Solutions to Ex 6: first set of questions

(1) The encryption key was 3.
Without any other information (such as a frequency analysis) the only method is to add 1 to the values of each of the letters successively until the text makes sense. In this case the message in cleartext is ETTUBRUTE.

(2) Here you have to subtract modulo 26 using SCRAMBLESCRA as the key. In the 2nd version of the question you should have got VENIVIDIVICI. In the 1st version with the typos you should have got ZENIVIDIZICI — both are great.

(3) This can be done via inspection

x	1	3	5	7	9	11	15	17	19	21	23	25
x^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

(4) $\det\begin{pmatrix}2 & 3\\ 3 & 2\end{pmatrix} = 21.$

By question (3) above, $21^{-1} = 5$

$$\therefore \begin{pmatrix}2 & 3\\ 3 & 2\end{pmatrix}^{-1} = 5\begin{pmatrix}2 & -3\\ -3 & 2\end{pmatrix} = \begin{pmatrix}10 & 11\\ 11 & 10\end{pmatrix}$$

Check $\begin{pmatrix}2 & 3\\ 3 & 2\end{pmatrix}\begin{pmatrix}10 & 11\\ 11 & 10\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ ✓

(5) We have to find $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ s.t.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} H \\ A \end{pmatrix} = \begin{pmatrix} F \\ U \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} N \\ D \end{pmatrix} = \begin{pmatrix} S \\ S \end{pmatrix}$$

$$\therefore \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 7 \\ 0 \end{pmatrix} = \begin{pmatrix} 5 \\ 20 \end{pmatrix} \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 13 \\ 3 \end{pmatrix} = \begin{pmatrix} 18 \\ 18 \end{pmatrix}$$

$$\therefore \quad 7a = 5 \qquad 13a + 3b = 18$$

$$7c = 20 \qquad 13c + 3d = 18$$

$$a = 7^{-1} \times 5 = 15 \times 5 = 23 \qquad (\text{mod } 26)$$

$$c = 7^{-1} \times 20 = 15 \times 20 = 14 \qquad (\text{mod } 26)$$

$$3b = 18 - 13a$$

$$= 5$$

$$\therefore b = 3^{-1} \times 5 = 9 \times 5 = 19$$

$$3d = 18 - 13c = 18 - 13 \cdot 14 = 18$$

$$\therefore d = 3^{-1} \times 18 = 9 \times 18 = 6$$

$$\therefore \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 23 & 19 \\ 14 & 6 \end{pmatrix}$$ & check

(6) 257 is prime $\therefore \varphi(257) = 257-1 = \underline{256}$

$253 = 11 \times 23$

$$\therefore \phi(253) = \varphi(11)\,\varphi(23)$$
$$= (11-1)(22-1)$$
$$= 10 \cdot 22 = \underline{220}$$

Solutions to Ex 6 (2nd set)

1. $77 = 7 \times 11$. $\therefore$ $\varphi(77) = 6 \times 10 = \underline{60}$

Solve extended Euclidean algorithm for 60 and 43.

$$\left(\begin{array}{cc|c} 1 & 0 & 60 \\ 0 & 1 & 43 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -1 & 17 \\ 0 & 1 & 43 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -1 & 17 \\ -2 & 3 & 9 \end{array}\right) \to \left(\begin{array}{cc|c} 3 & -4 & 8 \\ -2 & 3 & 9 \end{array}\right)$$

$$\to \left(\begin{array}{cc|c} 3 & -4 & 8 \\ -5 & 7 & 1 \end{array}\right) \to \left(\begin{array}{cc|c} * & * & * \\ -5 & 7 & 1 \end{array}\right)$$

$\therefore$ $-5 \times 60 + 7 \times 43 = 1$

$\therefore$ $7 \times 43 \equiv 1 \pmod{60}$

$\therefore$ $\underline{d = 7}$

8. $\varphi(47 \cdot 59) = 2668$

$$\left(\begin{array}{cc|c} 1 & 0 & 2668 \\ 0 & 1 & 157 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -16 & 156 \\ 0 & 1 & 157 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -16 & 156 \\ -1 & 17 & 1 \end{array}\right) \to *$$

$-2668 + 17 \times 157 = 1 \Rightarrow \underline{157^{-1} = 17}$

$\underline{17 = 16 + 1}$

1044	*
1044^2	147
1044^4	2198
1044^8	638
1044^{16}	2186 *

$2186 \times 1044 \equiv \underline{\underline{5}} \mod 2773$

3.

5^1	5^2	5^3	5^4	5^5	5^6	5^7	5^8	5^9	5^{10}	5^{11}	5^{12}
5	2	10	4	20	8	17	16	11	9	22	18

5^{13}	5^{14}	5^{15}	5^{16}	5^{17}	5^{18}	5^{19}	5^{20}	5^{21}	5^{22}
21	13	19	3	15	6	7	12	14	1

$2 = 5^{\underline{\underline{2}}}$, $3 = 5^{\underline{\underline{16}}}$

$x = 2$, $y = 16$.