Week 5 COMP90043

RSA Exercise

Q1. RSA Parameter creation: Fill in the blanks:

p =13 q = 7 n = 91 phi(n) = 72

Choose e= 5. Repeat for e =7

How to determine d such that de = 1 mod n? Use Euclid's algorithm

GCD (72, 5) GCD(72, 7)

72 = 14 x 5 + 2 72 = ___ x 7 + 2___

5 = 2 x 2 + 1

2 = 2 x 1 + 0

Back substitution:

1 = 5 – 2 x 2

1 = 5 – 2 [72 – 14 x 5]

1 = 5 [1+ 28] – 2 x72

Hence d = 29

Show that the RSA encryption and decryption functions are inverse operations by trying with some example messages. You can use the package magma online (http://magma.maths.usyd.edu.au/calc/).

Q2. Repeat the steps above another example below:

p =23 q = 37 n = _____ phi(n) = _____

Choose e= 5. Choose e = 61

GCD (, 5) GCD(, 61)