UEE4611 Assignment #7, 2020 due May 28

---

1. In an RSA system, the public key of a given user is $e = 65$, $n = 2881$. What is the private key of this user? Hint: First use trial-and-error to determine p and q; then use the extended Euclidean algorithm to find the multiplicative inverse of 65 modulo $\phi(n)$. (10%)

2. 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 ($A \to 0, \ldots, Z \to 25$) and then encrypting each number separately using RSA with large e and large n. Is this method secure? If not, describe an efficient attack against this encryption method. (10%)

3. Use the fast exponentiation algorithm of Figure 9.8 to determine $6^{472} \bmod 3415$. (10%)

4. This problem illustrates a simple application of the chosen ciphertext attack. Bob intercepts a ciphertext C that is intended for Alice and encrypted with Alice's public key e. Bob wants to obtain the original message $M = C^d \mod n$ but he does not know the private key d. Bob chooses a random value r less than n and computes

$$\begin{aligned} Z &= r^e \mod n \\ X &= ZC \mod n \\ t &= r^{-1} \mod n \end{aligned}$$

   Next, Bob gets Alice to authenticate (sign) X with her private key (as in Figure 9.3), thereby decrypting X. Alice returns $Y = X^d \mod n$. Show how Bob can use the information now available to him to determine M. (10%)