3.2 Question 2

Suppose Bob uses the RSA cryptosystem with a very large modulus *n* for which the factorization cannot be found in a reasonable amount of time. Suppose Alice sends a message to Bob by representing each alphabetic character as an integer between 0 and 25 (A→0,...,Z→25) and then encrypting each number separately using RSA with large *e* and large *n*.

3.2.A Is this method secure?

No, it is not secure!

3.2.B If not, describe the most efficient attack against this encryption method.

The simplest attack would be that an intruder computes $m^e \ mod \ n$, for all possible values of m. This does not take much time because m has only 26 values. Then the intruder can create a decryption table in which the decryption of $m^e \ mod \ n$ is m.