

Section 6 Lecture 39 – RSA Messaging - Exercises

Q1)

Work through all the steps of the RSA algorithm with the following value of p , q and e chosen by Bob, and message m from Alice:

- (i) $p = 3, q = 7, e = 5, m = 3$
- (ii) $p = 5, q = 13, e = 7, m = 5$
- (iii) $p = 11, q = 5, e = 3, m = 10$

Q2)

(i)

What is unusual (and extremely undesirable) about the encrypted message in Q1(iii)? Do you think this is likely to happen for large numbers?

(ii)

In Q1(ii), Bob chose $e = 7$. Why would values of (a) $e = 3$ and (b) $e = 61$ not have been suitable choices?