1.

a. 1

b. 3

c. 39

d. $3^{17} \bmod 25 = \{(3 \bmod 25) \cdot [(3^4 \bmod 25)^4 \bmod 25] \bmod 25\}$

$= [3 \cdot (6^2 \bmod 25)^2 \bmod 25] \bmod 25$

$= [3 \cdot (121 \bmod 25)] \bmod 25$

$= 63 \bmod 25$

$= 13$ #

e. $X = \log_{7,25} 18 \Rightarrow 7^X \bmod 25 = 18$

$\Rightarrow X = 3$ #

2. $x = 7467^{-1} \bmod 2464 \Rightarrow 7467x + 2464y = 1$

r	q	x	y
7467	x	1	0
2464	x	0	1
75	3	1	-3
64	32	-32	97
11	1	33	-100
9	5	-197	597
2	1	230	-697
1	4	-1117	3385

$x = -1117 + 2464n, n \in \mathbb{Z}$ #

3. Fermat's theorem : $\begin{cases} a^{p-1} \equiv 1 \pmod{p} \\ a^p \equiv a \pmod{p} \end{cases}$, if p is prime and $a \neq p$

$$4^{225} \bmod 17 = \{(4^4 \bmod 17)[(4^{13})^{17} \bmod 17]\} \bmod 17$$

$$= \{(4^4 \bmod 17) \cdot (4^{13} \bmod 17)\} \bmod 17$$

$$= 4^{17} \bmod 17$$

$$= 4$$

#

4. Euler's theorem : $\begin{cases} a^{\phi(n)} \equiv 1 \pmod n \\ a^{\phi(n)+1} \equiv a \pmod n \end{cases}$, if $\gcd(a,n)=1$

$\phi(18)=6 \Rightarrow x^6 \bmod 18 = 1$

$5 = x^{47} \bmod 18 \neq \{[(x^6 \bmod 18)^7 \bmod 18] \cdot (x^5 \bmod 18)\} \bmod 18$

$= x^5 \bmod 18$

$\Rightarrow 5x \bmod 18 = 1$

$\Rightarrow 5x + 18y = 1$

r	q	x	y
18	X	0	1
5	X	1	0
3	3	-3	1
2	1	4	-1
1	1	-7	2

$x = -7 + 18n, n \in \mathbb{Z}$

#

5. $M = 7 \cdot 11 \cdot 12 = 924$

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

$132C_1 + 7y = 1$

r	q	C_1	y
132	X	1	0
7	X	0	1
6	18	1	-18
1	1	-1	19

$C_1 = -1$

$84C_2 + 11y = 1$

r	q	C_2	y
84	X	1	0
11	X	0	1
7	7	1	-7
4	1	-1	8
3	1	2	-15
1	1	-3	23

$C_2 = -3$

$77C_3 + 12y = 1$

r	q	C_3	y
77	X	1	0
12	X	0	1
5	6	1	-6
2	2	-2	13
1	2	5	-32

$C_3 = 5$

$X = 3 \cdot 132 \cdot (-1) + 5 \cdot 84 \cdot (-3) + 2 \cdot 77 \cdot 5 + 924n$

$= -396 - 1260 + 770 + 924n$

$= -886 + 924n$ #

6. By frequency test, n is the letter appears the most frequent so guess that n → e, and q → a, 0z → th ... and then gradually decrypt the message by the corresponding table:

a → x		q → a	y → g
b → d	j → r	r → l	z → h
c → s	k → f	s → i	
d → v	l → o		
e → u	m → k		
f → n	n → e	v → y	
g → m	o → t	w → w	
h → p	p → b	x → c	

plaintext:

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. 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 favoured 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 QUEST ANYIN FORMATIONX

=> PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKETT STRAIT TWO MILES SW MERESU COCE X CREW OF TWELVE X REQUEST ANY INFORMATION X #

8.

$$\begin{bmatrix} 12 & 4 & 4 \\ 19 & 12 & 4 \\ 0 & 19 & 19 \\ 7 & 4 & 20 \\ 18 & 20 & 0 \\ 11 & 15 & 11 \\ 0 & 2 & 4 \\ 0 & 19 & 19 \\ 4 & 13 & 17 \\ 0 & 19 & 7 \\ 4 & 17 & 19 \\ 7 & 0 & 13 \\ 4 & 8 & 6 \\ 7 & 19 & 0 \\ 12 & 25 & 25 \end{bmatrix} \begin{bmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \\ 7 & 5 & 4 \end{bmatrix} \equiv \begin{bmatrix} 22 & 20 & 22 \\ 19 & 21 & 1 \\ 15 & 15 & 8 \\ 25 & 7 & 9 \\ 6 & 4 & 2 \\ 14 & 18 & 7 \\ 6 & 2 & 2 \\ 15 & 15 & 8 \\ 19 & 19 & 10 \\ 9 & 7 & 12 \\ 15 & 19 & 16 \\ 20 & 8 & 9 \\ 10 & 22 & 14 \\ 19 & 19 & 19 \\ 3 & 1 & 24 \end{bmatrix} \pmod{26}$$

=> wuwt vb pp izh jgeco shgcc pp itt kjhmpt guij kwott td by #

9. using pseudo code below to run:

```
string s = "cryptographic"
string key = "hellohellohel"
for i to s.size
    int tmp = key[i] - 'a' + s[i]
    if (tmp > 'z') tmp -= 26
    cout << (char) tmp
```

result: jvjahvkcldomn #

10.

a. using the below pseudo code to run:

```
string s = "sendmoremoney"
for i to s.size
    int key
    cin >> key
    int tmp = s[i]+key
    if(tmp > 'z') tmp -= 26
    cout << (char) tmp
```

result: vpskdjrpawurh #

b. using the below pseudo code to run:

```
string s = "vpskdjrpawurh"
string p = "cashnotneeded"
for i to s.size
    if(s[i] > p[i]) cout << s[i]-p[i]
    else cout << s[i]-p[i]+26
    cout << " "
```

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

#

11. pick $a = 392$

$392^{150} \bmod 151 = 1$

$392^{75} \bmod 151 = 1$

pick $a = 2185$

$2185^{150} \bmod 151 = 1$

$2185^{75} \bmod 151 = -1$

pick $a = 661$

$661^{150} \bmod 151 = 1$

$661^{75} \bmod 151 = -1$

pick $a = 8000$

$8000^{150} \bmod 151 = 1$

$8000^{75} \bmod 151 = 1$

Therefore, we guess that 151 is a prime number #

pick $a = 147$

$147^{160} \bmod 161 = 49$

Therefore, 161 is a composite number #