Student Number: [redacted] Name: Bryan Hoang

1. (10 points)

(a)

(i) **Answer:**

$$\begin{aligned} e_k(m) &\equiv k_1 \cdot m + k_2 \pmod p \\ &\equiv \left(\begin{smallmatrix} 1 & 3 \\ 2 & 2 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 5 \\ 4 \end{smallmatrix}\right) \pmod 7 \\ &\boxed{\equiv \left(\begin{smallmatrix} 5 \\ 3 \end{smallmatrix}\right)} \pmod 7. \end{aligned}$$

(ii) **Answer:**
The matrix k_1^{-1} used for decryption is $\boxed{k_1^{-1} = \left(\begin{smallmatrix} 3 & 6 \\ 4 & 5 \end{smallmatrix}\right)}$.

(iii) **Answer:**

$$\begin{aligned} d_k(c) &\equiv k_1^{-1} \cdot (c - k_2) \pmod p \\ &\equiv \left(\begin{smallmatrix} 3 & 6 \\ 4 & 5 \end{smallmatrix}\right) \cdot \left(\left(\begin{smallmatrix} 3 \\ 5 \end{smallmatrix}\right) - \left(\begin{smallmatrix} 5 \\ 4 \end{smallmatrix}\right)\right) \pmod 7 \\ &\boxed{\equiv \left(\begin{smallmatrix} 0 \\ 4 \end{smallmatrix}\right)} \pmod 7. \end{aligned}$$

(b) **Answer:**
The Hill cipher is vulnerable to a plaintext attack because each known plaintext and cipher text pair gives a congruence of the form $c \equiv k_1 \cdot m + k_2$. This yields n linear equations for the $n^2 + n = n \cdot (n+1)$ unknown entries of the keys k_1 and k_2. Thus, knowing $n+1$ plaintext and ciphertext pairs for an attack would give enough equations for an attacke to solve for the keys k_1 and k_2.

(c) **Answer:**

(d) **Answer:**