**Bài tập thuật mã - Ôn tập**

**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

•1. Người A,B chọn 2 số nguyên tố chung là g=2 , p = 997, a=47, b= 43. Tính khóa công khai, khóa riêng của người gửi và người nhận A, B theo thuật mã Diffie-Hellman ?

g=2 , p = 997, a=47, b= 43

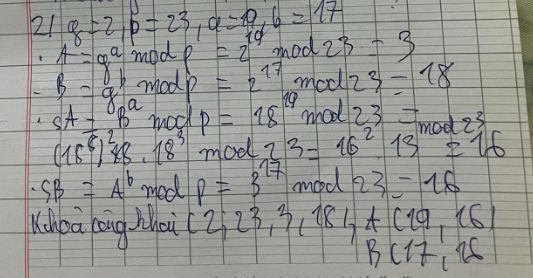
A = ga mod p = 247 mod 997 = 135

B= gb mod p = 243 mod 997 = 320

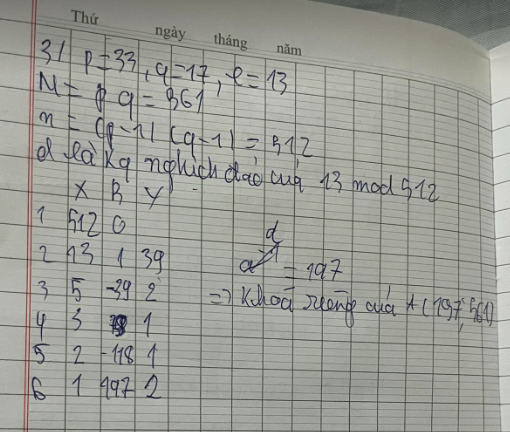
SA = ba mod p = 32047 mod 997 = 370

SB = Ab mod p = 13543 mod 997 = 370

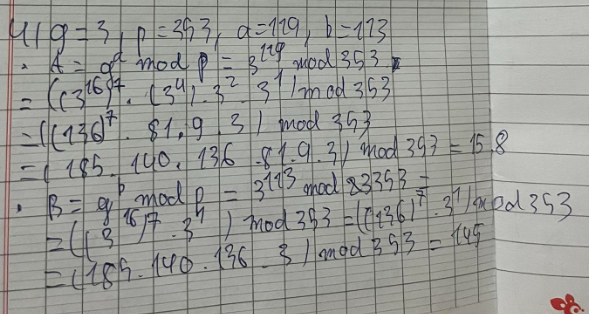
•2. Người A,B chọn 2 số nguyên tố chung là g=2 , p = 23, a=19, b=17. Tính khóa công khai, khóa riêng của người gửi và người nhận A, B theo thuật mã Diffie-Hellman ?

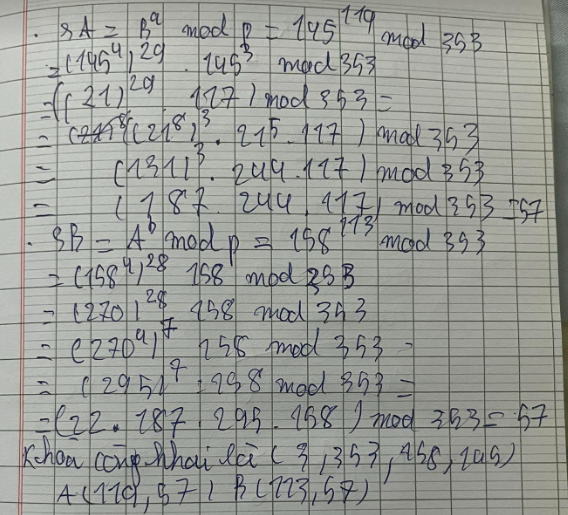


•3. Theo thuật mã Diffie-Hellman. Giả sử người A chọn các thông số p =33, q =17, e = 13. Hỏi cặp khóa riêng của A là gì?

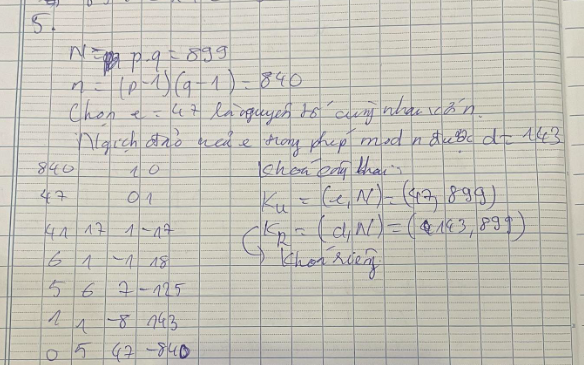


•4. Theo thuật mã Diffie-Hellman, giả sử Alice & Bob chọn 2 số nguyên tố chung là g = 3, p = 353, với a=119, b=113 . Khóa riêng của Alice & Bob là ?

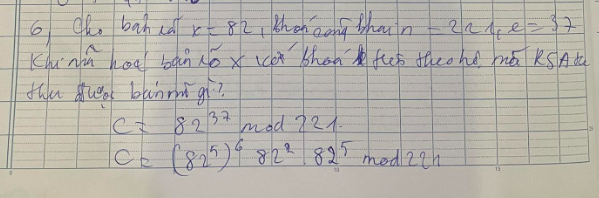


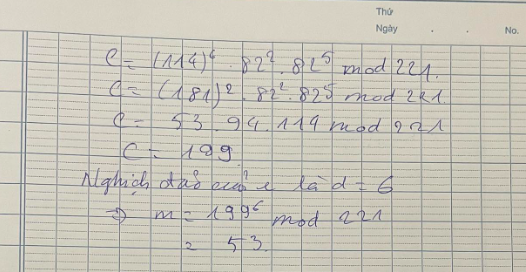


•5. Cho bản mã y = 97, khóa riêng là p =31, q= 29, e =47. Khi giải mã bản mã y theo hệ RSA ta sẽ thu được bản rõ nào ?



•6.Cho bản rõ x = 82, khóa công khai n = 221, e = 37. Khi mã hóa bản rõ x với khóa trên theo hệ mã RSA ta sẽ thu được bản mã gì ?





•7. Cho bản mã “VPTLJXAMJWVFKUBLJ” khóa k là “CITY”. Khi giải mã bản mã trên với khóa k theo hệ mã Vigenere ta sẽ thu được bản rõ nào?

| 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 |

| **C** | **V** | **P** | **T** | **L** | **J** | **X** | **A** | **M** | **J** | **W** | **V** | **F** | **K** | **U** | **B** | **L** | **J** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **21** | **15** | **19** | **11** | **9** | **23** | **0** | **12** | **9** | **22** | **21** | **5** | **10** | **20** | **1** | **11** | **9** |
| **k** | **C** | **I** | **T** | **Y** | **C** | **I** | **T** | **Y** | **C** | **I** | **T** | **Y** | **C** | **I** | **T** | **Y** | **C** |
|  | **2** | **8** | **19** | **24** | **2** | **8** | **19** | **24** | **2** | **8** | **19** | **24** | **2** | **8** | **19** | **24** | **2** |
| **(C - k) mod N** | **19** | **7** | **0** | **13** | **7** | **15** | **7** | **14** | **07** | **14** | **2** | **7** | **8** | **12** | **8** | **13** | **7** |
| **P** | **T** | **H** | **A** | **N** | **H** | **P** | **H** | **O** | **H** | **O** | **C** | **H** | **I** | **M** | **I** | **N** | **H** |

**Kết quả giải mã:** P = THANH PHO HO CHI MINH

•8. Cho bản mã “YIVNQLTDF” khóa k là (23,29).Khi giải mã bản mã trên với khóa k theo hệ mã Affine ta sẽ thu được bản rõ ?.

| 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 |

**a = 23, b = 29**

**Ta có a^(-1) là nghịch đảo của a theo modulo n:**

**a\*a^(-1) mod 26 = 1 => a^(-1) = -9 + 26 = 17**

| **C =** | **Y** | **I** | **V** | **N** | **Q** | **L** | **T** | **D** | **F** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **x =** | **24** | **8** | **21** | **13** | **16** | **11** | **19** | **3** | **5** |
| **a^(-1)(x-b) mod 26** | **19** | **7** | **20** | **14** | **13** | **06** | **12** | **0** | **08** |
| **P =** | **T** | **H** | **U** | **O** | **N** | **G** | **M** | **A** | **I** |

**Kết quả giải mã: P = THUONG MAI**

•9. Cho bản mã “SKRQCFPDRN” khóa k là MONARCHY. Khi giải mã bản mã trên với khóa k theo hệ mã Playfair ta sẽ thu được bản rõ gì ?

| **M** | **O** | **N** | **A** | **R** |
| --- | --- | --- | --- | --- |
| **C** | **H** | **Y** | **B** | **D** |
| **E** | **F** | **G** | **I/J** | **K** |
| **L** | **P** | **Q** | **S** | **T** |
| **U** | **V** | **W** | **X** | **Z** |

| **C =** | **S** | **K** | **R** | **Q** | **C** | **F** | **P** | **D** | **R** | **N** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **P =** | **T** | **I** | **N** | **T** | **H** | **E** | **T** | **H** | **A** | **O** |

**Kết quả giải mã: P = TIN THE THAO**

•10. Cho bản mã “KRPKANHKPKKNUNOM” khóa k:

6 5

3 4

Khi giải mã với khóa k theo hệ mã Hill ta sẽ thu được bản rõ nào ? Biết hàm mã y=kx ?

| 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 |

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 =** | **K** | **R** | **P** | **K** | **A** | **N** | **H** | **K** | **P** | **K** | **K** | **N** | **U** | **N** | **O** | **M** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **10** | **17** | **15** | **10** | **0** | **13** | **7** | **10** | **15** | **10** | **10** | **13** | **20** | **13** | **14** | **12** |

| **k(-1)** |  | **KR** | **PK** | **AN** | **HK** | **PK** | **KN** | **UN** | **OM** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **12** | **11** | **10** | **15** | **0** | **7** | **15** | **10** | **20** | **14** |
| **17** | **18** | **17** | **10** | **13** | **10** | **10** | **13** | **13** | **12** |
| **y = kx** |  | **21** | **4** | **13** | **12** | **4** | **3** | **19** | **14** |
| **y = kx** |  | **8** | **19** | **0** | **13** | **19** | **14** | **2** | **12** |

**Kết quả giải mã: P =** VIETNAMNET DOTCOM

•11. Theo thuật mã Diffie-Hellman, giả sử A & B chọn 2 số nguyên tố chung là g = 2, p = 997, với a=131, b=151 . Tính khóa công khai, khóa riêng của của A & B ?

Bài làm:

A = ga mod P = 2131 mod 997

= 9964 \* 23 mod 997 = 398

B = gb mod P = 2151 mod 997

= 15

SA = ba mod P = 15131 mod 997 = 249

SB = Ab mod P = 249151 mod 997

= 406

Khóa công khai (2,997,398,15)

A(398,406)

B(15, 406)

•12. Người A chọn các thông số p =31, q =37, e = 119. Theo thuật mã RSA hỏi cặp khóa riêng và khóa công khai của A là gì ? Trong trường hợp nhận được bản mã là 1091, hãy tìm bản rõ ?

p =31, q =37, e = 119,c=1091,P=?

N=p\*q = 31\*37=1080

n=(p-1)\*(q-1) = 1147

D = e-1 mod n = 119-1 mod 1080 = 1080 – 481 = 599

| X | B | Y |
| --- | --- | --- |
| 1080 | 0 |  |
| 119 | 1 | 9 |
| 9 | -9 | 13 |
| 2 | 118 | 4 |
| 1 | -481 | 2 |

Kr=(d,N) = (599,1147)

Kc=(e,N)=(119,1147)

M=cd mod N = 1091599 mod 1147

= (10913 mod 1147)199 \* 10192 mod 1147

=( 1020199 mod 1147)66 \*1102 mod 1147 \* 842

= 6675 mod 1147 \*(1062 \* 461) mod 1147

= 6673 mod 1147 \* 6672 mod 1147 \* 960 mod 1147

=(593 \* 100 \* 960) mod 1147 = 960

•13. Cho bản mã “CLGSKOOUOUISOCSHBERU” khóa k là "CITY". Khi giải mã bản mã trên với khóa k theo hệ mã Playfair ta sẽ thu được bản rõ gì ?

| **C** | **I/J** | **T** | **Y** | **A** |
| --- | --- | --- | --- | --- |
| **B** | **D** | **E** | **F** | **G** |
| **H** | **K** | **L** | **M** | **N** |
| **O** | **P** | **Q** | **R** | **S** |
| **U** | **V** | **W** | **X** | **Z** |

| **C =** | **C** | **L** | **G** | **S** | **K** | **O** | **O** | **U** | **O** | **U** | **I** | **S** | **O** | **C** | **S** | **H** | **B** | **E** | **R** | **U** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **P =** | **T** | **H** | **A** | **N** | **H** | **P** | **H** | **O** | **H** | **O** | **A** | **P** | **H** | **U** | **O** | **N** | **G** | **D** | **O** | **X** |

**Kết quả giải mã: P = THANH PHO HOA PHUONG DO X**

•14. Cho bản mã “FJTQCQJCZHOIQM” khóa k:

19 3

5 24

Khi giải mã với khóa k theo hệ mã Hill ta sẽ thu được bản rõ nào ? Biết hàm mã y=xk

| 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 |

Det(k) = (19\*24 -3\*5) = 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 =** | **F** | **J** | **T** | **Q** | **C** | **Q** | **J** | **C** | **Z** | **H** | **O** | **I** | **Q** | **M** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **5** | **9** | **19** | **16** | **2** | **16** | **9** | **2** | **25** | **7** | **14** | **8** | **16** | **12** |

| **x =** | **F** | **J** | **T** | **Q** | **C** | **Q** | **J** | **C** | **Z** | **H** | **O** | **I** | **Q** | **M** | **k(-1)** |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **5** | **9** | **19** | **16** | **2** | **16** | **9** | **2** | **25** | **7** | **14** | **8** | **16** | **12** | **2** | **3** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | **5** | **7** |
| **y = xk** | **3** | **0** | **14** | **13** | **6** | **14** | **2** | **15** | **7** | **20** | **16** | **20** | **14** | **2** |  |  |

**Kết quả giải mã: P = DAO NGOC PHU QUOC**

•15. Cho bản mã “FPBDCFDJIZUJTSKEIZGS” khóa k:

19 3

5 24

Khi giải mã với khóa k theo hệ mã Hill ta sẽ thu được bản rõ nào ? Biết hàm mã y=kx

| 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 |

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 =** | **F** | **P** | **B** | **D** | **C** | **F** | **D** | **J** | **I** | **Z** | **U** | **J** | **T** | **S** | **K** | **E** | **I** | **Z** | **G** | **S** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **5** | **15** | **1** | **3** | **2** | **5** | **3** | **9** | **8** | **25** | **20** | **9** | **19** | **18** | **10** | **4** | **8** | **25** | **6** | **18** |

| **k(-1)** |  | **FP** | **BD** | **CF** | **DJ** | **IZ** | **UJ** | **TS** | **KE** | **IZ** | **GS** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **2** | **3** | **5** | **1** | **2** | **3** | **8** | **20** | **19** | **10** | **8** | **6** |
| **5** | **7** | **15** | **3** | **5** | **9** | **25** | **9** | **18** | **4** | **25** | **18** |
| **y = kx** |  | **3** | **11** | **19** | **7** | **13** | **15** | **14** | **6** | **13** | **14** |
| **y = kx** |  | **0** | **0** | **19** | **0** | **7** | **7** | **13** | **0** | **7** | **0** |

**Kết quả giải mã: P =** DA LAT THANH PHO NGAN HOA

•16. Cho bản mã “SOLUJHDWQMFYJHNAHA” khóa k:

6 5

3 4

Khi giải mã với khóa k theo hệ mã Hill ta sẽ thu được bản rõ nào ? Biết hàm mã y=xk?

| 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 |

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 =** | **S** | **O** | **L** | **U** | **J** | **H** | **D** | **W** | **Q** | **M** | **F** | **Y** | **J** | **H** | **N** | **A** | **H** | **A** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **18** | **14** | **11** | **20** | **9** | **7** | **3** | **22** | **16** | **12** | **5** | **24** | **9** | **7** | **13** | **0** | **7** | **0** |

| **x =** | **S** | **O** | **L** | **U** | **J** | **H** | **D** | **W** | **Q** | **M** | **F** | **Y** | **J** | **H** | **N** | **A** | **H** | **A** | **k(-1)** |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **18** | **14** | **11** | **20** | **9** | **7** | **3** | **22** | **16** | **12** | **5** | **24** | **9** | **7** | **13** | **0** | **7** | **0** | **12** | **11** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | **17** | **18** |
| **y = xk** | **12** | **8** | **4** | **13** | **19** | **17** | **20** | **13** | **6** | **2** | **0** | **19** | **19** | **17** | **0** | **13** | **6** | **25** |  |  |

**Kết quả giải mã: P = MIEN TRUNG CAT TRANG Z**

•17.Cho k = 25, N = 26, giải mã văn bản, dùng thuật mã Caesar:

với C = BZBDLBNFZMFNMSZO

| 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 |

| **C** | **p = (C - k) mod N** | **p** |
| --- | --- | --- |
| B | 2 | C |
| Z | 0 | A |
| B | 2 | C |
| D | 4 | E |
| L | 12 | M |
| B | 2 | C |
| N | 14 | O |
| F | 6 | G |
| Z | 0 | A |
| M | 13 | N |
| F | 6 | G |
| N | 14 | O |
| M | 13 | N |
| S | 19 | T |
| Z | 0 | A |
| O | 15 | P |

**Kết quả giải mã:** p = CAC EM CO GANG ON TAP

•18.Cho k = 23, N = 26, giải mã văn bản, dùng thuật mã Caesar:

với C = QEFAXQHBQNRX

| 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 |

| **C** | **p = (C - k) mod N** | **p** |
| --- | --- | --- |
| Q | 19 | T |
| E | 7 | H |
| F | 8 | I |
| A | 3 | D |
| X | 0 | A |
| Q | 19 | T |
| H | 10 | K |
| B | 4 | E |
| Q | 19 | T |
| N | 16 | Q |
| R | 20 | U |
| X | 0 | A |

**Kết quả giải mã:** p = THI DAT KET QUA

•19.Cho k = 24, N = 26, giải mã văn bản, dùng thuật mã Caesar:

với C = AFSAAYACKRFYLFAMLE

| 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 |

| **C** | **p = (C - k) mod N** | **p** |
| --- | --- | --- |
| A | 2 | C |
| F | 7 | H |
| S | 20 | U |
| A | 2 | C |
| A | 2 | C |
| Y | 0 | A |
| A | 2 | C |
| C | 4 | E |
| K | 12 | M |
| R | 19 | T |
| F | 7 | H |
| Y | 0 | A |
| L | 13 | N |
| F | 7 | H |
| A | 2 | C |
| M | 14 | O |
| L | 13 | N |
| E | 6 | G |

**Kết quả giải mã:** p = CHUC CAC EM THANH CONG

•20. Cho k = 19, N = 26, giải mã văn bản, dùng thuật mã Caesar:

với C = ZHHWURXTGWLXXRHN

| 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 |

| **C** | **p = (C - k) mod N** | **p** |
| --- | --- | --- |
| Z | 6 | G |
| H | 14 | O |
| H | 14 | O |
| W | 3 | D |
| U | 1 | B |
| R | 24 | Y |
| X | 4 | E |
| T | 0 | A |
| G | 13 | N |
| W | 3 | D |
| L | 18 | S |
| X | 4 | E |
| X | 4 | E |
| R | 24 | Y |
| H | 14 | O |
| N | 20 | U |

**Kết quả giải mã:** p = GOOD BYE AND SEE YOU