1 – letter

The first digit is the number of months in two years mod 5.
24 mod 5 = **4**

To obtain the second digit, take the number of the letters in alphabet, divide it by the number of the consonants (assume 'y' is a vowel) and take the biggest integer smaller than the result.
26/20 = 1.3 » 1

For 3rd and 4th digit: there is no unique answer for these, so make sure you calculate them correctly!

2 – symbolic cipher

Find the objects on the map and write down their location (e.g. A5)

Object	location
1. Tower Bridge	H6
2. Big Ben	D7
3. Madame Tussauds	A3
4. The Globe	F6

P.S. recall Caesar cipher to decipher the text!

3 – Caesar cipher

Xvh wkh orfdwlrqv ri wkh remhfwv wr ghflskhu d phhwlqj sodfh.
Use the locations of the objects to decipher a meeting place.

Fkdqjh ohwwhuv lqwr qxpehuv (l.h. D=0, E=1...).
Change letters into numbers (i.e. A=0, B=1...).

Glylgh wkh qxpehu lqwr 4 hyhq fkxqnv (h.j. 1245 → 12, 45; 357233 → 35, 72, 33).
Divide the number into 4 even chunks (e.g. 1245 → 12, 45; 357233 → 35, 72, 33).

Sxeolf nhb lv (123, 22), sulydwh nhb lv 28.
Public key is (123, 22), private key is 28.

Ghflskhu whaw: V=0, X=1, G=2, F=3, Q=4, P=5, O=6, D=7, H=8, U=9.
Decipher text: S=0 U=1, D=2, C=3, N=4, M=5, L=6, A=7, E=8, R=9.

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

[Notice: there are two ways of deciphering the message: you can either take the first letter and decipher it, then the second one, then the third one etc. (i.e. do it linearly) or you can use the fact that most of the letters repeat, so when you decipher one, you write down the letter corresponding to it below every occurrence of that particular letter – decryption may be more chaotic at first, but is also faster.]

3 – letter – meeting place

Need to decrypt: H6 - D7 - A3 - F6
A = 0, B = 1, C = 2, D = 3, E = 4, F = 5, G = 6, H = 7
The numerical code is: 76 - 37 - 03 - 56
Public key is (123, 22), private key is 28.
Hence, n = 123 and d = 28

$P_i = C_i \times d \ (mod\ n)$

$P_1 = 76 \times 28 \ (mod\ 123) = 2128 \ (mod\ 123) = 37$

$P_2 = 37 \times 28 \ (mod\ 123) = 1036 \ (mod\ 123) = 52$

$P_3 = 3 \times 28 \ (mod\ 123) = 84 \ (mod\ 123) = 84$

$P_4 = 56 \times 28 \ (mod\ 123) = 1568 \ (mod\ 123) = 92$

The decrypted number is: 37 - 52 - 84 – 92
Recall: S=0 U=1, D=2, C=3, N=4, M=5, L=6, A=7, E=8, R=9
This corresponds to: CA - MD - EN – RD

** The choice of private and public key (i.e. the choice of *e, d* and *n*) is determined by four numbers (*a, b, A, B*), which generally are quite big, but in our examples are small, just to make things simpler. For more information about the calculation, see: Lecture → Background material → 4. Kid-RSA

$$\boldsymbol{a = 2,\ b = 3, A = 4, B = 5}$$
$$\boldsymbol{M = a \times b - 1 = 2 \times 3 - 1 = 6 - 1 = 5}$$
$$\boldsymbol{e = A \times M + a = 4 \times 5 + 2 = 20 + 2 = 22}$$
$$\boldsymbol{d = B \times M + b = 5 \times 5 + 3 = 25 + 3 = 28}$$
$$\boldsymbol{n = \frac{e \times d - 1}{M} = \frac{22 \times 28 - 1}{5} = \frac{615}{5} = 123}$$

4 – letter

Again: S=0 U=1, D=2, C=3, N=4, M=5, L=6, A=7, E=8, R=9

Original message	encrypted message
Name: Acer	4758: 7389
Land: Sudan	6742: 01274
Care Needed	3798 488282
Demand Alarm	285742 76795

Divide the message into chunks (bold numbers correspond to even lines of text):
(Each number must be the highest possible, but still smaller than $132 - 1 = 131$;
'01' appears in the text, since '012' or '0127' wouldn't make much sense.)

47 - 58 - 73 - 89 - **67 - 42 - 01 - 27 - 4**3 - 79 - 84 - 88 - 28 - 2**2 - 85 - 74 - 27 - 67 - 95**

The public key is (132, 37) $\Rightarrow n = 132, e = 37$

$C_i = P_i \times e\ (mod\ n)$
$C_1 = 47 \times 37\ (mod\ 132) = 1739\ (mod\ 132) = 23$
$C_2 = 58 \times 37\ (mod\ 132) = 2146\ (mod\ 132) = 34$

$$C_3 = 73 \times 37\ (mod\ 132) = 2701\ (mod\ 132) = 61$$
$$C_4 = 89 \times 37\ (mod\ 132) = 3293\ (mod\ 132) = 125$$
$$C_5 = 67 \times 37\ (mod\ 132) = 2479\ (mod\ 132) = 103$$
$$C_6 = 42 \times 37\ (mod\ 132) = 1554\ (mod\ 132) = 102$$
$$C_7 = 1 \times 37\ (mod\ 132) = 37\ (mod\ 132) = 37$$
$$C_8 = 27 \times 37\ (mod\ 132) = 999\ (mod\ 132) = 75$$
$$C_9 = 43 \times 37\ (mod\ 132) = 1591\ (mod\ 132) = 7$$
$$C_{10} = 79 \times 37\ (mod\ 132) = 2923\ (mod\ 132) = 19$$
$$C_{11} = 84 \times 37\ (mod\ 132) = 3108\ (mod\ 132) = 72$$
$$C_{12} = 88 \times 37\ (mod\ 132) = 3256\ (mod\ 132) = 88$$
$$C_{13} = 28 \times 37\ (mod\ 132) = 1036\ (mod\ 132) = 112$$
$$C_{14} = 22 \times 37\ (mod\ 132) = 814\ (mod\ 132) = 22$$
$$C_{15} = 85 \times 37\ (mod\ 132) = 3145\ (mod\ 132) = 109$$
$$C_{16} = 74 \times 37\ (mod\ 132) = 2738\ (mod\ 132) = 98$$
$$C_{17} = 27 \times 37\ (mod\ 132) = 999\ (mod\ 132) = 75$$
$$C_{18} = 67 \times 37\ (mod\ 132) = 2479\ (mod\ 132) = 103$$
$$C_{19} = 95 \times 37\ (mod\ 132) = 3515\ (mod\ 132) = 83$$

Therefore, the encrypted message is:
23 - 34 - 61 - 125 - 103 - 102 - 37 - 75 - 07 - 19 - 72 - 88 - 112 - 22 - 109 - 98 - 75 - 103 – 83

** Notice that even though the numbers we use are exactly the same as previously (i.e. 2, 3, 4, 5), different substitution to *a, b, A, B* gives completely different values of the private and public key. For more information about the calculation, see: Lecture → Background material → 4. Kid-RSA

$$\boldsymbol{a = 2,\ b = 4, A = 5, B = 3}$$
$$\boldsymbol{M = a \times b - 1 = 2 \times 4 - 1 = 8 - 1 = 7}$$
$$\boldsymbol{e = A \times M + a = 5 \times 7 + 2 = 35 + 2 = 37}$$
$$\boldsymbol{d = B \times M + b = 3 \times 7 + 4 = 21 + 4 = 25}$$
$$\boldsymbol{n = \frac{e \times d - 1}{M} = \frac{37 \times 25 - 1}{7} = \frac{924}{7} = 132}$$