1. Encode the following text using the substitution key described in page 1 of the RSA lecture notes.

```
THIS IS A VERY SECRET MESSAGE
```

2. If a simple substitution encoding (letter is encoded to a letter) is used (with an unknown key) and you are able to catch a secret message `OXAO`, then explain why you can be confident that the plaintext is not (a) `CAR` or (b) `JOHN`.

3. Solve the following code. We know that the text is English and the blanks betweeen the words are in their correct spots. Simple substitution is used.

```
A U H C    M V K F C    V    B Y Z U G C    V

I Z M C    C J    G U M B Z Y A Z D    U K U V M.

V C    H Z Z G Z B    C J    G Z    V    H C J J B

P D    C F Z    V Y J M    K U C Z    A Z U B V M K

C J    C F Z    B Y V W Z    U M B    O J Y    U

I F V A Z    V    T J N A B    M J C    Z M C Z Y

O J Y    C F Z    I U D    I U H    P U Y Y Z B

C J    G Z.
```

Hint: The three most frequently occurring letters in the above text agree with the graph in Figure 1 of lecture notes. Replace these in the text first.

4. We know that the number $n = 982\,340\,323$ is a product of two primes p and q. What these primes are? How did you found them?

5. RSA encryption. Suppose that $p = 109$ and $q = 131$ are two primes.

(a) Compute n and ϕ.
(b) Select a suitable public encryption key e.
(c) Encrypt the message $M = 9876$

6. RSA decryption.

(a) Compute the decryption key d corresponding your encryption key e of Excercise 5.
(b) Decrypt your segret message obtained in 5(c). Did you manage to get the original message?