UEE4611 Assignment #7 Solution

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 $\phi(n)$.

$n = p \times q$.
$\phi(n) = (67 - 1)(43 - 1) = 2772$.
By trial=and-error, we get $p = 43, q = 67$.
Then we applied Extended Euclidean algorithm, and will get $65^{-1} \equiv 725 \mod 2772$.

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 $(A \to 0, ..., Z \to 25)$ 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.

The method is not secure.
The set of corresponding ciphertext block values are $\{0^e \mod n, 1^e \mod n, ..., 25^e \mod n\}$, with the knowledge of public key, they can be easily computed.
Compute $M^e \mod n$ for all M, then create a table based on the relationship.
We can easily attack this encryption method with the table.

3. Use the fast exponentiation algorithm of Figure 9.8 to determine $6^{472} \mod 3415$.

$a = 6, b = 472 = 111011000, n = 3415$

i	8	7	6	5	4	3	2	1	0
b_i	1	1	1	0	1	1	0	0	0
c	1	3	7	14	29	59	118	236	472
f	6	216	3321	2006	166	1416	451	1916	3346

$6^{472} \mod 3415 = 3346.$

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

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

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.

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

$$\begin{aligned} \because X &= ZC \\ Y &\equiv X^d (\mod n) \\ &\equiv (ZC)^d (\mod n) \\ &\equiv Z^d c^d (\mod n) \end{aligned}$$

$$\begin{aligned} Y &\equiv rM (\mod n) \\ M &\equiv r^{-1} Y \equiv tY (\mod n) \end{aligned}$$