1.  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  
Trả lời:  
“KS” (10 18)  
Det(K) = (3\*3 – 1\*4) mod 26 = 5 mod 26 = 5  
Tính Det(K^-1) theo Euclid mở rộng:  
     X   B   Y  
1  26  0  
2  5    1   5  
3  1   -5   5  
  
=>(-5 + 26) mod 26 = 21  
K^-1 = Det(K^-1)\* (3   -4   -1   3)  = 21 \* (3   -4   -1   3)  mod 26 = (11   20   5   11)  
P = K^-1 \* C = (11   20   5   11)\*(10   18) = (11\*10+20\*18) (5\*10 + 11\*18)= ( 470 248) mod 26 = (2 14) => “CO”  
=> “CO”  
2.  Cho bản rõ “THUA” 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  
Trả lời:  
“TH” (19 7)  
“UA” (20 0)  
P1 = (19 7) ta có C1 = K \* P1 = (9   7   3   4)\*(19   7) = (220 85) mod 26 = (12 7) => “MH”  
P2 = (20 0) ta có C2 = K \* P2 = (9   7   3   4)\*(20   0) = (180 60) mod 26 = (24 8) => “YI”  
=>“MHYI”  
•3.  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 tìm bản rõ ? Biết hàm mã hóa y=kx  
  
“KD” (10 3)  
“IY” (8 24)  
Det(K) = (8\*3 – 3\*5) mod 26 = 9 mod 26 = 9  
Tính Det(K^-1) theo Euclid mở rộng:  
    X    B   Y  
1  26  0  
2  9    1   2  
3  8   -2  1  
4  1    3   8  
  
=>Det(K^-1) = 3  
K^-1 = Det(K^-1)\*(8   3   5   3)  = 21 \*(8   3   5   3) mod 26 = (24   9   15   9)   
P1 = K^-1 \* C1 = (24   9   15   9)\*(10   3) =(24\*10+9\*3) (15\*10 + 9\*3)= (267 177) mod 26 = (7 21) => “HV”  
P2 = K^-1 \* C2 = (24   9   15   9)\*(8   24) =(24\*8+9\*24) (15\*8 + 9\*24)= (408 336) mod 26 = (18 24) => “SY”  
=>“HVSY”  
  
•4.  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  
Trả lời:  
“CN” (2 13)  
“PZ” (15 25)  
“IE” (8 4)  
“QN” (16 13)  
Det(K) = (6\*4 – 3\*5) mod 26 = 9 mod 26 = 9  
Tính Det(K^-1) theo Euclid mở rộng:  
    X    B   Y  
1  26  0  
2  9   1    2  
3  8   -2  1  
4  1   3   8  
  
=>Det(K^-1) = 3  
K^-1 = Det(K^-1)\*(6   5   3   4)  = 21 \*(6   5   3   4) mod 26 = (18   15   9   12)  
P1 = K^-1 \* C1 = (18   15   9   12)\*(2   13) =(18\*2+15\*13) (9\*2+12\*13)= (231 174) mod 26 = (23 18) => “XS”  
P2 = K^-1 \* C2 = (18   15   9   12)\*(15   25) =(18\*15+15\*25) (9\*15+12\*25)= (645 435) mod 26 = (21 19) => “VT”  
P3 = K^-1 \* C3 = (18   15   9   12)\*(8   4) =(18\*8+15\*4) (9\*8+12\*4)= (204 120) mod 26 = (22 16) => “WQ”  
P4 = K^-1 \* C4 = (18   15   9   12)\*(16   13) =(18\*16+15\*13) (9\*16+12\*13)= (483 300) mod 26 = (15 14) => “PO”  
=>“ XSVTWQPO”  
  
•5.  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  
  
Trả lời:  
“CO” (2 14)  
“SL” (18 11)  
“CZ” (2 25)  
Det(K) = (6\*4 – 3\*5) mod 26 = 9 mod 26 = 9  
Tính Det(K^-1) theo Euclid mở rộng:  
    X    B   Y  
1  26  0  
2  9    1   2  
3  8   -2   1  
4  1    3   8  
  
=>Det(K^-1) = (3 + 26) mod 26 = 3  
K^-1 = 3 \* (4   21   23   6) = (12   63   69   18) mod 26 = (12   11   17   18)   
P1 = C1 \* K^-1= (2   14) . (12   11   17   18) = (262 274) mod 26 = (2 14) => “CO”  
P2 = P3= C2 \* K^-1 = (18   11) . (12   11   17   18) = (403 396) mod 26 = (13 6) => “NG”  
P4 = C4 \* K^-1 = (2   25) . (12   11   17   18) = (449 472) mod 26 = (7 4) => “HE”  
=>“CONGNGHE”  
  
•6.  Cho bản rõ “RZCDPA” 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=xk  
Trả lời:  
“RZ” (17 25)  
“CD” (2 3)  
“PA” (15 0)  
P1 = (17 25) ta có C1 = P1\*K = (17   25) . (9   7    3   4) = (228 219) mod 26 = (20 11) => “UL”  
P2 = (2 3) ta có C2 = P2\*K = (2   3) . (9   7    3   4) = (27 26) mod 26 = (1 0) => “BA”  
P3 = (15 0) ta có C3 = P3\*K = (15   0) . (9   7    3   4) = (135 105) mod 26 = (5 1) => “FB”  
=>“ULBAFB”  
•7.  Cho bản mã “RMKCEJVI” khóa k là ma trận cấp 2 sau:  
  
8       3  
  
5       3  
Giải mã bản mã với khóa k theo hệ mã Hill tìm bản rõ ? Biết hàm mã hóa y=xk  
  
Det(k) = (8\*3 – 3\*5) = 9  
Áp dụng thuật toán Euclide tính được Det(k-1) = 3  
  
k-1 = 3\* (3 -3 -5 8) = (9 -9 -15 24) = (9 27 11 24)  
  
RM: P1= C1 \* K-1 = (17 12) . (9 27 11 24) = (25 5) : ZF  
  
KC: P2= C2 \* K-1 = (10 2) . (9 27 11 24) = (8 10) : IK  
  
EJ : P3 = C3 \* K-1 = (4 9) . (9 27 11 24) = (5 24) : FY  
  
VI : P4 = C4 \* K -1 = (21 8) . (9 27 11 24) = (17 3) : RD  
=>“ZFIKFYRD”  
  
•8.  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 – 2\*3) = 15  
Áp dụng thuật toán Euclide tính được Det(k-1) = 7  
  
k-1 = 7\* (3 -2 -3 7) = (21 12 5 23)  
  
BK : P1= C1 \* K-1 = (1 10) . (21 12 5 23)= (19 8) : TI  
  
IV: P2= C2 \* K-1 = (8 21) . (21 12 5 23) = (13 7) : NH  
  
AI: P3 = C3 \* K-1 = (0 8) . (21 12 5 23) = (14 2) : OC  
  
WO : P4 = C4 \* K -1 = (22 14) . (21 12 5 23) = (12 14) : MO  
=>“TINHOCMO”  
  
•9.  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  
TH (19 7) -> C1 = K.P1 = (7 2 3 3) . (19 7) = (17 0) -> RA  
  
EG (4 6) -> C2 = K.P2 = (7 2 3 3) . (4 6) = (14 4) -> OE  
  
IO (8 14) -> C3 = K.P3 = (7 2 3 3) . (8 14) = (6 14) -> GO  
  
ID (8 3) -> C4 = K.P4 = (7 2 3 3) . (8 3) = (10 7) -> KH  
  
OD (14 3) -> C5 = K.P5 = (7 2 3 3) . (14 3) = (0 25) -> AZ  
  
AY (0 24) -> C4 = K.P4 = (7 2 3 3) . (0 24) = (22 20) -> WU  
  
=> RAOEGOKHAZWU  
  
•10.  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  
  
“VI” (21 8) -> C1 = K.P1 = (9 7 3 4) . (21 8) = (11 17) -> “LR”  
  
“NH” (13 7) -> C2 = K.P2 = (9 7 3 4) . (13 7) = (10 15) -> “KP”  
  
“HA” (7 0) -> C3 = K.P3 = (9 7 3 4) . (7 0) = (11 21) -> “LV”  
  
“LO” (11 14) -> C4 = K.P4 = (9 7 3 4) . (11 14) = (15 11) -> “PL”  
  
“NG” (13 6) -> C5 = K.P5 = (9 7 3 4) . (13 6) = (3 11) -> “DL”  
  
=> “LRKPLVPLDL”