Q_1:

$x = d_K(y)$

$x = d_K(e_K(x))$

$x = e_K((x+K) \bmod 26)$ // Because K is an involutory key

$x = [(x+K) \bmod 26 + K] \bmod 26$

$x = (x + 2K) \bmod 26$

$$\Rightarrow \begin{cases} 2K \bmod 26 = 0 \\ 0 \leqslant K \leqslant 25 \end{cases} \Rightarrow \begin{cases} K_1 = 0 \\ K_2 = 13 \end{cases}$$

Q2:

a) "⇒"

$x = d_k(y)$

$x = d_k(e_k(x))$

$x = d_k((ax+b) \bmod n)$

$x = e_k((ax+b) \bmod n)$ // Because K is an involutory key

$x = [a((ax+b) \bmod n) + b] \bmod n$

$x = a^2x + ab + b \bmod n$

$x = [a^2x + b(a+1)] \bmod n$

$\Rightarrow \begin{cases} b(a+1) \equiv 0 \pmod n \\ a^2 \equiv 1 \pmod n \Rightarrow a \equiv a^{-1} \pmod n \Rightarrow a^{-1} \bmod n = a \end{cases}$

"⇐"

$e_k(y) = e_k(e_k(x))$

$e_k(y) = a^2x + ab + b \bmod n$

$e_k(y) = a^2x + b(a+1) \bmod n$

$e_k(y) = a^2x \bmod n$ // Because $b(a+1) \equiv 0 \pmod n$

$e_k(y) = aa^{-1}x \bmod n$ // Because $a^{-1} \bmod n = a$

$e_k(y) = x$

From $e_k(y) = x$ and $d_k(y) = x$, we know K is an involutory key

b)

$a \in \{1, 2, 4, 7, 8, 11, 13, 14\}$ // Because $\gcd(a, 15) = 1$

$a \in \{1, 4, 11, 14\}$ // Because $a^{-1} \bmod 15 = a$

$\Rightarrow K_1 = (1, 0)$ $K_2 = (4, 3)$ $K_3 = (4, 6)$ $K_4 = (4, 9)$ $K_5 = (4, 12)$ $K_6 = (4, 0)$

$K_7 = (11, 5)$ $K_8 = (11, 10)$ $K_9 = (11, 0)$

$K_{10} = (14, 1)$ $K_{11} = (14, 2)$ $K_{12} = (14, 3)$ $K_{13} = (14, 4)$ $K_{14} = (14, 5)$ $K_{15} = (14, 6)$

$K_{16} = (14, 7)$ $K_{17} = (14, 8)$ $K_{18} = (14, 9)$ $K_{19} = (14, 10)$ $K_{20} = (14, 11)$ $K_{21} = (14, 12)$

$K_{22} = (14, 13)$ $K_{23} = (14, 14)$ $K_{24} = (14, 0)$ // Because $b(a+1) \equiv 0 \pmod{n}$

Q3:

a)

$\det(K) = 10 - 45 = -35 = 17$

$(\det K)^{-1} = 23$

$K^{-1} = 23 \cdot \begin{bmatrix} 5 & -5 \\ -9 & 2 \end{bmatrix} = \begin{bmatrix} 11 & 15 \\ 1 & 20 \end{bmatrix}$

b)

$\det(K) = 5$

$(\det K)^{-1} = 21$

$K^{-1} = 21 \cdot \begin{bmatrix} 21 & 3 & 6 \\ 24 & 13 & 20 \\ 7 & 16 & 5 \end{bmatrix} = \begin{bmatrix} 25 & 11 & 22 \\ 10 & 13 & 4 \\ 17 & 24 & 1 \end{bmatrix}$

Q4:

a)

x	1	2	3	4	5	6	7	8
$\pi^{-1}(x)$	2	4	6	1	8	3	5	7

b)

gentleme ndonotre adeachot hersmail