**BÀI LÀM**

1. Hãy giải mã bản mật mã theo pp Affine với **C** và **K** như sau:
2. C=“SKTCK” ; K=(5,10)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| p | R1 | R2 | R | T1 | T2 | T |
| 5 | 26 | 5 | 1 | 0 | 1 | -5 |
| 1 | 5 | 1 | 0 | 1 | -5 | 6 |
|  | 1 | 0 |  | -5 | 6 |  |

= -5 + 26 = 21

C = S = 18 ; P = 21x(18 – 10) mod 26 = 12 => M

C = K = 10; P = 21x(10 – 10) mod 26 = 0 => A

C = T = 19; P = 21x(19 – 10) mod 26 = 7 => H

C = C = 02; P = 21x(2 – 10) mod 26 = 14 => O

=> P = MAHOA

1. C= “CQMQSM” ; K=(7,12)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| p | R1 | R2 | R | T1 | T2 | T |
| 3 | 26 | 7 | 5 | 0 | 1 | -3 |
| 1 | 7 | 5 | 2 | 1 | -3 | 4 |
| 2 | 5 | 2 | 1 | -3 | 4 | -11 |
| 1 | 2 | 1 | 0 | 4 | -11 | 26 |
|  | 1 | 0 |  | -11 | 26 |  |

= -11 + 26 = 15

C = C = 02 ; P = 15x(02 – 12) mod 26 = 6 => G

C = Q = 16; P = 15x(16 – 12) mod 26 = 8 => I

C = M = 12; P = 15x(12 – 12) mod 26 = 0 => A

C = S = 18; P = 15x(18 – 12) mod 26 = 12 => M

=> P = GIAIMA

1. C= “FNJONAP” ; K=(9,13)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| p | R1 | R2 | R | T1 | T2 | T |
| 2 | 26 | 9 | 8 | 0 | 1 | -2 |
| 1 | 9 | 8 | 1 | 1 | -2 | 3 |
| 8 | 8 | 1 | 0 | -2 | 3 | -26 |
|  | 1 | 0 |  | 3 | -26 |  |

= 3

C = F = 05 ; P = 3x(05 – 13) mod 26 = 02 => C

C = N = 13; P = 3x(13 – 13) mod 26 = 00 => A

C = J = 09; P = 3x(09 – 13) mod 26 = 14 => O

C = O = 14; P = 3x(14 – 13) mod 26 = 03 => D

C = A = 00; P = 3x(00 – 13) mod 26 = 13 => N

C = P = 15; P = 3x(15 – 13) mod 26 = 6 => G

=> P =CAODANG

1. C= “PTABCKOC” ; K=(11,14)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| p | R1 | R2 | R | T1 | T2 | T |
| 2 | 26 | 11 | 4 | 0 | 1 | -2 |
| 2 | 11 | 4 | 3 | 1 | -2 | 5 |
| 1 | 4 | 3 | 1 | -2 | 5 | -7 |
| 3 | 3 | 1 | 0 | 5 | -7 | 26 |
|  | 1 | 0 |  | -7 | 26 |  |

= -7 + 26 = 19

C = P = 15 ; P = 19x(15 – 14) mod 26 = 19 => T

C = T = 19 ; P = 19x(19 – 14) mod 26 = 17 => R

C = A = 00 ; P = 19x(00 – 14) mod 26 = 20 => U

C = B= 01 ; P = 19x(01 – 14) mod 26 = 13 => N

C = C = 02 ; P = 19x(02 – 14) mod 26 = 06 => G

C = K = 10 ; P = 19x(15 – 14) mod 26 = 02 => C

C = O = 14 ; P = 19x(14 – 14) mod 26 = 00 => A

=> P =TRUNGCAG

1. C= “OQMPGDR” ; K=(15,16)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| p | R1 | R2 | R | T1 | T2 | T |
| 1 | 26 | 15 | 11 | 0 | 1 | -1 |
| 1 | 15 | 11 | 4 | 1 | -1 | 2 |
| 2 | 11 | 4 | 3 | -1 | 2 | -5 |
| 1 | 4 | 3 | 1 | 2 | -5 | 7 |
| 3 | 3 | 1 | 0 | -5 | 7 | -26 |
|  | 1 | 0 |  | 7 | -26 |  |

K^-1 = 7

C = O = 14 ; P = 7x(14 – 16) mod 26 = 12 => M

C = Q = 16 ; P = 7x(16 – 16) mod 26 = 0 => A

C = M = 12 ; P = 7x(12 – 16) mod 26 = 24 => Y

C = P = 15 ; P = 7x(15 – 16) mod 26 = 19 => T

C = G = 6 ; P = 7x(6 – 16) mod 26 = 8 => I

C = D = 3 ; P = 7x(3 – 16) mod 26 = 13 => N

C = R = 17 ; P = 7x(17 – 16) mod 26 = 7 => H

=> P = MAYTINH

1. C= “AWONUDIV” ; K=(17,18)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| p | R1 | R2 | R | T1 | T2 | T |
| 1 | 26 | 17 | 9 | 0 | 1 | -1 |
| 1 | 17 | 9 | 8 | 1 | -1 | 2 |
| 1 | 9 | 8 | 1 | -1 | 2 | -3 |
| 8 | 8 | 1 | 0 | 2 | -3 | 26 |
|  | 1 | 0 |  | -3 | 26 |  |

= -3 + 26 = 23

C = A = 00 ; P = 23x(0 – 18) mod 26 = 2 => C

C = W = 22 ; P = 23x(2 – 18) mod 26 = 14 => O

C = O = 14 ; P = 23x(14 – 18) mod 26 = 12 => M

C = N = 13 ; P = 23x(13 – 18) mod 26 = 15 => P

C = U = 20 ; P = 23x(20 – 18) mod 26 = 20 => U

C = D = 03 ; P = 23x(03 – 18) mod 26 = 19 => T

C = I = 08 ; P = 23x(08 – 18) mod 26 = 4 => E

C = V = 21; P = 23x(21 – 18) mod 26 = 17 => R

=> P =COMPUTER

1. C= “RFKISHRQH” ; K=(19,20)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| p | R1 | R2 | R | T1 | T2 | T |
| 1 | 26 | 19 | 7 | 0 | 1 | -1 |
| 2 | 19 | 7 | 5 | 1 | -1 | 3 |
| 1 | 7 | 5 | 2 | -1 | 3 | -4 |
| 2 | 5 | 2 | 1 | 3 | -4 | 11 |
| 2 | 2 | 1 | 0 | -4 | 11 | -26 |
|  | 1 | 0 |  | 11 | -26 |  |

= 11

C = R = 17; P = 11x(17 – 20) mod 26 = 19 => T

C = F = 5; P = 11x(5 – 20) mod 26 = 17 => R

C = K = 10; P = 11x(10 – 20) mod 26 = 20 => U

C = I = 8; P = 11x(8 – 20) mod 26 = 24 => Y

C = S = 18; P = 11x(18 – 20) mod = 4 => E

C = H = 7; P = 11x(7 – 20) mod 26 = 13 => N

C = Q = 16; P = 11x(16 – 20) mod 26 = 8 => I

=> P= TRUYENTIN

1. C= “FNEJSFIJ” ; K=(21,22)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| p | R1 | R2 | R | T1 | T2 | T |
| 1 | 26 | 21 | 5 | 0 | 1 | -1 |
| 4 | 21 | 5 | 1 | 1 | -1 | 5 |
| 5 | 5 | 1 | 0 | -1 | 5 | -26 |
|  | 1 | 0 |  | 5 | -26 |  |

= 5

C = F = 5; P = 5x(5 – 22) mod 26 = 19 => T

C = N = 13; P = 5x(13 – 22) mod 26 = 7 => H

C = E = 4; P = 5x(4 – 22) mod 26 = 14 => O

C = J = 9; P = 5x(9 – 22) mod 26 = 13 => N

C = S = 18; P = 5x(18 – 22) mod 26 = 6 => G

C = I = 8; P = 5x(8 – 22) mod 26 = 8 => I

=> P=THONGTIN

1. C = “TDMMLP” ; K=(23,24)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| p | R1 | R2 | R | T1 | T2 | T |
| 1 | 26 | 23 | 3 | 0 | 1 | -1 |
| 7 | 23 | 3 | 2 | 1 | -1 | 8 |
| 1 | 3 | 2 | 1 | -1 | 8 | -9 |
| 2 | 2 | 1 | 0 | 8 | -9 | 26 |
|  | 1 | 0 |  | -9 | 26 |  |

= -9 + 26 = 17

C = T = 19; P = 17x(19 – 24) mod 26 = 19 => T

C = D = 3; P = 17x(3 – 24) mod 26 = 7 => H

C = M = 12; P = 17x(12 – 24) mod 26 = 4 => E

C = L = 11; P = 17x(11 – 24) mod 26 = 13 => N

C = P = 15; P = 17x(15 – 24) mod 26 = 3 => D

=> P= THEEND

1. Hãy mã hóa thông điệp “TRƯỜNG DẠI HỌC TRÀ VINH” theo phương pháp Hill với khóa *k* được chọn: sau đó giải mã lại thông điệp ban đầu.

**\* MÃ HOÁ:**

=> C = VJUYSLYDHKOWVJLGZIEH

**\* GIẢI MÃ:**

=> mod26 = 9

=> P = TRUONGDAIHOCTRAVINH(A-> bỏ vì từ thêm vào)

1. Hãy mã hóa thong điệp “ATTACK IS TODAY” theo phương pháp Hill với khóa *k* được chọn: , sau đó giải mã lại thông điệp ban đầu.

**\* MÃ HOÁ:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | T | T | A | C | K | I | S | T | O | D | A | Y |
| 0 | 19 | 19 | 0 | 2 | 10 | 8 | 18 | 19 | 14 | 3 | 0 | 24 |

=> C= DKIPMAYYCVEBGI

**\* GIẢI MÃ:**

=> P=ATTACKISTODAY(A->Bỏ A vì tự thêm vào)

1. Hãy giải mã bản mật “RKBPOA” theo phương pháp Hill với khóa k được thống nhất là: .

**\* GIẢI MÃ:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R | K | B | P | O | A |
| 17 | 10 | 1 | 15 | 14 | 0 |

=3 =>

= =

=> P=CDTACK

-hết-