIB” được giải mã thành “BAOMATHETHONG”

Câu 5 (Nguyễn Văn Cảnh): k = 19, N = 26, p = CONGNGHETHONGTIN

|  |  |  |  |
| --- | --- | --- | --- |
| Trước mã hóa | p | C = (p + k) mod N | Sau mã hóa |
| C | 2 | (2 + 19) mod 26 = 21 | V |
| O | 14 | (14 + 19) mod 26 = 7 | H |
| N | 13 | (13 + 19) mod 26 = 6 | G |
| G | 6 | (6 + 19) mod 26 = 25 | Z |
| N | 13 | (13 + 19) mod 26 = 6 | G |
| G | 6 | (6 + 19) mod 26 = 25 | Z |
| H | 7 | (7 + 19) mod 26 = 0 | A |
| E | 4 | (4 + 19) mod 26 = 23 | X |
| T | 19 | (19 + 19) mod 26 = 12 | M |
| H | 7 | (7 + 19) mod 26 = 0 | A |
| O | 14 | (14 + 19) mod 26 =7 | H |
| N | 13 | (13 + 19) mod 26 = 6 | G |
| G | 6 | (6 + 19) mod 26 = 25 | Z |
| T | 19 | (19 + 19) mod 26 = 12 | M |
| I | 8 | (8 + 19) mod 26 = 1 | B |
| N | 13 | (13 + 19) mod 26 = 6 | G |

* “CONGNGHETHONGTIN” được mã hoá thành “VHGZGZAXMAHGZMBG”

Câu 6 (Lê Trí Cường): k = 25, N =26, p = TRUONGDAIHOCMO

|  |  |  |  |
| --- | --- | --- | --- |
| Trước mã hóa | p | C = (p + k) mod N | Sau mã hóa |
| T | 19 | (19 + 25) mod 26 = 18 | S |
| R | 17 | (17 + 25) mod 26 = 16 | Q |
| U | 20 | (20 + 25) mod 26 = 19 | T |
| O | 14 | (14 + 25) mod 26 = 13 | N |
| N | 13 | (13 + 25) mod 26 = 12 | M |
| G | 6 | (6 + 25) mod 26 = 5 | F |
| D | 3 | (3 + 25) mod 26 = 2 | C |
| A | 0 | (0 + 25) mod 26 = 25 | Z |
| I | 8 | (8 + 25) mod 26 = 7 | H |
| H | 7 | (7 + 25) mod 26 = 6 | G |
| O | 14 | (14 + 25) mod 26 = 13 | N |
| C | 2 | (2 + 25) mod 26 = 1 | B |
| M | 12 | (12 + 25) mod 26 = 11 | L |
| O | 14 | (14+25) mod 26 = 13 | N |

* “TRUONGDAIHOCMO” được mã hoá thành “SQTNMFCZHGNBLN”

Câu 7 (Lê Trung Hiếu): k = 24, N = 26, p = ANTOANBAOMAT

|  |  |  |  |
| --- | --- | --- | --- |
| Trước giải mã | p | C = (p + k) mod N | Sau giải mã |
| A | 0 | (0 + 24) mod 26 = 24 | Y |
| N | 13 | (13 + 24) mod 26 = 11 | L |
| T | 19 | (19 + 24) mod 26 = 17 | R |
| O | 14 | (14 + 24) mod 26 = 12 | M |
| A | 0 | (0 + 24) mod 26 = 24 | Y |
| N | 13 | (13 + 24) mod 26 = 11 | L |
| B | 1 | (1 + 24) mod 26 = 1 | Z |
| A | 0 | (0 + 24) mod 26 = 24 | Y |
| O | 14 | (14 + 24) mod 26 = 12 | M |
| M | 12 | (12 + 24) mod 26 = 10 | K |
| A | 0 | (0 + 24) mod 26 = 24 | Y |
| T | 19 | (19 + 24) mod 26 = 17 | R |

* “ANTOANBAOMAT” được mã hoá thành “YLRMYLZYMKYR”

Câu 8 (Nguyễn Y Khoa): k = 25, N = 26, C = LZMFLZXSHMG

|  |  |  |  |
| --- | --- | --- | --- |
| Trước giải mã | C | p = (C - k) mod N | Sau giải mã |
| L | 11 | (11 - 25) mod 26 = 12 | M |
| Z | 25 | (25 - 25) mod 26 = 0 | A |
| M | 12 | (12 - 25) mod 26 = 13 | N |
| F | 5 | (5 - 25) mod 26 = 6 | G |
| L | 11 | (11 - 25) mod 26 = 12 | M |
| Z | 25 | (25 - 25) mod 26 = 0 | A |
| X | 23 | (23 - 25) mod 26 = 24 | Y |
| S | 18 | (18 - 25) mod 26 = 19 | T |
| H | 7 | (7 - 25) mod 26 = 8 | I |
| M | 12 | (12 - 25) mod 26 = 13 | N |
| G | 6 | (6 - 25) mod 26 = 7 | H |

* “LZMFLZXSHMG” được giải mã thành “MANGMAYTINH”

Câu 9 (Bùi Thị Ngân): k = 20, N = 26, C = KOUHNLCGUHA

|  |  |  |  |
| --- | --- | --- | --- |
| Trước giải mã | C | p = (C - k) mod N | Sau giải mã |
| K | 10 | (10 - 20) mod 26 =16 | Q |
| O | 14 | (14 - 20) mod 26 =20 | U |
| U | 20 | (20 - 20) mod 26 =0 | A |
| H | 7 | (7 - 20) mod 26 =13 | N |
| N | 13 | (13 - 20) mod 26 =19 | T |
| L | 11 | (11 - 20) mod 26 =17 | R |
| C | 2 | (2 - 20) mod 26 =8 | I |
| G | 6 | (6 - 20) mod 26 =12 | M |
| U | 20 | (20 - 20) mod 26 =0 | A |
| H | 7 | P= (7 - 20) mod 26 =13 | N |
| A | 0 | P= (0 - 20) mod 26 =6 | G |

* “KOUHNLCGUHA” được giải mã thành “QUANTRIMANG”

Câu 10 (Nguyễn Hữu Toàn): k = 16, N = 26, p = SEIETKBYUKDQDWSQE

|  |  |  |  |
| --- | --- | --- | --- |
| Trước giải mã | C | p = (C - k) mod N | Sau giải mã |
| S | 18 | (18 - 16) mod 26 = 2 | C |
| E | 4 | (4 - 16) mod 26 = 14 | O |
| I | 8 | (8 - 16) mod 26 = 18 | S |
| E | 4 | (4 - 16) mod 26 = 14 | O |
| T | 19 | (19 - 16) mod 26 = 3 | D |
| K | 10 | (10 - 16) mod 26 = 20 | U |
| B | 1 | (1 - 16) mod 26 = 0 | L |
| Y | 24 | (24 - 16) mod 26 = 8 | I |
| U | 20 | (20 - 16) mod 26 = 4 | E |
| K | 10 | (10 - 16) mod 26 = 20 | U |
| D | 3 | (3 - 16) mod 26 =13 | N |
| Q | 16 | (16 - 16) mod 26 = 0 | A |
| D | 3 | (3 - 16) mod 26 = 13 | N |
| W | 22 | (22 - 16) mod 26 = 6 | G |
| S | 18 | (18 - 16) mod 26 = 2 | C |
| Q | 16 | (16 - 16) mod 26 =0 | A |
| E | 4 | (4 - 16) mod 26 =14 | O |

* “SEIETKBYUKDQDWSQE” được giải mã thành “COSODULIEUNANGCAO”