Chapter 6 Homework 1-5, 9, 10

1. The ciphertext 5859 was obtained from the RSA algorithm using $n = 11413$ and $e = 7467$. Using the factorization $11413 = 101 \cdot 113$, find the plaintext.

   Using this factorization, we know $\phi(11413) = 100 \cdot 112 = 11200$. We are looking for $d \ni de \equiv 1 \pmod{\phi(n)}$. That is, we need $d \ni 7467d \equiv \pmod{11200}$. Notice

$$3(7467) = 22401 \equiv 1 \pmod{11200}$$

   So, $d = 3$.
   To decrypt, we use $m \equiv c^d \pmod{n}$. Here,

$$m \equiv 5859^3 \pmod{11413}$$

   Solving this gives $m = 1415$.

2. Suppose your RSA modulus is $n = 55 = 5 \times 11$ and your encryption exponent is $e = 3$.

   (a) Find the decryption modulus d.
   $\phi(55) = 40$, so we need $3d \equiv 1 \pmod{40}$. This gives that $d = 27$.

   (b) Assume that $gcd(m, 55) = 1$. Show that if $c \equiv m^3 \pmod{55}$ is the ciphertext, then the plaintext is $m \equiv c^d \pmod{55}$.
   From (a), $d = 27$. So, we are looking to show $m \equiv c^{20} \pmod{55}$.

$$\begin{aligned} c &\equiv m^3 \pmod{55} \\ \Rightarrow c^{27} &\equiv (m^3)^{27} \pmod{55} \\ &\equiv (m^{40})^2 m \pmod{55} \\ &\equiv m \pmod{55} \end{aligned}$$

   Since $m^{40} \equiv 1 \pmod{55}$ by Fermat's Little Theorem since $(m, 55) = 1$.

3. The ciphertext 75 was obtained using RSA with $n = 437$ and $e = 3$. You know the plaintext is either 8 or 9. Determine which it is without factoring n.

   $c \equiv m^e \pmod{n}$. So, we have two options.

$$75 \equiv 8^3 \pmod{437} \qquad\qquad 75 \equiv 9^3 \pmod{437}$$
$$8^3 = 512 \equiv 75 \pmod{437} \qquad\qquad 9^3 = 729 \equiv 292 \pmod{437}$$

   So, $m = 8$.

4. Suppose you encrypt messages m by computing $c \equiv m^3 \pmod{101}$. How do you decrypt?

   We want to find $de \equiv 1 \pmod{\phi(n)}$ so that we can decrypt using $c^d \equiv m \pmod{n}$.
   $\phi(n) = 100$ since $n = 101$ is prime.
   So, we want $3d \equiv 1 \pmod{100}$. Notice that $67(3) = 201 \equiv 1 \pmod{100}$, so $c^{67} \equiv m \pmod{101}$ can be used to decrypt.

5. Let p be a large prime. Suppose you encrypt a message x by computing $y \equiv x^e \pmod{p}$ for some (suitably chosen) encryption exponent e. How do you find the decryption exponent d such that $y^d \equiv x \pmod{p}$?

   Choose d with $de \equiv 1 \pmod{(p-1)}$. Then, we have

$$y^d \equiv x^{de} \equiv x^1 \equiv x \pmod{p}$$

   since we work modulo $p-1$ in the exponent.

9. Let p and q be distinct odd primes, and let $n = pq$. Suppose that the integer x satisfies $gcd(x, pq) = 1$.

   (a) Show that $x^{\frac{1}{2}\phi(n)} \equiv 1 \pmod{p}$ and $x^{\frac{1}{2}\phi(n)} \equiv 1 \pmod{q}$.

$$x^{\frac{1}{2}\phi(n)} = x^{\frac{1}{2}(p-1)(q-1)}$$

   Notice that since p and q are odd, $(p-1)$ and $(q-1)$ are even. Now, we know by Fermat's Little Theorem, that $m^{q-1} \equiv 1 \pmod{q}$ and $m^{p-1} \equiv \pmod{p}$. Then,
   $x^{\frac{1}{2}(p-1)(q-1)} = x^{k(q-1)}$ for some $k \in \mathbb{Z}$
   So,
   $x^{\frac{1}{2}(p-1)(q-1)} = (x^k)^{(q-1)} \equiv 1 \pmod{q}$
   and $x^{\frac{1}{2}(p-1)(q-1)} = x^{n(p-1)}$ for some $n \in \mathbb{Z}$
   which gives
   $x^{\frac{1}{2}(p-1)(q-1)} = (x^n)^{(p-1)} \equiv 1 \pmod{p}$

   (b) Use (a) to show that $x^{\frac{1}{2}\phi(n)} \equiv 1 \pmod{n}$.
   $x^{\frac{1}{2}\phi(n)} \equiv 1 \pmod{p} \Rightarrow$ for $s \in \mathbb{Z}$, $x^{\frac{1}{2}\phi(n)} = sp + 1 \Rightarrow x^{\frac{1}{2}\phi(n)} - 1 = sp$. Similarly, for $t \in \mathbb{Z}$, $x^{\frac{1}{2}\phi(n)} - 1 = tq$. So, we have

$$sp = tq \Rightarrow s = \frac{tq}{p}$$

   where $p|t$ because q is prime. That is, $kp = t$ for some $k \in \mathbb{Z}$. Then,

$$x^{\frac{1}{2}\phi(n)} = tq + 1 = kpq + 1 = kn + 1 \Rightarrow x^{\frac{1}{2}\phi(n)} \equiv 1 \pmod{n}$$

   (c) Use (b) to show that if $ed \equiv 1 \pmod{\frac{1}{2}\phi(n)}$ then $x^{ed} \equiv x \pmod{n}$.
   $ed \equiv 1 \pmod{\frac{1}{2}\phi(n)} \Rightarrow ed = k\left(\frac{1}{2}\phi(n)\right) + 1$ for some $k \in \mathbb{Z}$
   $x^{ed} \equiv x^{k\left(\frac{1}{2}\phi(n)\right)+1} \pmod{n}$
   $\equiv x^{k\left(\frac{1}{2}\phi(n)\right)} \cdot x \pmod{n}$
   $\equiv x \pmod{n}$
   because $x^{\frac{1}{2}\phi(n)} \equiv 1 \pmod{n}$.

10. The exponent $e = 1$ and $e = 2$ could not be used in RSA. Why?

    For $e = 1$, we would have $m^1 \equiv m \pmod{n}$, which does not change the plaintext.

    For $e = 2$, we want to find $d \ni 2d \equiv 1 \pmod{\phi(n)}$ since $\phi(n) = (p-1)(q-1)$ and $(2, \phi(n) = 2 \neq 1)$. So, no d can exist that makes an even number congruent to 1 modulo an even number.