1.

K	10	->	D	3
R	17	->	O	14
O	14	->		
N	13	->		

$Y= mx+c$

$3 = 10a+b$

$14 = 17a+b$

$B = 3-10a$

$B = 14-17a$

$3-10a = 14-17a$

$7a = 11 \bmod 26$

$11*15 = 165 \bmod 26 = 9$

$Y=9x+c$

$3 = 10*9 + c$

$3 = 90 + c \bmod 26$

$C = 17$

$Y=9a+17$

$3=9*10+17 \bmod 26$

$9*14+17 \bmod 26$ N

$9*13 + 17 \bmod 26$ E

DONE

2.

A

X = 6 mod 7

X = 2 mod 5

$N_{1}7 + N_{2}5 = 1$

$N_1 = -2$

$N_2 = 3$

$X = 2*7*N_1 + 6*5*N_2$ mod 7*5

X = 2*7*-2 + 6*5*3 = -28 + 90 = 62 mod 35

X = 27 + 35n for some n in Z

B

X= 6 mod 6

X = 2 mod 3

$M_1 = 6$

$M_2 = 3$

C

3

A

X = [[1, 0] [13, 0], [13, 0]]

y = [5 3]x + [14] for x in X

[3 0]   [2]

Y = ['t', 'd', 'b', 'n', 'b', 'n']

Tdbnbn

B

Find C^{-1} mod 26

$$C^{-1} = \begin{matrix} 0 & 1/3 \\ 1/3 & -5/9 \end{matrix}$$

$Y = C^{-1}(Y\text{-}D)$

$Y = C^{-1}Y - C^{-1}D$

$$Y = \begin{bmatrix} 0 & 1/3 \\ 1/3 & -5/9 \end{bmatrix} Y + \begin{bmatrix} 0 \\ -4\ 2/3 \end{bmatrix}$$

C

Ygyi = “cacy”

D

1. A Hill cipher uses a matrix key, which is typically randomly generated. Without knowledge of the key, Eve cannot decrypt any other messages encrypted with the same key.
2. Even if Eve were to guess the key size and matrix, she would still need to invert the matrix in order to decrypt other messages. Inverting a matrix is a computationally expensive operation, especially for larger matrices.
3. The known plaintext attack is only effective if the plaintext and ciphertext are from the same message. If Eve has access to the plaintext and ciphertext of different messages, she cannot use the known plaintext attack to break the cipher.