**Class Activity – 14 – RSA**

1. The RSA system was used to encrypt the message M into the cipher-text C= 9. The public key is given by n= 143 and e= 23. In the following, we will try to crack the system and to determine the original message M.
   1. What parameters comprises the public key and what parameters the private key?
   2. What steps are necessary to determine the private key from the public key?
   3. Determine the private key for the given system.
   4. What is the original message M?
2. The RSA system was used to encrypt the message M into the cipher-text C= 122. The public key is given by n=221 and e= 13. In the following, we will try to crack the system and to determine the original message M.
   1. What parameters comprises the public key and what parameters the private key?
   2. What steps are necessary to determine the private key from the public key?
   3. Determine the private key for the given system.
   4. What is the original message M?
3. In this exercise, the RSA algorithm is used. For each of the following cases, calculate pq, the totient value ф(n), the private key d, and the ciphertext C of the message M, given the values of p, q, and public key e.
4. p =7, q = 11, e = 17; M = 8.
5. p = 11, q = 13, e = 11; M = 7.
6. p = 17, q = 31, e = 7; M = 2.
7. Consider the RSA algorithm. Let the two prime numbers, p=11 and q=41. You need to derive appropriate public key (e,n) and private key (d,n).
   1. Can we pick e=5? If yes, what will be the corresponding (d,n)?
   2. Can we pick e=17? If yes, what will be the corresponding (d,n)?
   3. Use e=17, how to encrypt the number 3? You do not need to provide the encrypted value.



