1. An RSA cryptosystem has public key $N = 35$ and $e = 7$. Messages are encrypted one letter at a time, converting letters to numbers by $A = 2, B = 3, ..., Z = 27$, space = 28.

(a) Showing your working, encrypt the message: BE GOOD.
(b) Find the decryption exponent $d$ and decrypt the message: $20 \ 23 \ 26 \ 7 \ 15 \ 16$
(c) This choice of $N$ and $e$ has several weaknesses - name at least two different ones.
(d) Even if a good choice of $N$ and $e$ is made, the method of encrypting one letter at a time has weaknesses. Describe how we might find the plaintext if a very long ciphertext is given.
(e) Eve intercepts the RSA message $365, 0, 4845, 14930, 2608, 2608, 0$ sent from Alice to Bob. Alice and Bob are not using the scheme above. How does it seem they are converting letters to numbers? Decrypt the message.

2. (a) Suppose Alice uses RSA to send the same message $x$ (e.g. her credit card number), encrypted, to three companies, all of which use the easy choice of $e = 3$ in their public key. Eve intercepts these encrypted messages, i.e. $x^3 \pmod{N_1}, x^3 \pmod{N_2}, x^3 \pmod{N_3}$, where $N_1, N_2, N_3$ are the moduli used in the companies’ public keys (all $> x$). There is a method (the Chinese Remainder Theorem) by which she can use these to deduce the value of $x^3 \pmod{N_1N_2N_3}$. Assuming this can be done, explain how she can now compute $x$ exactly. This is one reason why $e = 3$ is a poor choice in practice.
(b) A popular choice for $e$ is 65537. What is special about this value of $e$ (as opposed to nearby values) that makes it a good choice?