**Question 1**

Textbook RSA is not secure, the encryption susceptible to several attacks, this is because it is malleable and deterministic. The attacks are common modulus, known-plaintext attack and chosen-ciphertext attack. The scenario in question gives each user a different modulus and decryption exponent, but all users are given the same encryption exponent. This exponent is a low number, 3, it also makes it easy to decrypt the cipher text without using the secret key because m is small also. By simply , this will the plain text message.

**Question 3**

To make textbook RSA a CPA-secure encryption it should combined with other schemes such as Optimal Asymmetric Encryption Padding (OAEP), where the padded message is passed through 2 random oracles then xor together to produce the cipher text.