Chapter 9 Homework

Homework - RSA

1. Test all odd numbers in the range from 233 to 241 for primality using the Miller-Rabin test with base 2
2. Encrypt the message M = 2 using RSA with the following parameters
   – n=56153, e = 23
3. Compute a private key (d, p, q) corresponding to the public key
   – Hint: p and q are in the above range
4. Decrypt the ciphertext obtained above using the CRT

Homework - RSA

- Due date
  - 2017. Nov. 15, 23:59
  - Upload your answer into the Blackboard