Assignment 3: Hill Ciphers

① $K = \begin{pmatrix} 11 & 8 \\ 12 & 9 \end{pmatrix}$

x = hello

Encryption: $e_K(x) = Kx$

Step 1. Convert into integers

h	e	l	l	o	z
7	4	11	11	14	25

z letter has been added to complete the last two-integers block

Step 2. Encrypt each block of two integers

$$\begin{pmatrix} 11 & 8 \\ 12 & 9 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 77+32 \\ 84+36 \end{pmatrix} = \begin{pmatrix} 109 \\ 120 \end{pmatrix} = \begin{pmatrix} 5 \\ 16 \end{pmatrix}$$

$$\begin{pmatrix} 11 & 8 \\ 12 & 9 \end{pmatrix} \cdot \begin{pmatrix} 11 \\ 11 \end{pmatrix} = \begin{pmatrix} 121+88 \\ 132+99 \end{pmatrix} = \begin{pmatrix} 209 \\ 231 \end{pmatrix} = \begin{pmatrix} 1 \\ 23 \end{pmatrix}$$

$$\begin{pmatrix} 11 & 8 \\ 12 & 9 \end{pmatrix} \cdot \begin{pmatrix} 14 \\ 25 \end{pmatrix} = \begin{pmatrix} 154+200 \\ 168+225 \end{pmatrix} = \begin{pmatrix} 354 \\ 393 \end{pmatrix} = \begin{pmatrix} 16 \\ 3 \end{pmatrix}$$

Step 3 convert each two-integers block to characters

$y = f\,q\,b\,x\,g\,d$

② $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$

$y = x_i y_j$ Decryption: $d_K(y) = K^{-1} \cdot y$

compute K^{-1} if $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$

~~detA~~

$\det K = 11 \cdot 7 - 3 \cdot 8 = 77 - 24 = 53$ ~~mod 26 = 1~~

$\det K \bmod 26 = 53 \bmod 26 = 1$

$K^{-1} = (\det(K))^{-1} \cdot \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix}$

$\det(K)^{-1} = 1$

$K^{-1} = \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$

x i j y

23 8 9 24

$\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \begin{pmatrix} 23 \\ 8 \end{pmatrix} = \begin{pmatrix} 56 & 414 \\ 7 \cdot 8 + 18 \cdot 23 \\ 23 \cdot 23 + 11 \cdot 8 \\ 529 \quad 88 \end{pmatrix} = \begin{pmatrix} 470 \\ 617 \end{pmatrix} = \begin{pmatrix} 2 \\ 19 \end{pmatrix}$

$\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \begin{pmatrix} 9 \\ 24 \end{pmatrix} = \begin{pmatrix} 7 \cdot 9 + 18 \cdot 24 \\ 23 \cdot 9 + 11 \cdot 24 \end{pmatrix} = \begin{pmatrix} 495 \\ 471 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$

convert each two-block integers

ctbd