**Bài tập thuật mã 2 - Thuật mã Vigenere**

**Nhóm 1**

* Hồ Phan Tấn Khoa
* Trần Minh Bảo Long
* Lê Văn Hiếu
* Phan Minh Thuận
* Trịnh Thanh Hải
* Nguyễn Minh Sang
* Phan Hoàng Triều
* Lê Trương Minh Hoàng

| 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 |

**• 1. Cho k = MAHOA, N = 26, giải mã văn bản, dùng thuật mã Vigenere**

**với C = SIHWMMTOCNSTPB**

| **C** | **S** | **I** | **H** | **W** | **M** | **M** | **T** | **O** | **C** | **N** | **S** | **T** | **P** | **B** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **18** | **08** | **07** | **22** | **12** | **12** | **19** | **14** | **02** | **13** | **18** | **19** | **15** | **01** |
| **k** | **M** | **A** | **H** | **O** | **A** | **M** | **A** | **H** | **O** | **A** | **M** | **A** | **H** | **O** |
|  | **12** | **00** | **07** | **14** | **00** | **12** | **00** | **07** | **14** | **00** | **12** | **00** | **07** | **14** |
| **(C - k) mod N** | **06** | **08** | **00** | **08** | **12** | **00** | **19** | **07** | **14** | **13** | **06** | **19** | **08** | **13** |
| **P** | **G** | **I** | **A** | **I** | **M** | **A** | **T** | **H** | **O** | **N** | **G** | **T** | **I** | **N** |

**Kết quả giải mã:** P = GIAIMATHONGTIN

| 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 |

**• 2. Cho k = KHOA, N = 26, giải mã văn bản, dùng thuật mã Vigenere**

**với  C = DOONRWVOWHBGDLBBKJ**

| **C** | **D** | **O** | **O** | **N** | **R** | **W** | **V** | **O** | **W** | **H** | **B** | **G** | **D** | **L** | **B** | **B** | **K** | **J** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **03** | **14** | **14** | **13** | **17** | **22** | **21** | **14** | **22** | **07** | **01** | **06** | **03** | **11** | **01** | **01** | **10** | **09** |
| **k** | **K** | **H** | **O** | **A** | **K** | **H** | **O** | **A** | **K** | **H** | **O** | **A** | **K** | **H** | **O** | **A** | **K** | **H** |
|  | **10** | **07** | **14** | **00** | **10** | **07** | **14** | **00** | **10** | **07** | **14** | **00** | **10** | **07** | **14** | **00** | **10** | **07** |
| **(C - k) mod N** | **19** | **07** | **00** | **13** | **07** | **15** | **07** | **14** | **12** | **00** | **13** | **06** | **19** | **04** | **13** | **01** | **00** | **02** |
| **P** | **T** | **H** | **A** | **N** | **H** | **P** | **H** | **O** | **M** | **A** | **N** | **G** | **T** | **E** | **N** | **B** | **A** | **C** |

**Kết quả giải mã:** P = THANHPHOMANGTENBAC

| 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 |

**• 3. Cho k = KEY, N = 26, mã hóa văn bản,dùng thuật mã Vigenere**

**với   P = KHOACONGNGHETHONGTIN**

| **P** | **K** | **H** | **O** | **A** | **C** | **O** | **N** | **G** | **N** | **G** | **H** | **E** | **T** | **H** | **O** | **N** | **G** | **T** | **I** | **N** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **10** | **07** | **14** | **00** | **02** | **14** | **13** | **06** | **13** | **06** | **07** | **04** | **19** | **07** | **14** | **13** | **06** | **19** | **08** | **13** |
| **k** | **K** | **E** | **Y** | **K** | **E** | **Y** | **K** | **E** | **Y** | **K** | **E** | **Y** | **K** | **E** | **Y** | **K** | **E** | **Y** | **K** | **E** |
|  | **10** | **04** | **24** | **10** | **04** | **24** | **10** | **04** | **24** | **10** | **04** | **24** | **10** | **04** | **24** | **10** | **04** | **24** | **10** | **04** |
| **(P + k) mod N** | **20** | **11** | **12** | **10** | **06** | **12** | **23** | **10** | **11** | **16** | **11** | **02** | **03** | **11** | **12** | **23** | **10** | **17** | **18** | **17** |
| **C** | **U** | **L** | **M** | **K** | **G** | **M** | **X** | **K** | **L** | **Q** | **L** | **C** | **D** | **L** | **M** | **X** | **K** | **R** | **S** | **R** |

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

| 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 |

**• 4. Cho k = TRUONGDH, N = 26, giải mã văn bản, dùng thuật mã Vigenere**

**với C = WRCVBIPVMGBQZ**

| **C** | **W** | **R** | **C** | **V** | **B** | **I** | **P** | **V** | **M** | **G** | **B** | **Q** | **Z** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **22** | **17** | **02** | **21** | **01** | **08** | **15** | **21** | **12** | **06** | **01** | **16** | **25** |
| **k** | **T** | **R** | **U** | **O** | **N** | **G** | **D** | **H** | **T** | **R** | **U** | **O** | **N** |
|  | **19** | **17** | **20** | **14** | **13** | **06** | **03** | **07** | **19** | **17** | **20** | **14** | **13** |
| **(C - k) mod N** | **03** | **00** | **08** | **07** | **14** | **02** | **12** | **14** | **19** | **15** | **07** | **02** | **12** |
| **P** | **D** | **A** | **I** | **H** | **O** | **C** | **M** | **O** | **T** | **P** | **H** | **C** | **M** |

**Kết quả giải mã:** P = DAIHOCMOTPHCM

| 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 |

**• 5. Cho k = BIMAT, N = 26,  giải mã văn bản, dùng thuật mã Vigenere**

**với  C= LPAADJBTUTUFMYWVVS**

| **C** | **L** | **P** | **A** | **A** | **D** | **J** | **B** | **T** | **U** | **T** | **U** | **F** | **M** | **Y** | **W** | **V** | **V** | **S** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **11** | **15** | **00** | **00** | **03** | **09** | **01** | **19** | **20** | **19** | **20** | **05** | **12** | **24** | **22** | **21** | **21** | **18** |
| **k** | **B** | **I** | **M** | **A** | **T** | **B** | **I** | **M** | **A** | **T** | **B** | **I** | **M** | **A** | **T** | **B** | **I** | **M** |
|  | **01** | **08** | **12** | **00** | **19** | **01** | **08** | **12** | **00** | **19** | **01** | **08** | **12** | **00** | **19** | **01** | **08** | **12** |
| **(C - k) mod N** | **10** | **07** | **14** | **00** | **10** | **08** | **19** | **07** | **20** | **00** | **19** | **23** | **00** | **24** | **03** | **20** | **13** | **06** |
| **P** | **K** | **H** | **O** | **A** | **K** | **I** | **T** | **H** | **U** | **A** | **T** | **X** | **A** | **Y** | **D** | **U** | **N** | **G** |

**Kết quả giải mã:** P = KHOAKITHUATXAYDUNG

| 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 |

**• 6. Cho k = SECRET, N = 26, mã hóa văn bản,dùng thuật mã Vigenere**

**với   P = HETHONGTHONGTIN**

| **P** | **H** | **E** | **T** | **H** | **O** | **N** | **G** | **T** | **H** | **O** | **N** | **G** | **T** | **I** | **N** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **7** | **4** | **19** | **7** | **14** | **13** | **6** | **19** | **7** | **14** | **13** | **6** | **19** | **8** | **13** |
| **k** | **S** | **E** | **C** | **R** | **E** | **T** | **S** | **E** | **C** | **R** | **E** | **T** | **S** | **E** | **C** |
|  | **18** | **04** | **02** | **17** | **04** | **19** | **18** | **04** | **02** | **17** | **04** | **19** | **18** | **04** | **02** |
| **(P + k) mod N** | **25** | **08** | **21** | **24** | **18** | **06** | **24** | **23** | **09** | **05** | **17** | **25** | **11** | **12** | **15** |
| **C** | **Z** | **I** | **V** | **Y** | **S** | **G** | **Y** | **X** | **J** | **F** | **R** | **Z** | **L** | **M** | **P** |

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

| 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 |

**• 7. Cho k = MONARCHY,  N = 26, giải mã văn bản, dùng thuật mã Vigenere**

**với   C = MBAIEJOCFVBNX**

| **C** | **M** | **B** | **A** | **I** | **E** | **J** | **O** | **C** | **F** | **V** | **B** | **N** | **X** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **12** | **01** | **00** | **08** | **04** | **09** | **14** | **02** | **05** | **21** | **01** | **13** | **23** |
| **k** | **M** | **O** | **N** | **A** | **R** | **C** | **H** | **Y** | **M** | **O** | **N** | **A** | **R** |
|  | **12** | **14** | **13** | **00** | **17** | **02** | **07** | **24** | **12** | **14** | **13** | **00** | **17** |
| **(C - k) mod N** | **00** | **13** | **13** | **08** | **13** | **07** | **07** | **04** | **19** | **07** | **14** | **13** | **06** |
| **P** | **A** | **N** | **N** | **I** | **N** | **H** | **H** | **E** | **T** | **H** | **O** | **N** | **G** |

**Kết quả giải mã:** P =ANNINHHETHONG

| 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 |

**• 8. Cho k = SECRET, N = 26, mã hóa văn bản, dùng thuật mã Vigenere**

**với   P = KHOACONGNGHETHONGTIN**

| **P** | **K** | **H** | **O** | **A** | **C** | **O** | **N** | **G** | **N** | **G** | **H** | **E** | **T** | **H** | **O** | **N** | **G** | **T** | **I** | **N** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **10** | **07** | **14** | **00** | **02** | **14** | **13** | **06** | **13** | **06** | **07** | **04** | **19** | **07** | **14** | **13** | **06** | **19** | **08** | **13** |
| **k** | **S** | **E** | **C** | **R** | **E** | **T** | **S** | **E** | **C** | **R** | **E** | **T** | **S** | **E** | **C** | **R** | **E** | **T** | **S** | **E** |
|  | **18** | **04** | **02** | **17** | **04** | **19** | **18** | **04** | **02** | **17** | **04** | **19** | **18** | **04** | **02** | **17** | **04** | **19** | **18** | **04** |
| **(P + k) mod N** | **02** | **11** | **16** | **17** | **06** | **07** | **05** | **10** | **15** | **23** | **11** | **23** | **11** | **11** | **16** | **04** | **10** | **12** | **00** | **17** |
| **C** | **C** | **L** | **Q** | **R** | **G** | **H** | **F** | **K** | **P** | **X** | **L** | **X** | **L** | **L** | **G** | **E** | **K** | **M** | **A** | **R** |

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

| 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 |

**• 9. Cho k = MONARCHY,  N = 26, mã hóa văn bản,dùng thuật mã Vigenere**

**P =      ANTOANBAOMATTHONGTIN**

| **P** | **A** | **N** | **T** | **O** | **A** | **N** | **B** | **A** | **O** | **M** | **A** | **T** | **T** | **H** | **O** | **N** | **G** | **T** | **I** | **N** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **00** | **13** | **19** | **14** | **00** | **13** | **01** | **00** | **14** | **12** | **00** | **19** | **19** | **07** | **14** | **13** | **06** | **19** | **08** | **13** |
| **k** | **M** | **O** | **N** | **A** | **R** | **C** | **H** | **Y** | **M** | **O** | **N** | **A** | **R** | **C** | **H** | **Y** | **M** | **O** | **N** | **A** |
|  | **12** | **14** | **13** | **00** | **17** | **02** | **07** | **24** | **12** | **14** | **13** | **00** | **17** | **02** | **07** | **24** | **12** | **14** | **13** | **00** |
| **(P + k) mod N** | **12** | **01** | **06** | **14** | **17** | **15** | **08** | **24** | **00** | **00** | **13** | **19** | **10** | **09** | **21** | **11** | **18** | **07** | **21** | **13** |
| **C** | **M** | **B** | **G** | **O** | **R** | **P** | **I** | **Y** | **A** | **A** | **N** | **T** | **K** | **J** | **V** | **L** | **S** | **H** | **V** | **N** |

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

| 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 |

**• 10. Cho k = TRUONG, N = 26, giải mã văn bản, dùng thuật mã Vigenere**

**với C = LZKINTMYIBTZBE**

| **C** | **L** | **Z** | **K** | **I** | **N** | **T** | **M** | **Y** | **I** | **B** | **T** | **Z** | **B** | **E** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **11** | **25** | **10** | **08** | **13** | **19** | **12** | **24** | **08** | **01** | **19** | **25** | **01** | **04** |
| **k** | **T** | **R** | **U** | **O** | **N** | **G** | **T** | **R** | **U** | **O** | **N** | **G** | **T** | **R** |
|  | **19** | **17** | **20** | **14** | **13** | **06** | **19** | **17** | **20** | **14** | **13** | **06** | **19** | **17** |
| **(C - k) mod N** | **18** | **08** | **16** | **20** | **00** | **13** | **19** | **07** | **14** | **13** | **06** | **19** | **08** | **13** |
| **P** | **S** | **I** | **Q** | **U** | **A** | **N** | **T** | **H** | **O** | **N** | **G** | **T** | **I** | **N** |

**Kết quả giải mã:** P = SIQUANTHONGTIN