**Bài tập thuật mã 6 - Thuật mã Hill**

**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 bản rõ “THEGIOIDODAY” khóa k là ma trận cấp 2 sau:**

**7 2**

**3 3**

**Mã hóa bản rõ trên với khóa k theo hệ mã Hill tìm bản rõ ? Biết hàm mã hóa y = kx**

| **P =** | **T** | **H** | **E** | **G** | **I** | **O** | **I** | **D** | **O** | **D** | **A** | **Y** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **19** | **7** | **4** | **6** | **8** | **14** | **8** | **3** | **14** | **3** | **0** | **24** |

| **k** |  | **x = TH** | **x = EG** | **x = IO** | **x = ID** | **x = OD** | **x = AY** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **7** | **2** | **19** | **4** | **8** | **8** | **14** | **0** |
| **3** | **3** | **7** | **6** | **14** | **3** | **3** | **24** |
| **y = kx** |  | **17 = R** | **14 = O** | **6 = G** | **10 = K** | **0 = A** | **22 = W** |
| **y = kx** |  | **0 = A** | **4 = E** | **14 = O** | **7 = H** | **25 = Z** | **20 = U** |

**Kết quả mã hóa: C = RAOEGOKHAZWU**

| 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 bản rõ “VINHHALONG” khóa k là:**

**9 7**

**3 4**

**Mã hóa bản rõ với khóa k theo hệ mã Hill tìm bản mã ? Biết hàm mã**

**y = kx**

| **P =** | **V** | **I** | **N** | **H** | **H** | **A** | **L** | **O** | **N** | **G** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **21** | **8** | **13** | **7** | **7** | **0** | **11** | **14** | **13** | **6** |

| **k** |  | **x = VI** | **x = NH** | **x = HA** | **x = LO** | **x = NG** |
| --- | --- | --- | --- | --- | --- | --- |
| **9** | **7** | **21** | **13** | **7** | **11** | **13** |
| **3** | **4** | **8** | **7** | **0** | **14** | **6** |
| **y = kx** |  | **11 = L** | **10 = K** | **11 = L** | **15 = P** | **3 = D** |
| **y = kx** |  | **17 = R** | **15 = P** | **21 = V** | **11 = L** | **11 = L** |

**Kết quả mã hóa: C = LRKPLVPLDL**

| 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 bản mã “BKIVAIWO” khóa k là ma trận cấp 2 sau:**

**7 2**

**3 3**

**Giải mã bản mã với khóa k theo hệ mã Hill tìm bản rõ ? Biết hàm mã hóa y = xk**

Det(k) = (7\*3 - 3\*2) = 15

GCD(15, 26) = 1 => Có nghịch đảo của Det(k) theo modulo 26

(Det(k))(-1) = 7

**k(-1) = (Det(k))(-1) \* ma trận phụ hợp của k**

|  | **(Det(k))(-1)** | **ma trận phụ hợp k** | |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **k(-1) =** | **7** | **3** | **-2** | **=** | **21** | **12** |
| **-3** | **7** | **5** | **23** |

| **C =** | **B** | **K** | **I** | **V** | **A** | **I** | **W** | **O** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **1** | **10** | **8** | **21** | **0** | **8** | **22** | **14** |

| **x =** | **B** | **K** | **I** | **V** | **A** | **I** | **W** | **O** | **k(-1)** |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **1** | **10** | **8** | **21** | **0** | **8** | **22** | **14** | **21** | **12** |
|  |  |  |  |  |  |  |  |  | **5** | **23** |
| **y = xk** | **19** | **8** | **13** | **7** | **14** | **2** | **12** | **14** |  |  |
|  | **T** | **I** | **N** | **H** | **O** | **C** | **M** | **O** |  |  |

**Kết quả giải mã: P = TINHOCMO**

| 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 bản mã “KS” khóa k là ma trận cấp 2 sau:**

**3 4**

**1 3**

**Hãy giải mã bản mã với khóa k theo hệ mã Hill tìm bản rõ . Biết hàm mã hóa y = kx**

Det(k) = (3\*3 - 1\*4) = 5

GCD(5, 26) = 1 => Có nghịch đảo của Det(k) theo modulo 26

(Det(k))(-1) = -5 + 26 = 21

**k(-1) = (Det(k))(-1) \* ma trận phụ hợp của k**

|  | **(Det(k))(-1)** | **ma trận phụ hợp k** | |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **k(-1) =** | **21** | **3** | **-4** | **=** | **11** | **20** |
| **-1** | **3** | **5** | **11** |

| **C =** | **K** | **S** |
| --- | --- | --- |
|  | **10** | **18** |

| **k(-1)** |  | **x = KS** |
| --- | --- | --- |
| **11** | **20** | **10** |
| **5** | **11** | **18** |
| **y = kx** |  | **2 = C** |
| **y = kx** |  | **14 = O** |

**Kết quả giải mã: P =** CO

| 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 bản mã “KDIY” khóa k là ma trận cấp 2 sau:**

**8 3**

**5 3**

**Giải mã bản mã với khóa k theo hệ mã Hill sẽ tìm bản rõ ? Biết hàm mã hóa y = kx**

Det(k) = (8\*3 - 5\*3) = 9

GCD(9, 26) = 1 => Có nghịch đảo của Det(k) theo modulo 26

(Det(k))(-1) = 3

**k(-1) = (Det(k))(-1) \* ma trận phụ hợp của k**

|  | **(Det(k))(-1)** | **ma trận phụ hợp k** | |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **k(-1) =** | **3** | **3** | **-3** | **=** | **9** | **17** |
| **-5** | **8** | **11** | **24** |

| **C =** | **K** | **D** | **I** | **Y** |
| --- | --- | --- | --- | --- |
|  | **10** | **3** | **8** | **24** |

| **k(-1)** |  | **x = KD** | **x = IY** |
| --- | --- | --- | --- |
| **9** | **17** | **10** | **8** |
| **11** | **24** | **3** | **24** |
| **y = kx** |  | **11 = L** | **12 = M** |
| **y = kx** |  | **0 = A** | **14 = O** |

**Kết quả giải mã: P =** LAMO

| 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 bản mã “CNPZIEQN” khóa k là:**

**6 5**

**3 4**

**Giải mã với khóa k theo hệ mã Hill tìm bản rõ ? Biết hàm mã y = kx**

Det(k) = (6\*4 - 3\*5) = 9

GCD(9, 26) = 1 => Có nghịch đảo của Det(k) theo modulo 26

(Det(k))(-1) = 3

**k(-1) = (Det(k))(-1) \* ma trận phụ hợp của k**

|  | **(Det(k))(-1)** | **ma trận phụ hợp k** | |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **k(-1) =** | **3** | **4** | **-5** | **=** | **12** | **11** |
| **-3** | **6** | **17** | **18** |

| **C =** | **C** | **N** | **P** | **Z** | **I** | **E** | **Q** | **N** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **2** | **13** | **15** | **25** | **8** | **4** | **16** | **13** |

| **k(-1)** |  | **x = CN** | **x = PZ** | **x = IE** | **x = QN** |
| --- | --- | --- | --- | --- | --- |
| **12** | **11** | **2** | **15** | **8** | **16** |
| **17** | **18** | **13** | **25** | **4** | **13** |
| **y = kx** |  | **11 = L** | **13 = N** | **10 = K** | **23 = X** |
| **y = kx** |  | **8 = I** | **3 = D** | **0 = A** | **12 = M** |

**Kết quả giải mã: P =** LINDKAXM

| 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 bản mã “COSLSLCZ” khóa k là:**

**6 5**

**3 4**

**Giải mã với khóa k theo hệ mã Hill tìm bản rõ ? Biết hàm mã y = xk**

Det(k) = (6\*4 - 3\*5) = 9

GCD(9, 26) = 1 => Có nghịch đảo của Det(k) theo modulo 26

(Det(k))(-1) = 3

**k(-1) = (Det(k))(-1) \* ma trận phụ hợp của k**

|  | **(Det(k))(-1)** | **ma trận phụ hợp k** | |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **k(-1) =** | **3** | **4** | **-5** | **=** | **12** | **11** |
| **-3** | **6** | **17** | **18** |

| **C =** | **C** | **O** | **S** | **L** | **S** | **L** | **C** | **Z** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **2** | **14** | **18** | **11** | **18** | **11** | **2** | **25** |

| **x =** | **C** | **O** | **S** | **L** | **S** | **L** | **C** | **Z** | **k(-1)** |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **2** | **14** | **18** | **11** | **18** | **11** | **2** | **25** | **12** | **11** |
|  |  |  |  |  |  |  |  |  | **17** | **18** |
| **y = xk** | **2** | **14** | **13** | **6** | **13** | **6** | **7** | **4** |  |  |
|  | **C** | **O** | **N** | **G** | **N** | **G** | **H** | **E** |  |  |

**Kết quả giải mã: P = CONGNGHE**

| 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 bản mã “RZCDPA” khóa k là:**

**9 7**

**3 4**

**Thực hiện giải mã với khóa k theo hệ mã Hill tìm bản rõ ? Biết hàm mã y = xk**

Det(k) = (9\*4 - 3\*7) = 15

GCD(15, 26) = 1 => Có nghịch đảo của Det(k) theo modulo 26

(Det(k))(-1) =

**k(-1) = (Det(k))(-1) \* ma trận phụ hợp của k**

|  | **(Det(k))(-1)** | **ma trận phụ hợp k** | |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **k(-1) =** | **7** | **4** | **-7** | **=** | **2** | **3** |
| **-3** | **9** | **5** | **11** |

| **C =** | **R** | **Z** | **C** | **D** | **P** | **A** |
| --- | --- | --- | --- | --- | --- | --- |
|  | **17** | **25** | **2** | **3** | **15** | **0** |

| **x =** | **R** | **Z** | **C** | **D** | **P** | **A** | **k(-1)** |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **17** | **25** | **2** | **3** | **15** | **0** | **2** | **3** |
|  |  |  |  |  |  |  | **5** | **11** |
| **y = xk** | **3** | **14** | **19** | **13** | **4** | **19** |  |  |
|  | **D** | **O** | **T** | **N** | **E** | **T** |  |  |

**Kết quả giải mã: P = DOTNET**

| 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 bản mã “RMKCEJVI” khóa k là ma trận cấp 2 sau:**

**8 3**

**5 3**

**Giải mã với khóa k theo hệ mã Hill tìm bản rõ ? Biết hàm mã y = xk**

Det(k) = (8\*3 - 5\*3) = 9

GCD(9, 26) = 1 => Có nghịch đảo của Det(k) theo modulo 26

(Det(k))(-1) = 3

**k(-1) = (Det(k))(-1) \* ma trận phụ hợp của k**

|  | **(Det(k))(-1)** | **ma trận phụ hợp k** | |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **k(-1) =** | **3** | **3** | **-3** | **=** | **9** | **17** |
| **-5** | **8** | **11** | **24** |

| **C =** | **R** | **M** | **K** | **C** | **E** | **J** | **V** | **I** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **17** | **12** | **10** | **2** | **4** | **9** | **21** | **8** |

| **x =** | **R** | **M** | **K** | **C** | **E** | **J** | **V** | **I** | **k(-1)** |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **17** | **12** | **10** | **2** | **4** | **9** | **21** | **8** | **9** | **17** |
|  |  |  |  |  |  |  |  |  | **11** | **24** |
| **y = xk** | **25** | **5** | **8** | **10** | **5** | **24** | **17** | **3** |  |  |
|  | **Z** | **F** | **I** | **K** | **F** | **Y** | **R** | **D** |  |  |

**Kết quả giải mã: P = ZFIKFYRD**

| **k(-1)** |  | **x = RM** | **x = KC** | **x = EJ** | **x = VI** |
| --- | --- | --- | --- | --- | --- |
| **9** | **17** | **17** | **10** | **4** | **21** |
| **11** | **24** | **12** | **2** | **9** | **8** |
| **y = kx** |  | **19 = T** | **20 = U** | **7 = H** | **13 = N** |
| **y = kx** |  | **7 = H** | **2 = C** | **0 = A** | **7 = H** |

**Kết quả giải mã: P = THUCHANH**

| 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 bản mã “PJLXZYHO” khóa k là ma trận cấp 2 sau:**

**19 3**

**5 24**

**Giải mã với khóa k theo hệ mã Hill tìm bản rõ ? Biết hàm mã y = kx**

Det(k) = (19\*24 - 5\*3) = 441

GCD(441, 26) = 1 => Có nghịch đảo của Det(k) theo modulo 26

(Det(k))(-1) = -1

**k(-1) = (Det(k))(-1) \* ma trận phụ hợp của k**

|  | **(Det(k))(-1)** | **ma trận phụ hợp k** | |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **k(-1) =** | **-1** | **24** | **-3** | **=** | **2** | **3** |
| **-5** | **19** | **5** | **7** |

| **C =** | **P** | **J** | **L** | **X** | **Z** | **Y** | **H** | **O** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **15** | **9** | **11** | **23** | **25** | **24** | **7** | **14** |

| **k(-1)** |  | **x = PJ** | **x = LX** | **x = ZY** | **x = HO** |
| --- | --- | --- | --- | --- | --- |
| **2** | **3** | **15** | **11** | **25** | **7** |
| **5** | **7** | **9** | **23** | **24** | **14** |
| **y = kx** |  | **5 = F** | **13 = N** | **18 = S** | **4 = E** |
| **y = kx** |  | **8 = I** | **8 = I** | **7 = H** | **3 = D** |

**Kết quả giải mã: P =** FINISHED