2018 Q1

a) $37 = 22 + 15$ ✓

$22 = 15 + 7$ ✓

$15 = 2.7 + 1$ ✓

Do NOT use a red pen on my paper, else I'll dock you 50 marks!

$1 = 15 - 2.7$

$= 15 - 2.(22 - 15)$

$= 3.15 - 2.22$

$= 3(37 - 22) - 2.22$

$\equiv -5.22 \mod 37$

$$22^{-1} \equiv (-5) \equiv 32$$

b) 0x40042516

$1.0 + 2.x + 3.4 + 4.0 + 5.0$
$+ 6.4 + 7.2 + 8.5 + 9.1 + 10.6$

$\equiv 0 \mod 11$

$2x + 1 + 2 + 3 + 7 - 2 - 6 = 0$

$2x + 5 = 0$

$x = -5 . 2^{-1}$

$x = 6.6 = 3$

second digit is 3

c) i) $168 = 2 \cdot 84$

$= 2^2 \cdot 42$

$= 2^3 \cdot 21$

$\boxed{= 2^3 \cdot 3 \cdot 7}$

ii) $\phi(168) = \phi(2^3 \cdot 3 \cdot 7)$

$= \phi(2^3)\,\phi(3)\,\phi(7)$

$= (2^3 - 2^2) \cdot 2 \cdot 6$

$= \boxed{48}$

iii) ~~$a^{n-1} = 1 \mod \phi(n)$~~

$\boxed{a^{\phi(n)} = 1 \mod n}$

$$11^{100} = 11^{2 \cdot 48 + 4}$$

$$\equiv \left(11^{48}\right)^2 11^4 \pmod{168}$$

$$\equiv 11^4 \pmod{168}$$

$$\equiv (-47)(-47)$$

$$\equiv (47)(47)$$

$$= \boxed{25}$$

Q 2(a)

$$A = \begin{pmatrix} 2 & 5 \\ 1 & 4 \end{pmatrix} \pmod{26}$$

$$A^{-1} = |A|^{-1} \begin{pmatrix} 4 & -5 \\ -1 & 2 \end{pmatrix}$$

$$A^{-1} = (2.4 - 1.5)^{-1} \begin{pmatrix} 4 & -5 \\ -1 & 2 \end{pmatrix} \pmod{26}$$

$$A^{-1} = 9 \begin{pmatrix} 4 & -5 \\ -1 & 2 \end{pmatrix} \pmod{26}$$

$$\boxed{A^{-1} = \begin{pmatrix} 10 & -19 \\ -9 & 18 \end{pmatrix}}$$

2a (ii)

$$f_E(U) = AU + \begin{pmatrix} 15 \\ 20 \end{pmatrix}$$

$$f_D(U) = A^{-1}\left(U - \begin{pmatrix} 15 \\ 20 \end{pmatrix}\right)$$

$$f_D\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 10 & -19 \\ -9 & 18 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} 10 & -19 \\ -9 & 18 \end{pmatrix}\begin{pmatrix} 15 \\ 20 \end{pmatrix}$$

$$= \text{etc.}$$

Q2 (h)

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 5 & 1 & 6 & 0 & 1 & 0 \\ 7 & 1 & 9 & 0 & 0 & 1 \end{array}\right) \sim$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & -4 & -5 & 1 & 0 \\ 0 & 1 & -5 & -7 & 0 & 1 \end{array}\right) \sim$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & -4 & -5 & 1 & 0 \\ 0 & 0 & -1 & -2 & -1 & 1 \end{array}\right) \sim$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & -4 & -5 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 & -1 \end{array}\right) \sim$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -3 & -2 & 2 \\ 0 & 1 & 0 & 3 & 5 & -4 \\ 0 & 0 & 1 & 2 & 1 & -1 \end{array}\right)$$

$$A^{-1} = \begin{pmatrix} -3 & -2 & 2 \\ 3 & 5 & -4 \\ 2 & 1 & -1 \end{pmatrix}$$