University of Nevada, Las Vegas Las Vegas Computer Science 477/677 Fall 2019

Assignment 2: Due Wednesday September 4, 2019

Name:____

You are permitted to work in groups, get help from others, read books, and use the internet. But the handwriting on this document must be your own. Print out the document, staple, and fill in the answers. You may attach extra sheets. Turn in the pages to the graduate assistant at the beginning of class, September 4.

I made an important mistake in my lecture when I told you that the secret key should be chosen so that de **mod** $N = 1$ **That is incorrect.**

The correction is: if $N = pq$ **where** p **and** q **are primes, then the public key** e **must be relatively prime to** $(p-1)(q-1)$**, and the private key** d **must be chosen so that** de **mod** $(p-1)(q-1) = 1$

Here are some additional helpful facts.

- If N is prime and $gcd(N, a) = 1$, *i.e.* a is relatively prime to N, then a^{N-1} **mod** $N = 1$.
- If $N = pq$, where p and q are large primes, and if a is relatively prime to N, then $a^{(p-1)(q-1)}$ **mod** $N = 1$.

1. Work problems 1.11 and 1.14 on page 39 of the textbook.

2. Let $(91, 5)$ be the public key for an RSA encryption system. Note that $91 = 7 \cdot 13$. My program computes $5 \cdot i \ \mathbf{mod}\ 72$ for all i from 1 to 72, and I found $d = 29$ for the secret key. I then tested my program by entering a message (a number between 1 and 90). Here is part of my program:

```
int expo(int base, int exponent, int modulus)
   {
    assert(exponent >= 0);
    assert(modulus > 1);
    int leftside = base % modulus;
    int rightside = exponent;
    int rslt = 1;
    while(rightside > 0)
     {
      if(rightside%2) rslt = rslt*leftside % modulus;
      leftside = leftside*leftside % modulus;
      rightside = rightside/2;
     }
    return rslt;
   }
```

And here is part of my output.

```
The private key is 29
Enter a message
38
 Your message is: 38
 The encryption is 38^5 mod 91 = 12
 The decryption is 12^29 mod 91 = 38
```

Work problem 1.27 on page 40 of your textbook.

3. Work problem 1.33 on page 41 of your textbook.