•1. Cho k = (11,6), N = 26, giải mã văn bản, dùng thuật mã Affine:

 với C = CETUTUFYPFGTIYI

* Trong bảng mã ABC...XYZ, ta có N=26
* Văn bản gốc được chuyển thành dãy số [ 2, 4, 19, 20, 19, 20, 5, 24, 15, 5, 6, 19, 8, 24, 8]
* Áp dụng thuật toán mở rộng  Euclide ta có:

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | B | Y |
| 1 | 26 | 0 |  |
| 2 | 11 | 1 | 2 |
| 3 | 4 | -2 | 2 |
| 4 | 3 | 5 | 1 |
| 5 | 1 | -7 | 3 |

* B5 = -7 => a-1= (-7 + 26 ) mode 26 = 19
* k = (11,6), N = 26 => ta có a=11, b=6 , x là số tương ứng trên bản rõ, y là từng số tương ứng trên bản mã.
* C = CETUTUFYPFGTIYI, bản mã này được chuyển thành dãy số [2, 4, 19, 20, 19, 20, 5, 24, 15, 5, 6, 19, 8, 24, 8]
* Áp dụng hàm giải mã ta có: x = a-1 \*(y-b)\*(mod 26) => x = 19\*(y-6)\*(mod 26), ta được dãy số tương ứng: [2, 14, 13, 6, 13, 6, 7, 4, 15, 7, 0, 13, 12, 4, 12]  
  => Ta có văn bản gốc là : CONGNGHEPHANMEM

•2. Cho k = (17,12), N = 26, mã hóa văn bản, dùng thuật mã Affine:

 với  P = CONGNGHETHONGTIN

* k = (17,12), N = 26 => ta có a=17, b=12 , x là số tương ứng trên bản rõ, y là từng số tương ứng trên bản mã.
* P = CONGNGHETHONGTIN, bản mã này được chuyển thành dãy số [2, 14, 13, 6, 13, 6, 7, 4, 19, 7, 14, 13, 6, 19, 8, 13]
* Áp dụng hàm mã hóa E(x) = (17\*x + 12) mod 26 ta được dãy số tương ứng: [20, 16, 25, 10, 25, 10, 1, 2, 23, 1, 16, 25, 10, 23, 18, 25]  
  => Chuyển dãy số này về dạng ABC, văn bản đã mã hóa là : UQZKZKBCXBQZKXSZ.

•3. Cho k = (21,17), N = 26, mã hóa văn bản,dùng thuật mã Affine

với P = TRUONGDAIHOCMO

* k = (21, 17), N = 26 => ta có a=21, b=17 , x là số tương ứng trên bản rõ, y là từng số tương ứng trên bản mã.
* P = TRUONGDAIHOCMO, bản mã này được chuyển thành dãy số [19, 17, 20, 14, 13, 6, 3, 0, 8, 7, 14, 2, 12, 14]
* Áp dụng hàm mã hóa y= (21\*x + 17) mod 26 ta được dãy số tương ứng: [0, 10, 21, 25, 4, 13, 2, 17, 3, 8, 25, 7, 9, 25]  
  => Chuyển dãy số này về dạng ABC, văn bản đã mã hóa là : AKVZENCRDIZHJZ.

•4. Cho k = (25,29),  N = 26, giải mã văn bản, dùng thuật mã Affine:

C =      APWPDGJSFDQW

* Trong bảng mã ABC...XYZ, ta có N=26
* Văn bản gốc được chuyển thành dãy số [0, 15, 22, 15, 3, 6, 9, 18, 5, 3, 16, 22]
* Áp dụng thuật toán mở rộng  Euclide ta có:

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | B | Y |
| 1 | 26 | 0 |  |
| 2 | 25 | 1 | 1 |
| 3 | 1 | -1 | 25 |

B3 = -1 => a-1= 25

=> Vậy nghịch đảo của 25 theo module 26 là 25

* Với từng dãy số x trong C ta có hàm giải mã :                                                          D(x)= a-1(x-b) mod 26 = 25\*(x-29) mod 26 ta được dãy số [3, 14, 7, 14, 0, 23, 20, 11, 24, 0, 13, 7]
* Chuyển dãy số về dạng ABC...XYZ ta có bãn mã: DOHOAXULYANH

•5. Cho k = (31,12),  N = 26, giải mã văn bản, dùng thuật mã Affine:

C =      WEYEBIPAGI

* Trong bảng mã ABC...XYZ, ta có N=26
* Văn bản gốc được chuyển thành dãy số [ 22, 4, 24, 4, 1, 8, 15, 0, 6, 8]
* Áp dụng thuật toán mở rộng  Euclide ta có:

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | B | Y |
| 1 | 26 | 0 |  |
| 2 | 31 | 1 | 0 |
| 3 | 26 | -1 | 1 |
| 4 | 5 | 2 | 5 |
| 5 | 1 | -11 | 5 |

B5 = -11 => a-1= 15

=> Vậy nghịch đảo của 31 theo module 26 là 15

* Với từng dãy số x trong C ta có hàm giải mã :                                                          D(x)= a-1(x-b) mod 26 = 15\*(x-12) mod 26 ta được dãy số [20, 10, 24, 10, 17, 18, 19, 2, 14, 18]
* Chuyển dãy số về dạng ABC...XYZ ta có bãn mã: UKYKRSTCOS.

•6. Cho k = (31,24), N = 26, mã hóa văn bản, dùng thuật mã Affine:

 với  P = MANCHESTERUNITED

* k = (31,12), N = 26 => ta có a=31, b=12, x là số tương ứng trên bản rõ, y là từng số tương ứng trên bản mã
* P = MANCHESTERUNITED, bản mã này được chuyển thành dãy số [12, 0, 13, 2, 7, 4, 18, 19, 4, 17, 20, 13, 8, 19, 4, 3]
* Áp dụng hàm mã hóa y = (31\*x + 12) mod 26 ta được dãy số tương ứng :  [6, 24, 11, 8, 7, 18, 10, 15, 18, 5, 20, 11, 12, 15, 18, 13]

=> Chuyển dãy số này về dạng ABC, văn bản đã mã hóa là : GYLIHSKPSFULMPSN.

•7. Cho k = (31,24),  N = 26, giải mã văn bản, dùng thuật mã Affine:

C =      DYOSFLGULMIHXI

* Trong bảng mã ABC...XYZ, ta có N=26
* Văn bản gốc được chuyển thành dãy số [ 3,24,14,18,5,11,6,20,11,12,8,7,23,8]
* Áp dụng thuật toán mở rộng  Euclide ta có:

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | B | Y |
| 1 | 26 | 0 |  |
| 2 | 31 | 1 | 0 |
| 3 | 26 | 0 | 1 |
| 4 | 5 | 1 | 5 |
| 5 | 1 | -5 | 5 |

B5 = -5 => a-1= 21

=> Vậy nghịch đảo của 31 theo module 26 là 21

* Với từng dãy số x trong C ta có hàm giải mã :                                                          D(x)= a-1(x-b) mod 26 = 21\*(x-24) mod 26 ta được dãy số [1,0,24,4,17,13,12,20,13,8,2,7,5,2]
* Chuyển dãy số về dạng ABC...XYZ ta có bãn mã: BAYERNMUNICHFC

•8. Cho k = (41,35),  N = 26, giải mã văn bản, dùng thuật mã Affine:

C =      ERJSTLNZRCJCMTYJENJ

* Trong bảng mã ABC...XYZ, ta có N=26
* Văn bản gốc được chuyển thành dãy số                                                                                   [ 4,17,9,18,19,11,13,25,17,2,9,2,12,19,24,9,4,13,9]
* Áp dụng thuật toán mở rộng  Euclide ta có:

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | B | Y |
| 1 | 26 | 0 |  |
| 2 | 41 | 1 | 0 |
| 3 | 26 | 0 | 1 |
| 4 | 15 | 1 | 1 |
| 5 | 11 | -1 | 1 |
| 6 | 4 | 2 | 2 |
| 7 | 3 | -5 | 1 |
| 8 | 1 | 7 | 3 |

B8 = 7 => a-1= 7

=> Vậy nghịch đảo của 41 theo module 26 là 7

* Với từng dãy số x trong C ta có hàm giải mã :                                                          D(x)= a-1(x-b) mod 26 = 7\*(x-35) mod 26 ta được dãy số [17,4,0,11,18,14,2,8,4,3,0,3,21,18,1,0,17,2,0]
* Chuyển dãy số về dạng ABC...XYZ ta có bãn mã: REALSOCIECACVSBARCA

•9. Cho k = (53,21),  N = 26, giải mã văn bản, dùng thuật mã Affine:

C =      ODIOPXFCJVCJXFDOCPVO

* Trong bảng mã ABC...XYZ, ta có N=26
* Văn bản gốc được chuyển thành dãy số                                                                                [ 14,3,8,14,15,23,5,2,9,21,2,9,23,5,3,14,2,15,21,14]
* Áp dụng thuật toán mở rộng  Euclide ta có:

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | B | Y |
| 1 | 26 | 0 |  |
| 2 | 53 | 1 | 0 |
| 3 | 26 | 0 | 2 |
| 4 | 1 | 1 | 26 |

B4 = 1 => a-1= 1

=> Vậy nghịch đảo của 53 theo module 26 là 1

* Với từng dãy số x trong C ta có hàm giải mã :                                                          D(x)= a-1(x-b) mod 26 = 1\*(x-53) mod 26 ta được dãy số [13,2,7,13,14,22,4,1,8,20,1,8,22,4,2,13,1,14,20,13]
* Chuyển dãy số về dạng ABC...XYZ ta có bãn mã: NCHNOWEBIUBIWECNBOUN

Công thức tổng quát a-1 mod N:

+ Giá trị điền sẵn: X1=N, B1=0, X2=a, B2=1

+ Giá trị điền tính toán:

Xi = Xi-2 mod Xi-1

Yi = Xi-1 div Xi

Bi = Bi-2 – (B­i-1 \* Yi-1)

Dừng khi X1= 1, và kết quả là a-1= Bi (Nếu âm a-1= Bi + N)

Câu 10:

Cho k = (53,47),  N = 26, giải mã văn bản, dùng thuật mã Affine: C =      OCPJIBICVPGTOJCJIB

Trong bãng mã ABC...XYZ, ta có N = 26

Văn bản gốc được chuyển thành dãy số [14, 2, 15, 9, 8, 1, 8, 2, 21, 15, 6, 19, 14, 9, 2, 9, 8, 1]

Với từng số x trong dãy số trên, ta áp dụng hàm giải mã:

E(x) = (53x - 47) mod 26, ta được dãy số: [19, 7, 20, 14, 13, 6, 13, 7, 0, 20, 11, 24, 19, 14, 7, 14, 13, 6]

Chuyển dãy số về dạng ABC, ta cáo P = THUONGNHAULYTOHONG

•11. Hãy tìm số nghịch đảo modulo 26 của 11 bằng thuật toán Euclide mở rộng

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | B | Y |
| 1 | 26 | 0 |  |
| 2 | 11 | 1 | 2 |
| 3 | 4 | -2 | 2 |
| 4 | 3 | 5 | 1 |
| 5 | 1 | -7 | 3 |

=> (-7+26) mode 26 = 19

•12. Hãy tìm số nghịch đảo modulo 26 của 17 bằng thuật toán Euclide mở rộng

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | B | Y |
| 1 | 26 | 0 |  |
| 2 | 17 | 1 | 1 |
| 3 | 9 | -1 | 1 |
| 4 | 8 | 2 | 1 |
| 5 | 1 | -3 | 8 |

=> (-3+26) mode 26 = 23

•13. Hãy tìm số nghịch đảo modulo 26 của 19 bằng thuật toán Euclide mở rộng

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | B | Y |
| 1 | 26 | 0 |  |
| 2 | 19 | 1 | 1 |
| 3 | 7 | -1 | 2 |
| 4 | 5 | 3 | 1 |
| 5 | 2 | -4 | 2 |
| 6 | 1 | 11 | 1 |

=> 19-1 = 11

•14. Hãy tìm số nghịch đảo modulo 26 của 25 bằng thuật toán Euclide mở rộng

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | B | Y |
| 1 | 26 | 0 |  |
| 2 | 25 | 1 | 1 |
| 3 | 1 | -1 |  |

=> ( -1 + 26) mod 26 = 25