Mathematics A Assignment 11 (week 48)

Group 1 (Tue 30/11, 12–14), Group 2 (Thu 2/12, 12–14), Group 3 (Fri 3/12, 8–10)

1.

```
THIS IS A VERY SECRET MESSAGE
GCRF RF K BZJQ FZOJZG AZFFKHZ
```

2. a) The number of letters in words is not the same; b) Secret message `OXAO` contains two `O`'s, but in `JOHN` all letters are different.

3. There was a hint which said that "The three most frequently occurring letters in the above text agree with the graph in Figure 1 of lecture notes." The three most frequent letters in the text are: `Z` (19 times), `C` (16 times), and `U` (12 times). In Figure 1, we see that the three most frequent letters in English are `E`, `T`, `A`. Therefore, we get `Z` $\leftrightarrow$ `E`, `C` $\leftrightarrow$ `T` and `U` $\leftrightarrow$ `A`.

If we look at the text, there are two different one-letter words. The other we only know, and it should be clear what the other is. After we replace the known letters, we see that there are several instances of the `T?E` and `T?`. In this way, one can proceed. The message is

```
LAST NIGHT I DREAMT I
WENT TO MANDERLEY AGAIN.
IT SEEMED TO ME I STOOD
BY THE IRON GATES LEADING
TO THE DRIVE AND FOR A
WHILE I COULD NOT ENTER
THE WAY WAS BARRED
TO ME.
```

4. An easy way is to write a short Python script:

```
for n in range(2, 982340323):
    if 982340323 % n == 0:
        print(n)
```

It prints the numbers:

```
1459
673297
```

5. a) $n = 109 \cdot 131 = 14279$ and $\phi = (109 - 1) \cdot (131 - 1) = 14279 = 14040$.

b) Let us select $e = 12473$. Now $\gcd(14040, 12473) = 1$:

$$\begin{aligned}
14040 &= 1 * 12473 + 1567\\
12473 &= 7 * 1567 + 1504\\
1567 &= 1 * 1504 + 63\\
1504 &= 23 * 63 + 55\\
63 &= 1 * 55 + 8\\
55 &= 6 * 8 + 7\\
8 &= 1 * 7 + 1\\
7 &= 7 * 1 + 0
\end{aligned}$$

c) $C = \mathrm{rem}(9876^{12473}, 14279)$. We can compute this using Python:

```
>>> pow(9876, 12473, 14279)
8431
```

6. a) We have

$$\begin{aligned}
1 &= 8 - 7 = (63 - 55) - (55 - 6 * 8) = 63 - 2 * 55 + 6 * (63 - 55) = 7 * 63 - 8 * 55\\
&= 7 * (1567 - 1504) - 8 * (1504 - 23 * 63)\\
&= 7 * 1567 - 15 * 1504 - 8 * (-23 * (1567 - 1504))\\
&= (7 + 8 * 23) * 1567 + (-15 - 8 * 23) * 1504 = 191 * 1567 - 199 * 1504\\
&= 191 * (14040 - 12473) - 199 * (12473 - 7 * 1567)\\
&= 191 * (14040 - 12473) - 199 * (12473 - 7 * (14040 - 12473))\\
&= (191 + 199 * 7) * 14040 - (191 + 199 + 199 * 7) * 12473\\
&= 1584 * 14040 - 1783 * 12473
\end{aligned}$$

The multiplicative inverse of 12473 is $-1783 \equiv 12257 \bmod \phi$.
b) Using Python we have:

```
>>> pow(8431, 12257, 14279)
9876
```

We managed to get back the original message!