Tutorial Questions

Cryptography and Network Security

Date: 2/11/23 and 9/11/23

Q1. In a PKS (Public Key System) using RSA, you intercept the ciphertext C = 10 sent to the user whose public key is e = 5, n = 35. What is the plaintext M?

Q2. In a RSA system, the public key of a given user is e = 31, x = 3599. What is the private key of this user?

Q3. Suppose we have a set of blocks, encoded with the RSA algorithm and we don’t have the private key. Suppose also someone tells us they know one of the plaintext blocks has a common factor with “n”. Does this help us in any way?

Q4. In the RSA, public key encryption scheme, each user has a public key e and a private key d. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to generate new e and d. Is this safe?