Lema 4

④ $\sqrt{13147}$ | $= 123$

$1 \quad 2 \cdot 2 = 24$

$131 \quad 243 \cdot 3 = 729$

$=31$

24

5747

729

18

$x = \lfloor \sqrt{13147} \rfloor + 1 = 124$

$x^2 - n = 15376 - 13147 = 2229$

$\sqrt{2229}$ | 47

$16 \quad 87 \cdot 7 = 609$

$=629$

609

20

$x = 125$, $x^2 - n = 15625 - 13147 = 2478$

$\sqrt{2478}$ | 49

$16 \quad 89 \cdot 9 = 801$

$=878$

801

77

$\sqrt{2729}$ | 52

$25 \quad 102 \cdot 2 = 204$

$=229$

204

$=25$

$x = 126$, $x^2 - n = 2729$

$\sqrt{2582}$ | 54

$25 \quad 104 \cdot 4 = 416$

$=482$

416

66

$x = 127$ $x^2 - n = 2982$

Lema 5

(7) $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{Z}_{26})$

Τώρα διώ

$$\det A = \begin{vmatrix} 2 & 3 \\ 7 & 8 \end{vmatrix} = 2\cdot 8 - 7\cdot 3 = 16 - 21 = -5 = 21 \pmod{26}$$

$26 = 1\cdot 21 + 5$

$21 = 4\cdot 5 + 1$

$5 = 5\cdot 1 + 0$

$21 - 4\cdot 5 = 1 \Rightarrow 1 = 21 - 4(26 - 1\cdot 21)$

$1 = 5\cdot 21 - 4\cdot 26$

$5\cdot 21 \equiv 1 \pmod{26}$

$21^{-1} = 5 \pmod{26}$

$$\text{adj}(A) = \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix} \equiv \begin{pmatrix} 8 & 23 \\ 19 & 2 \end{pmatrix} \pmod{26}$$

$$A^{-1} = 21^{-1}\,\text{adj}\,A \pmod{26} = 5\cdot\begin{pmatrix} 8 & 23 \\ 19 & 2 \end{pmatrix} \pmod{26} = \begin{pmatrix} 40 & 115 \\ 95 & 10 \end{pmatrix} \pmod{26} =$$

$$= \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \pmod{26}$$

Τώρα διώ, $\Gamma = 5$, $\Omega = 22$, $\Lambda = 12$, $\Delta = 5$, $\Sigma = 8$, $\Phi = 16$

(11) $\begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix}\begin{pmatrix} 5 \\ 22 \end{pmatrix} = \begin{pmatrix} 70 + 242 \\ 85 + 220 \end{pmatrix} \pmod{26} = \begin{pmatrix} 0 \\ 15 \end{pmatrix} \pmod{26} = \begin{pmatrix} A \\ T \end{pmatrix}$

$\begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix}\begin{pmatrix} 12 \\ 3 \end{pmatrix} = \begin{pmatrix} 201 \\ 234 \end{pmatrix} \pmod{26} = \begin{pmatrix} 19 \\ 0 \end{pmatrix} = \begin{pmatrix} T \\ A \end{pmatrix}$

$\begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix}\begin{pmatrix} 8 \\ 16 \end{pmatrix} = \begin{pmatrix} 112 + 176 \\ 136 + 160 \end{pmatrix} \pmod{26} = \begin{pmatrix} 288 \\ 296 \end{pmatrix} \pmod{26} = \begin{pmatrix} 2 \\ 10 \end{pmatrix} = \begin{pmatrix} C \\ K \end{pmatrix}$

$\begin{pmatrix} A & T & C \\ T & A & K \end{pmatrix}$, ATTACK