Homework 3

page 104

1. (a) Apply the Euclidean algorithm to 17 and 101:

$$101 = 5 \cdot 17 + 16$$

$$17 = 1 \cdot 16 + 1.$$

The Extended Euclidean algorithm, yields $1 = (-1) \cdot 101 + 6 \cdot 17$.

4. (a)

$$\begin{aligned} 30030 &= 116 \cdot 257 + 218 \\ 257 &= 1 \cdot 218 + 39 \\ 218 &= 5 \cdot 39 + 23 \\ 39 &= 1 \cdot 23 + 16 \\ 23 &= 1 \cdot 16 + 7 \\ 16 &= 2 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Therefore, $\gcd(30030, 257) = 1$.

(b) If 257 is composite, it is divisible by a prime $p \leq \sqrt{257} = 16.03\ldots$. The primes satisfying this are exactly the prime factors of 30030. Since the gcd is 1, none of them divide 257, so 257 is prime.

5. (a)

$$\begin{aligned} 4883 &= 1 \cdot 4369 + 514 \\ 4369 &= 8\dot{5}14 + 257 \\ 514 &= 2 \cdot 257 + 0. \end{aligned}$$

Therefore, the gcd is 257.

(b) We know that both numbers have 257 as a factor. This yields $4883 = 257 \cdot 19$ and $4369 = 257 \cdot 17$.

12. By Fermat's theorem, $2^{100} \equiv 1 \pmod{101}$. Therefore, $2^{10203} \equiv (2^{100})^{102} 2^3 \equiv 1^{102} 2^3 \equiv 8$. Therefore, the remainder is 8.

page 192:

1. We have $\phi(n) = (p-1)(q-1) = 100 * 112 = 11200$. A quick calculation shows that $3 \equiv 7467^{-1} \pmod{11200}$. We have $5859^3 \equiv 1415 \pmod{11413}$, so the plaintext was $1415 = no$.

4. Here, we want a number d such that $(m^3)^d \pmod{101} = m^{3d} = m \pmod{101}$. By Fermat's Little Theorem, we need to find d such that $3d = 1 \pmod{100}$. Solving, we get $d = 67$ and thus decryption is accomplished by $c^{67} \pmod{101}$.
7. Nelson decrypts $2^e c$ to get $2^{ed} c^d \equiv 2c^d \equiv 2m \pmod{n}$, and therefore sends $2m$ to Eve. Eve divides by 2 mod n to obtain m.
10. $e = 1$ means that the ciphertext is the same as the plaintext, so there is no encryption. The exponent $e = 2$ does not satisfy $\gcd(e, (p-1)(q-1)) = 1$, so it is not allowed in RSA (no d will exist).
11. Since $n_1 \neq n_2$, and since they are not relatively prime, we have $\gcd(n_1, n_2)$ must be a nontrivial common factor of n_1 and n_2. Therefore, we can factor n_1 and n_2 and break the systems.
17. Make a list of $1^e, 2^e, \ldots, 26^e \pmod{n}$. For each block of ciphertext, look it up on the list and write down the corresponding letter. The message given is *hello*.
21. Note that $d = e$, so Alice sends $m^{e^2} \equiv m^{ed} \equiv m \equiv 12345$.
25. Since $ed \equiv 1 \pmod{270300}$ we have $ed = 1 + 270300k$ for some integer k. Then $c^d \pmod{1113121} \equiv m^{ed} \equiv (m^{270300})^k m = m \pmod{1113121}$.

I.

3832920	1	0
65537	0	1
31774	1	-58
1989	-2	117
1939	31	-1813
50	-33	1930
39	1285	-75153
11	-1318	77083
6	5239	-306402
5	-6557	383485
1	11796	-689887

This tells us that $1 = 3832920 \cdot (11796) + 65537 \cdot (-689887)$. Therefore, $(65537)^{-1} \equiv -689887 \equiv 3143033 \pmod{3832920}$, so $d = 3143033$.

page 197:
1. First, we convert the two text messages to numerical values by:

```
>> text2int1('one')

ans =
   151405
>> text2int1('two')

ans =
   202315

>> powermod(sym('151405'), sym('6551'), sym('712446816787'))

ans =
   273095689186
>> powermod(sym('202315'), sym('6551'), sym('712446816787'))

ans =
   709427776011
```

Therefore the message was “one” (as we already knew from Longfellow’s poem).