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

(b) $-9 \bmod 4 = 3$ or -1 #

(c) $2718 \bmod 47$

$\because 2718 = 9 \times 302$

$\therefore 2718 \bmod 47 = [(9 \bmod 47)(302 \bmod 47)] \bmod 47$

$\Rightarrow (9 \times 20) \bmod 47 = 180 \bmod 47 = 39$ #

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

$\Rightarrow (3^3)^5 \cdot 3^2 \bmod 25$

$= \{[(3^3 \bmod 25)^5 \bmod 25] \cdot 3^2 \bmod 25\} \bmod 25$

$= [(2^5 \bmod 25) \cdot (3^2 \bmod 25)] \bmod 25$

$= [(32 \bmod 25) \cdot (9 \bmod 25)] \bmod 25$

$= (7 \cdot 9) \bmod 25 = 63 \bmod 25 = 13$ #

(e) $d\log_{7,25} 18$

let $d\log_{7,25} 18 = x$, then $18 = 7^x \bmod 25$

for $x = 3$, $7^3 = 343$

$343 \bmod 25 = 18$

$\therefore d\log_{7,25} 18 = 3$ #

2. $7467^{-1} \bmod 2464$

We suppose an x, such that $x \cdot 7467 \equiv 1 \pmod{2464}$, which also means that there is a y, such that

$x \cdot 7467 = 1 + y \cdot 2464$,

$\Rightarrow x \cdot 7467 - y \cdot 2464 = 1 = \gcd(7467, 2464)$

let $x_1 = 1$, $y_1 = 0$, $x_2 = 0$, $y_2 = 1$

$7467 \bmod 2464 = 75$, $r_1 = 75$, $q_1 = 3$

$x_3 = x_1 - 3 \cdot x_2 = 1$

$y_3 = y_1 - 3 \cdot y_2 = -3$

$2464 \bmod 75 = 64$, $r_2 = 64$, $q_2 = 32$

$x_4 = x_2 - 32 x_3 = -32$

$y_4 = y_2 - 32 y_3 = 1 + 32 \cdot 3 = 1 + 96 = 97$

$75 \bmod 64 = 11$, $r_3 = 11$, $q_3 = 1$

$x_5 = x_3 - x_4 = 1 + 32 = 33$

$y_5 = y_3 - y_4 = -3 - 97 = -100$

$64 \bmod 11 = 9$, $r_4 = 9$, $q_4 = 5$

$x_6 = x_4 - 5x_5 = -32 - 5 \cdot 33 = -32 - 165 = -197$

$y_6 = y_4 - 5y_5 = 97 - 5 \times -100 = 597$

$11 \bmod 9 = 2$, $r_5 = 2$, $q_5 = 1$

$x_7 = x_5 - x_6 = 33 + 197 = 230$

$y_7 = y_5 - y_6 = -100 - 597 = -697$

$9 \bmod 2 = 1$, $r_6 = 1$, $q_6 = 4$

$x_8 = x_6 - 4x_7 = -197 - 4 \times 230 = -197 - 920 = -1117$

$y_8 = y_6 - 4y_7 = 597 + 4 \times 697 = 3385$

$2 \bmod 1 = 0$, $r_7 = 0$, $q_7 = 0$

$\because 2 \bmod 1 = 0$

$\therefore x7467 - y2464 = \gcd(7467, 2464) = 1$

and $\because -1117$ is a negative number

$\therefore$ we plus 2464 to -1117 equal 1347

$\Rightarrow x = 1347$ #

3. $4^{225} \bmod 17$

$= \{[(4^{16}) \bmod 17]^{14} (4 \bmod 17)\} \bmod 17$

for Fermat's theorem: $a^{p-1} \equiv 1 \bmod p$

$\therefore 4^{16} \bmod 17 = 1$

$= [(1)^{14} (4 \bmod 17)] \bmod 17$

$= 4$ #

4. $5 = x^{47} \bmod 18$

$\Rightarrow [x^{47} \equiv 5) \bmod 18$

$\phi(18) = 2^{1-1}(2-1) \cdot 3^{2-1}(3-1) = 6$

$\Rightarrow$ for $0 < a < 18$, $\gcd(a, 18) = 1$

we have $a^6 \equiv 1 \bmod 18$

take $a = 11$, $(11^6 \equiv 1) \bmod 18$, then $[(11^6)^7 \equiv 11^6] \bmod 18$

$\Rightarrow 11^{42} \bmod 18 = 1$

And $11^5 \bmod 18 = 5$

$\therefore [(11^{42} \bmod 18)(11^5 \bmod 18)] \bmod 18 = 5$

$\Rightarrow 11^{47} \bmod 18 = 5$

$\therefore X = 11$ #

5. $\begin{cases} 3 = x \bmod 7 \\ 5 = x \bmod 11 \\ 2 = x \bmod 12 \end{cases} \Rightarrow M = 924$

$M_1 = 132$, $M_2 = 84$, $M_3 = 77$

$M_1^{-1} \bmod 7 = 6$, $M_2^{-1} \bmod 11 = 8$, $M_3^{-1} \bmod 12 = 5$

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

$= (2376 + 3360 + 770) \bmod 924$

$= 6506 \bmod 924 = 38$ #

6. Using program to calculate the frequency of each alphabet.
The alphabet "n" has the most frequencies of others.
We suppose "n" as "e".
And we find "ozn" which appears for many times.
So, substitute "ozn" as "the".
At line four, there is a word for only one alphabet "q", it may be "a" or "I", at here, choosing "a"
Then suppose the third word at first line "wqc" as "was".
And another word "wzsxz" as "which".
After a few supposing substitution, we can decrypt this message

"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 non penetrated. a single domestic suffered to serve him. he breakfasted 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 favored members. he passed ten hours out of the twenty-four in saville row, either in sleeping or making his toilet." #

7.

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

ptboa toneo wenin elost inact
ionin black ettst raitt womil
esswm eresu cocex crewo ftwel
vexre guest anyin forma tionx
#

"pt boat one owe nine lost in action in blacket t strait two middles sw mere su cocex crew of twelve x reguest any information x" #

8. "mee tme att heu sua lpl ace att enr ath ert han eig hta m" + "zz"

$$\begin{bmatrix} 12 & 4 & 4 \\ 19 & 12 & 4 \\ 0 & 19 & 19 \\ 7 & 4 & 20 \\ 18 & 20 & 0 \\ 11 & 15 & 11 \\ 0 & 2 & 4 \\ 0 & 19 & 19 \\ 4 & 13 & 17 \\ 0 & 19 & 7 \\ 4 & 17 & 19 \\ 7 & 0 & 13 \\ 4 & 8 & 6 \\ 7 & 19 & 0 \\ 12 & 25 & 25 \end{bmatrix} \begin{bmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \\ 7 & 5 & 4 \end{bmatrix} \bmod 26 = \begin{bmatrix} 48 & 72 & 100 \\ 71 & 125 & 183 \\ 171 & 171 & 190 \\ 155 & 137 & 139 \\ 58 & 134 & 240 \\ 118 & 148 & 189 \\ 32 & 28 & 28 \\ 171 & 171 & 190 \\ 149 & 149 & 166 \\ 87 & 111 & 142 \\ 171 & 175 & 198 \\ 98 & 86 & 87 \\ 62 & 74 & 92 \\ 95 & 97 & 149 \\ 237 & 261 & 310 \end{bmatrix} \bmod 26 = \begin{bmatrix} 22 & 20 & 22 \\ 19 & 21 & 1 \\ 15 & 15 & 8 \\ 25 & 7 & 9 \\ 6 & 4 & 2 \\ 14 & 18 & 7 \\ 6 & 2 & 2 \\ 15 & 15 & 8 \\ 19 & 19 & 10 \\ 9 & 7 & 12 \\ 15 & 19 & 16 \\ 20 & 8 & 9 \\ 10 & 22 & 14 \\ 19 & 19 & 19 \\ 3 & 1 & 24 \end{bmatrix}$$

Then translate the numbers to alphabets.
We can get the answer:

WLJW TVB PPI ZHJ GEC OSH GCC PPI TTK JHM PTQ LJI KWO TTT DBY #

9. Key: hello ⇒ 7,4,11,11,14
Word: cryptographic

⇒ encrypt: JVJAHVKCLDOMN#

10.(a)

	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
+	3	11	5	7	17	21	0	11	14	8	7	13	9
=	21	15	18	10	29	35	17	15	26	22	20	17	33
mod 26	21	15	18	10	3	9	17	15	0	22	20	17	7
⇒	V	P	S	K	D	J	R	P	A	W	U	R	H

⇒ encrypt: VPSKDJRPAWURH#

(b)

	V	P	S	K	D	J	R	P	A	W	U	R	H
⇒	21	15	18	10	3	9	17	15	0	22	20	17	7
−	2	0	18	7	13	14	19	13	4	4	3	4	3
=	19	15	0	3	-10	-5	-2	2	-4	18	17	13	4
mod 26	19	15	0	3	16	21	24	2	22	18	17	13	4

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

11. |5|:
I. |5|−1 = 150 = 2×75
II. let a = 43
$43^{150} \bmod |5| = 1$
$43^{75} \bmod |5| = 1$

let a = 98
$98^{150} \bmod |5| = 1$
$98^{75} \bmod |5| = 1$

let $a = 25$

$25^{150} \bmod |5| = 1$

$25^{75} \bmod |5| = 1$

let $a = 129$

$129^{150} \bmod |5| = 1$

$129^{75} \bmod |61| = -1$

From I and II, we can conclude $|5|$ is probably a prime number. ✌

$|61|$:

I. $|61| - 1 = 2^5 5$

II. let $a = 15$

$$\begin{aligned} 15^{160} \bmod |61| &= (15^5 \bmod |61|)^{2^5} \bmod |61| \\ &= (99^2 \bmod |61|)^{2^4} \bmod |61| \\ &= (14^2 \bmod |61|)^{2^3} \bmod |61| \\ &= (78^2 \bmod |61|)^{2^2} \bmod |61| \\ &= (127^2 \bmod |61|)^2 \bmod |61| \\ &= 29^2 \bmod |61| \\ &= 36 \end{aligned}$$

$36 \neq 1$, from Fermat's Little Theorem, we can have the answer that $|61|$ is not a prime number. ✌