

## Ciphers and Number Theory 7

1. Calculate the following using fast exponentiation.
  - (a)  $27^{89} \bmod 101$ .
  - (b)  $35^{111} \bmod 89$ .
2. Bob wishes to use the RSA cryptosystem. He chooses primes 11 and 13.
  - (a) Determine which of the following is suitable for use as a public key with  $n = 11 \times 13$ .
    - i.  $e = 5$ .
    - ii.  $e = 7$ .
  - (b) Calculate the private key associated with this choice of public key.
  - (c) Show how to encode  $m = 35$ .
  - (d) Verify that the private key does decode the encrypted form of  $m$ .
3. Repeat the steps in Q2 for the following data:
  - (a)  $n = 17 \times 31$ ,  $e = 11$  and  $m = 4$ .
  - (b)  $n = 19 \times 29$ ,  $e = 5$  and  $m = 101$ .