Sheet #4

1. State the problems exist in the symmetric key cryptography and discuss how the public key cryptography solved these problems.
2. Prove the correctness of RSA (**you don't have to prove in case of GCD(m,N)≠1**).
3. In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M?
4. Suppose Bob uses the RSA cryptosystem with a very large modulus n for which the factorization cannot be found in a reasonable amount of time. Suppose Alice sends a message to Bob by representing each alphabetic character as an integer between 0 and 25(A ,..., Z), and then encrypting each number separately using RSA with large e and large n. Is this method secure? If not, describe the most efficient attack against this encryption method.
5. In an RSA system, the public key of a given user is e = 31, n = 3599. What is the private key of this user? Hint: You will need extended Euclidean algorithm to find the multiplicative inverse of 31 modulo f(n).
6. Given **Public key:** (N, e) = (33, 3) and **Private key:** d = 7
    a. Suppose message M = 8 Find C.
    b. Decrypt C to recover the message M