1. (a) $9 \bmod 4 = 1$

(b) $-9 \bmod 4 = 3$

(c) $2718 \bmod 47 = 39$

(d) $3^{17} \bmod 25 = 13$

$17 \to 10001$. $b=3$ $e=17$.

step 0: $R \leftarrow 1$. $x \leftarrow 3$

step 1: $R \leftarrow R \cdot x \pmod{25} \equiv 3 \pmod{25}$

$x \leftarrow x^2 \pmod{25} \equiv 9 \pmod{25}$

step 2: $x \leftarrow x^2 \pmod{25} \equiv 81 \pmod{25} \equiv 6 \pmod{25}$

step 3: $x \leftarrow x^2 \pmod{25} \equiv 36 \pmod{25} \equiv 11 \pmod{25}$

step 4: $x \leftarrow x^2 \pmod{25} \equiv 121 \pmod{25} \equiv 1 \pmod{25}$

step 5: $R \leftarrow R \cdot x \pmod{25} \equiv 63 \pmod{25} \equiv 13 \pmod{25}$

$\therefore 3^{17} \equiv 13 \pmod{25}$ ✻

(e) $d\log_{7,25} 18 = x \Rightarrow 18 = 7^x \bmod 25 \Rightarrow x = 3$ ✻.

2. $a=7467$ $b=2464$. $x_i a + y_i b = r_i$ for all i

i	r_i	q_i	x_i	y_i
-1	7467		1	0
0	2464		0	1
1	75	3	1	-3
2	64	32	-32	97
3	11	1	33	-100
4	9	5	-197	597
5	2	1	230	-697
6	1	4	-1117	3385
7	0	2	2464	-7467

$xa+yb=1$

$\Rightarrow x \equiv a^{-1} \bmod b$ $\therefore 2464 \equiv 7467^{-1} \bmod 2464$.

3. $4^{225} \bmod 17 = (4^{16})^{14} \cdot 4^{1} \bmod 17$

$= 1 \cdot 4 \bmod 17 = 4$ ✱

4. 18 is composite ⇒ use Euler's theorem.

$x^{\phi(18)} \equiv 1 \pmod{18} \Rightarrow x^{6} \equiv 1 \pmod{18}$

$x^{47} \pmod{18} \equiv (x^{6})^{8} \cdot x^{-1} \pmod{18} \equiv x^{-1} \pmod{18}$

$5 \equiv x^{-1} \pmod{18} \Rightarrow 5x \equiv 1 \pmod{18} \Rightarrow x = 11$ ✱

5.
$$\begin{cases} 3 = X \bmod 7 & M_1 = 132 & C_1 = 132^{-1} \bmod 7 = 6 \\ 5 = X \bmod 11 & M_2 = 84 & C_2 = 84^{-1} \bmod 11 = 8 \\ 2 = X \bmod 12 & M_3 = 77 & C_3 = 77^{-1} \bmod 12 = 5 \end{cases}$$

$x = (3 \times 132 \times 6 + 5 \times 84 \times 8 + 2 \times 77 \times 5) \bmod 924$

$\Rightarrow x = 6506 \bmod 924 = 38$ ✱

6. Phileas Fogg was not known to have either wife or children, which may happen to the most honest people; either relatives or near friends, which is certainly more unusual. He lived alone in his house in Saville Row, whither none penetrated. A single domestic sufficed to serve him. His breakfast and dined at the club, at hours mathematically fixed, in the same room at the same table, never taking his meals with other members, much less bringing a guest with him; and went home at exactly midnight, only to retire at once to bed. He never used the cosy chambers which the Reform provides for its favoured members. He passed ten hours out of the twenty-four in Saville Row, either in sleeping or making his toilet.

2. key = royal new zealand navy

R	O	Y	A	L
N	E	W	Z	D
V	B	C	F	G
H	I/J	K	M	P
Q	S	T	U	X

KXJEY UREBE ZWEHE WRYTU
PTBOA TONEO WENIN ELOST
HEYFS KREHE GOYFI WTTTU
INACT IONIN BLACK ESSST
OLKSY CAJPO BOTEI ZONTX
RAITT WOMIL ESSWM ERESU
BYBWT GONEY CUZWR GDSON
COCEX CREWO FTWEL VEXRE
SXBOU YWRHE BAAHY USEDQ
QUEST ANYIN FORMA TIONX

去除X佔位符號=

PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKESS STRAIT TWO MILES SW MERESU COCE CREW OF TWELVE REQUEST ANY INFORMATION.

8. plaintext: mee tme att heu sua lpl ace att enr ath ert han eig hta mzz.

$$[12\ 4\ 4]\begin{bmatrix}1&3&5\\2&4&6\\7&5&4\end{bmatrix}=[48\ 72\ 100]\bmod 26=[22\ 14\ 22]$$ W O W

$$[19\ 12\ 4]\begin{bmatrix}1&3&5\\2&4&6\\7&5&4\end{bmatrix}=[71\ 125\ 183]\bmod 26=[19\ 21\ 17]$$ T V R

$$[0\ 19\ 19]\begin{bmatrix}1&3&5\\2&4&6\\7&5&4\end{bmatrix}=[171\ 171\ 190]\bmod 26=[15\ 15\ 8]$$ P P I

$$[7\ 4\ 20]\begin{bmatrix}1&3&5\\2&4&6\\7&5&4\end{bmatrix}=[155\ 137\ 139]\bmod 26=[25\ 7\ 9]$$ Z H J

$$[18\ 20\ 0]\begin{bmatrix}1&3&5\\2&4&6\\7&5&4\end{bmatrix}=[58\ 134\ 210]\bmod 26=[6\ 4\ 2]$$ G E C

$$[11\ 15\ 11]\begin{bmatrix}1&3&5\\2&4&6\\7&5&4\end{bmatrix}=[118\ 148\ 189]\bmod 26=[14\ 18\ 7]$$ O S H

$$[0\ 2\ 4]\begin{bmatrix}1&3&5\\2&4&6\\7&5&4\end{bmatrix}=[32\ 28\ 28]\bmod 26=[6\ 2\ 2]$$ G C C

$$[0\ 19\ 19]\begin{bmatrix}1&3&5\\2&4&6\\7&5&4\end{bmatrix}=[171\ 171\ 190]\bmod 26=[15\ 15\ 8]$$ P P I

$$[4\ 13\ 17]\begin{bmatrix}1&3&5\\2&4&6\\7&5&4\end{bmatrix}=[169\ 149\ 166]\bmod 26=[13\ 19\ 10]$$
N T K

$$[0\ 19\ 7]\begin{bmatrix}1&3&5\\2&4&6\\7&5&4\end{bmatrix}=[87\ 111\ 142]\bmod 26=[9\ 7\ 12]$$
J H H

$$[4\ 17\ 19]\begin{bmatrix}1&3&5\\2&4&6\\7&5&4\end{bmatrix}=[170\ 175\ 198]\bmod 26=[14\ 19\ 16]$$
O T Q

$$[7\ 0\ 13]\begin{bmatrix}1&3&5\\2&4&6\\7&5&4\end{bmatrix}=[98\ 86\ 87]\bmod 26=[20\ 8\ 9]$$
U I J

$$[4\ 8\ 6]\begin{bmatrix}1&3&5\\2&4&6\\7&5&4\end{bmatrix}=[62\ 72\ 92]\bmod 26=[10\ 20\ 14]$$
K U O

$$[7\ 19\ 0]\begin{bmatrix}1&3&5\\2&4&6\\7&5&4\end{bmatrix}=[45\ 97\ 149]\bmod 26=[19\ 19\ 19]$$
T T T

$$[12\ 25\ 25]\begin{bmatrix}1&3&5\\2&4&6\\7&5&4\end{bmatrix}=[239\ 261\ 310]\bmod 26=[3\ 1\ 24]$$
D B Y

∴ Ciphertext: WOWTVRPPIZHJGECOSHGCCPPINTKJHHOTQ

UIJKUOTTTDBY

9. Key : H E L L O H E L L O H E L

Plain : C R Y P T O G R A P H I C

Cipher : J V J A H V K C L D O H N

10. (a) plain : s e n d m o r e m o n e y

18 4 13 3 12 14 17 4 12 14 13 4 24

key : 3 11 5 7 17 21 0 11 14 8 7 13 9

21 15 18 10 3 9 17 15 0 22 20 17 7

cipher : V P S K D J R P A W U R H

(b) cipher : V P S K O J R P A W U R H

21 15 18 10 3 9 17 15 0 22 20 17 7

plain : C a s h n o t n e e d e d

2 0 18 7 13 14 19 13 4 4 3 4 3

key : 19 15 0 3 16 21 24 2 22 18 17 13 4

11. $151-1=150=2^1\times 75$

Try $a=2$

$a^{150} \bmod 151 = 1$

$a^{75} \bmod 151 = 1$

→ no witness is found

2^{75} $75 \Rightarrow 1001011$

0: $R \leftarrow 1$ $x \leftarrow 2$

1: $R \leftarrow 1\times 2 \equiv 2 \pmod{151}$

$x \leftarrow 4 \pmod{151}$

2: $R \leftarrow 2\times 4 \equiv 8 \pmod{151}$

$x \leftarrow 16 \pmod{151}$

3: $x \leftarrow 256 \pmod{151} \equiv 105 \pmod{151}$

4: $R \leftarrow 8\times 105 \pmod{151} \equiv 85 \pmod{151}$

$x \leftarrow 105^2 \pmod{151} \equiv 2 \pmod{151}$

5: $x \leftarrow 4 \pmod{151}$

6: $x \leftarrow 16 \pmod{151}$

7: $R \leftarrow 85\times 16 \pmod{151} \equiv 1 \pmod{151}$

Try $a=11$

11^{75} $75 \Rightarrow 1001011$

$a^{150} \bmod 151 = 1$

$a^{75} \bmod 151 = 1$

→ no witness is found

0: $R \leftarrow 1$ $x \leftarrow 11$

1: $R \leftarrow 1 \times 11 \equiv 11 \pmod{151}$

$x \leftarrow 121 \pmod{151}$

2: $R \leftarrow 11 \times 121 \equiv 123 \pmod{151}$

$x \leftarrow 121^2 \pmod{151} \equiv 145 \pmod{151}$

3: $x \leftarrow 145^2 \pmod{151} \equiv 36 \pmod{151}$

4: $R \leftarrow 123 \times 36 \equiv 4428 \pmod{151} \equiv 49 \pmod{151}$

$x \leftarrow 36^2 \pmod{151} \equiv 88 \pmod{151}$

5: $x \leftarrow 88^2 \pmod{151} \equiv 43 \pmod{151}$

6: $x \leftarrow 43^2 \pmod{151} \equiv 37 \pmod{151}$

7: $R \leftarrow 49 \times 37 \equiv 1 \pmod{151}$

Try $a=3$

3^{75} $75 \Rightarrow 1001011$

$a^{150} \bmod 151 = 1$

$a^{75} \bmod 151 = -1$

→ no witness is found.

0: $R \leftarrow 1$ $x \leftarrow 3$

1: $R \leftarrow 3 \pmod{151}$

$x \leftarrow 9 \pmod{151}$

2: $R \leftarrow 27 \pmod{151}$

$x \leftarrow 81 \pmod{151}$

3: $x \leftarrow 81^2 \pmod{151} \equiv 68 \pmod{151}$

4: $R \leftarrow 27 \times 68 \pmod{151} \equiv 24 \pmod{151}$

$x \leftarrow 68^2 \pmod{151} \equiv 94 \pmod{151}$

5: $x \leftarrow 94^2 \pmod{151} \equiv 78 \pmod{151}$

6: $x \leftarrow 78^2 \pmod{151} \equiv 44 \pmod{151}$

7: $R \leftarrow 24 \times 44 \pmod{151} \equiv 150 \pmod{151} \equiv -1 \pmod{151}$

Since we found no witness. 151 is probably prime. ☆

11. $161-1=160=2^5\times 5$

Try $a=7$

$a^{160} \bmod 161=1$

$a^{80} \bmod 161=140$

→ 140 is a witness

∴ 161 is composite ✱

7^{80} $80\Rightarrow 1010000$

0: $R\leftarrow 1$ $x\leftarrow 7$

1: $x\leftarrow 49 \pmod{161}$

2: $x\leftarrow 49^2 \pmod{161}\equiv 147 \pmod{161}$

3: $x\leftarrow 147^2 \pmod{161}\equiv 35 \pmod{161}$

4: $x\leftarrow 35^2 \pmod{161}\equiv 98 \pmod{161}$

5: $R\leftarrow 98 \pmod{161}$

$x\leftarrow 98^2 \pmod{161}\equiv 105 \pmod{161}$

6: $x\leftarrow 105^2 \pmod{161}\equiv 77 \pmod{161}$

7: $R\leftarrow 98\times 77 \pmod{161}\equiv 140 \pmod{161}$