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

**Nhóm 1**

| 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 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

* Để chữ cái **C** mã hóa một chữ cái **p** với khóa **k** và **N** ta có công thức như sau:

**C = (p + k) mod N**

* Tương tự với mã hóa ta có công thức giải mã như sau:

**p = (C – k) mod N**

1. Cho k = 25, N = 26, **mã hóa văn bản**, dùng thuật mã Caesar với

p = HEDIEUHANH

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

**Kết quả mã hóa:** C = GDCHDTGZMG

1. Cho k = 24, N = 26, **giải mã văn bản**, dùng thuật mã Caesar với

C = RGLFMASLEBSLE

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

**Kết quả giải mã:** p = TINHOCUNGDUNG

1. Cho k = 22, N = 26, **giải mã văn bản**, dùng thuật mã Caesar với

C = WJPKWJDAPDKJCPDKJCPEJ

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

**Kết quả giải mã:** p = ANTOANHETHONGTHONGTIN

1. Cho k = 21, N = 26, **giải mã văn bản**, dùng thuật mã Caesar với

C = WVJHVOCZOCJIB

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

**Kết quả giải mã:** p = BAOMATHETHONG

1. Cho k = 19, N = 26, **mã hóa văn bản**, dùng thuật mã Caesar với

p = CONGNGHETHONGTIN

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

**Kết quả mã hóa:** C = VHGZGZAXMAHGZMBG

1. Cho k = 25, N = 26, **mã hóa văn bản**, dùng thuật mã Caesar với

p = TRUONGDAIHOCMO

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

**Kết quả mã hóa:** C = SQTNMFCZHGNBLN

1. Cho k = 24, N = 26, **mã hóa văn bản**, dùng thuật mã Caesar với

p = ANTOANBAOMAT

| **p** | **C = (p + k) mod N** | **C** |
| --- | --- | --- |
| A | (0 + 24) mod 26 = 24 | Y |
| N | (13 + 24) mod 26 = 11 | L |
| T | (19 + 24) mod 26 = 17 | R |
| O | (14 + 24) mod 26 = 12 | M |
| A | (0 + 24) mod 26 = 24 | Y |
| N | (13 + 24) mod 26 = 11 | L |
| B | (1 + 24) mod 26 = 25 | Z |
| A | (0 + 24) mod 26 = 24 | Y |
| O | (14 + 24) mod 26 = 12 | M |
| M | (12 + 24) mod 26 = 10 | K |
| A | (0 + 24) mod 26 = 24 | Y |
| T | (19 + 24) mod 26 = 17 | R |

**Kết quả mã hóa:** C = YLRMYLZYMKYR

1. Cho k = 25, N = 26, **giải mã văn bản**, dùng thuật mã Caesar với

C = LZMFLZXSHMG

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

**Kết quả giải mã:** p = MANGMAYTINH

1. Cho k = 20, N = 26, **giải mã văn bản**, dùng thuật mã Caesar với

C = KOUHNLCGUHA

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

**Kết quả giải mã:** p = QUANTRIMANG

1. Cho k = 16, N = 26, **giải mã văn bản**, dùng thuật mã Caesar với

C = SEIETKBYUKDQDWSQE

| **C** | **p = (C - k) mod N** | **p** |
| --- | --- | --- |
| S | (18 - 16) mod 26 = 2 | C |
| E | (4 - 16) mod 26 = 14 | O |
| I | (8 - 16) mod 26 = 18 | S |
| E | (4 - 16) mod 26 = 14 | O |
| T | (19 - 16) mod 26 = 3 | D |
| K | (10 - 16) mod 26 = 20 | U |
| B | (1 - 16) mod 26 = 11 | L |
| Y | (24 - 16) mod 26 = 8 | I |
| U | (20 - 16) mod 26 = 4 | E |
| K | (10 - 16) mod 26 = 20 | U |
| D | (3 - 16) mod 26 = 13 | N |
| Q | (16 - 16) mod 26 = 0 | A |
| D | (3 - 16) mod 26 = 13 | N |
| W | (22 - 16) mod 26 = 6 | G |
| S | (18 - 16) mod 26 = 2 | C |
| Q | (16 - 16) mod 26 = 0 | A |
| E | (4 - 16) mod 26 = 14 | O |

**Kết quả giải mã:** p = COSODULIEUNANGCAO