<u>Solutions to Assignment 10</u>

<u>Barr 4.1: 16*, 17</u>

16*. A Sophie Germain prime is a prime number p such that 2p + 1 is also prime. So, the first ten Sophie Germain primes are: 2, 3, 5, 11, 23, 29, 41, 53, 83, 89.

17. A Mersenne prime is a prime number of the form $2^n – 1$.

(a) The first four Mersenne primes are:

$3 = 2^2 – 1$,

$7 = 2^3 – 1$,

$31 = 2^5 – 1$, and

$127 = 2^7 – 1$.

(b) and (c) If n = r•s, where r and s are greater than 1, then

$2^n - 1 = 2^{rs} - 1 = (2^r)^s - 1 = (2^r - 1) \cdot ((2^r)^{s-1} + (2^r)^{s-2} + ... + 1)$, which is a factorization of $2^n – 1$ into nontrivial factors.

Verify that $(2^r)^s - 1 = (2^r - 1) \cdot ((2^r)^{s-1} + (2^r)^{s-2} + \ldots + 1)$ by multiplying out the terms.

Thus $2^n – 1$ cannot be prime whenever n is even/composite.

So, if a prime number is a Mersenne prime, it is of the form $2^p – 1$, where p is also a prime number.

<u>Barr 4.3: 1d*, 1e*, 6*.</u>

1. Use the repeated squaring method to calculate each of the following.

   (d) 4^{22} mod 11.

   $4^2 = 16 \equiv 5 \bmod 11$,

   $4^4 = (4^2)^2 = (5)^2 = 25 \equiv 3 \bmod 11$,

   $4^8 = (4^4)^2 = (3)^2 = 9 \equiv 9 \bmod 11$,

   $4^{16} = (4^8)^2 = (9)^2 = 81 \equiv 4 \bmod 11$, and

   $4^6 = 4^4 \bullet 4^2 = 3 \bullet 5 = 15 \equiv 4 \bmod 11$.

   Thus, $4^{22} = 4^{16} \bullet 4^6 = 4 \bullet 4 = 16 \equiv 5 \bmod 11$.

   (e) 3^{65} mod 71

   Proceeding analogously as above, we obtain:

   $3^2 = 9 \equiv 9 \bmod 71$

   $3^4 = (3^2)^2 = (9)^2 = 81 \equiv 10 \bmod 71$,

   $3^8 = (3^4)^2 = (10)^2 = 100 \equiv 29 \bmod 71$,

   $\vdots$

   and we find that $3^{65} \bmod 71 \equiv 45 \bmod 71$.

6.* Using exercise 5, prove the following analog to (4.28):

If gcd(a,n) = 1, then $a^e \equiv a^{e \bmod \phi(n)}$ (mod n).

By exercise 5, $a^{\phi(n)} \equiv 1$ mod (n). If $e = q\phi(n) + r$, where $0 \leq r < \phi(n)$, then

$a^e \bmod n = a^{q\phi(n) + r} \bmod n = (a^q)^{\phi(n)} \bullet a^r \bmod n \equiv 1 \bullet a^r \bmod n$.

Thus $a^e = a^r$ (mod n).

Note e mod $\phi(n) = r$ so, $a^e \equiv a^r = a^{e \bmod \varphi(n)}$.

Barr 4.4: 4, 6*, 8

4. Using a three-letter base twenty-six encoding and RSA,

(a) LIE is encoded as 22681,

(b) MAD is encoded as 14248, and

(c) SUN is encoded as 05589.

(see solutions to #6 for procedure)

6.* Encipher the message TAKE A HIKE using m – 22987 and exponent 7.

First split TAKE A HIKE into TAK EAH IKE.

T is the 20^{th} letter in the alphabet so its numerical equivalent in base 26 is 19.

A is the 1^{st} letter in the alphabet so its numerical equivalent in base 26 is 0.

K is the 11^{th} letter in the alphabet so its numerical equivalent in base 26 is 10.

So, following example 4.4.1 – with 3 letter blocks, we get

$x = x_2 \bullet 26^2 + x_1 \bullet 26^1 + x_0$. Enciphering TAK we have $x_2 = 19$, $x_1 = 0$, $x_0 = 10$.

So, $x = 19 \bullet 26^2 + 0 \bullet 26^1 + 10 = 12854$.

$y \equiv x^7 \bmod 22987 = (12854)^7 \bmod 22987 \equiv 6712 \bmod 22987$.

Similarly enciphering EAH we have $x_2 = 4$, $x_1 = 0$, $x_0 = 7$.

So $x = 4 \bullet 26^2 + 0 \bullet 26^1 + 7 = 2711$.

$y \equiv x^7 \bmod 22987 = (2711)^7 \bmod 22987 \equiv 5879 \bmod 22987$.

Enciphering IKE we get $x_2 = 8$, $x_1 = 10$, $x_0 = 4$

So, $x = 8 \bullet 26^2 + 10 \bullet 26^1 + 4 = 5672$

$y \equiv x^7 \bmod 22987 = (5672)^7 \bmod 22987 \equiv 2989 \bmod 22987$

Thus, the enciphered message is 06712 05879 02989.

8. m = 11,885,807, s = 6,395,437. We follow the procedure described in Example 4.4.3 (Page 290).

   Trying to factor m, we obtain $m = 1741 \bullet 6827$.

   Thus, p = 1741 and q = 6827. Thus, n = (p – 1)(q – 1) = 11,877,240.

   We then find the inverse d of s modulo 11,877,240. Using the extended Euclidean algorithm, we obtain d = 13.

   Now, the numerical equivalent of the plaintext is $(8648422)^{13}$ (mod 11,885,907).

   Finally, we find that the plaintext letters have numerical equivalents 2, 11, 4, 0 and 17. Thus, the message is CLEAR.