21. More on RSA

We began with the homework problem. Ryan presented the solution.

**Problem:** Suppose $\epsilon(x) = x^{4007}\%6319$ is the encryption function. Find the decryption function $\delta(x)$.

**Solution:** (Ryan) For starters, Ryan used his calculator program to factor $N$ into primes: $6319 = 71 \cdot 89$. Therefore, $k = (71 - 1)(89 - 1) = 6160$. Now, the decryption exponent $d$ is just the inverse of 4007 modulo 6160. One can use the Euclidean Algorithm to find this inverse:

\[
\begin{align*}
6160 &= 1(4007) + 2153 \\
4007 &= 1(2153) + 1854 \\
2153 &= 1854(1) + 299 \\
1854 &= 6(299) + 60 \\
299 &= 4(60) + 59 \\
60 &= 1(59) + 1
\end{align*}
\]

Using back substitution, Ryan found that $1 = 103(4007) - 67(6160)$. (We’ve done this many times before, so I did not write out the work this time.) Hence, $103 \cdot 4007 \equiv 1 \pmod{6160}$, so $103 \equiv 4007^{-1} \pmod{6160}$. Therefore, $d = 103$ is the decryption exponent. So $\delta(x) = x^{103}\%6319$.

From the above example we see that one can find the decryption exponent fairly quickly once we’ve found the prime factorization of $N$. Even for very large values of $N$ (several hundred digits long), a computer can efficiently implement the Euclidean algorithm to find the inverse of an element once the prime factors of $N$ have been identified. The security of this cryptosystem lies in the fact that there is no known efficient method for finding the prime factorization of $N$ if $N$ is a very large integer (at least 300 digits long). Thus, even if Eve knows the value of $N$ and $e$, he cannot find the decryption exponent (as Ryan did above) until he first finds the prime factorization of $N$. This could take hundreds or thousands of years using the fastest computers if $N$ is large! On the other hand, it is fairly effortless for a computer to find large primes and multiply them together. So Alice can easily “cook up” a large $N$ to use as her public key so that only she will know the prime factorization. Hence, Alice will be the only one who can decrypt messages using her keys, even though everyone knows how to encrypt using her keys! This is the beauty (and utility) of public key cryptography.

We then gave a proof of why RSA works. Recall that set-up for this cryptosystem: Let $p$ and $q$ be distinct primes, $N = pq$, $k = (p - 1)(q - 1)$, $e$ any positive integer relatively prime to $k$, and $d = e^{-1}\%k$. Then $\epsilon(x) = x^e\%N$ is the encryption function and $\delta(x) = x^d\%N$ is the decryption function. We need to prove that for all $x$, $\delta(\epsilon(x)) = x$; that is, $x^d\%N = x$. Thus, we need to prove that $x^{ed} \equiv x \pmod{N}$.

**Theorem:** Let $p, q, N, k, e, d$ be chosen as above. Then $x^{ed} \equiv x \pmod{N}$ for all integers $x$.

**Proof:** (Erica, Megan, Gabe) First, since $N = pq$ and $p$ and $q$ are distinct primes, Megan pointed out that by a previous homework problem it suffices to prove that $x^{ed} \equiv x \pmod{p}$
and \( x^{ed} \equiv x \pmod{q} \). We focus on showing \( x^{ed} \equiv x \pmod{p} \). The proof for \( q \) is exactly the same. If \( p \mid x \) then certainly (as Gabe mentioned) \( p \mid x^{ed} \), and therefore both \( x \) and \( x^{ed} \) are congruent to zero modulo \( p \). So let’s assume for the remainder of this proof that \( p \) does not divide \( x \). This is where Erica took over: As \( d \equiv e^{-1} \pmod{k} \), we know that \( ed \equiv 1 \pmod{k} \). Therefore \( ed = k\ell + 1 \) for some integer \( \ell \). Since \( k = (p-1)(q-1) \), we have \( ed = (p-1)(q-1)\ell + 1 \). Now, recall that Fermat’s Theorem says that if \( p \) does not divide \( x \) then \( x^{p-1} \equiv 1 \pmod{p} \). Then we get

\[
x^{ed} = x^{(p-1)(q-1)\ell + 1} = x \cdot (x^{p-1})^{(q-1)\ell} = x \cdot (1)^{(q-1)\ell} = x
\]

Hence, we see that \( x^{ed} \equiv x \pmod{p} \). \( \square \)

We next moved on to a new topic.

**Definition:** Let \( m \geq 2 \) be an integer. We define \( \phi(m) \) to be the number of integers \( a \) in the range \( 1 \leq a \leq m \) such that \( \gcd(a, m) = 1 \). The function \( \phi \) is called the *Euler \( \phi \)-function*.

**Problem:** For \( m = 1, 2, \ldots, 16 \), find all values of \( a \) between 1 and \( m \) such that \( \gcd(a, m) = 1 \). Use this to compute \( \phi(m) \). What patterns or conjectures can you make about the \( \phi \)-function?

Everyone helped to fill in the following table:

<table>
<thead>
<tr>
<th>( m )</th>
<th>list of all ( a ) with ( 1 \leq a \leq m ) such that ( \gcd(a, m) = 1 )</th>
<th>( \phi(m) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1,2</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>1,3</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>1,2,3,4</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>1,5</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>1,2,3,4,5,6</td>
<td>6</td>
</tr>
<tr>
<td>8</td>
<td>1,3,5,7</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>1,2,4,5,7,8</td>
<td>6</td>
</tr>
<tr>
<td>10</td>
<td>1,3,7,9</td>
<td>4</td>
</tr>
<tr>
<td>11</td>
<td>1,2,3,4,5,6,7,8,9,10</td>
<td>10</td>
</tr>
<tr>
<td>12</td>
<td>1,5,7,11</td>
<td>4</td>
</tr>
<tr>
<td>13</td>
<td>1,2,3,4,5,6,7,8,9,10,11,12</td>
<td>12</td>
</tr>
<tr>
<td>14</td>
<td>1,3,5,9,11,13</td>
<td>6</td>
</tr>
<tr>
<td>15</td>
<td>1,2,4,7,8,11,13,14</td>
<td>8</td>
</tr>
<tr>
<td>16</td>
<td>1,3,5,7,9,11,13,15</td>
<td>8</td>
</tr>
</tbody>
</table>

Lisa provided us with the first observation:

**Theorem:** Let \( p \) be a prime. Then \( \phi(p) = p - 1 \).

**Proof:** (Lisa) All the numbers from 1 to \( p - 1 \) are relatively prime to \( p \). \( \square \)
Rachel also noticed a pattern when $m$ is a power of 2:

**Theorem:** For $\ell \geq 1$ we have $\phi(2^\ell) = \frac{1}{2}(2^\ell) = 2^{\ell-1}$.

**Proof:** (Rachel) The numbers which are relatively prime to $2^\ell$ are precisely all odd numbers. So $\phi(2^\ell)$ is the number of odd integers between 1 and $2^\ell$. Since half of the numbers in this interval are odd and half are even, we get $\phi(2^\ell) = \frac{1}{2}(2^\ell) = 2^{\ell-1}$. \[\square\]

Next, Megan conjectured the value of $\phi(3^\ell)$ for $\ell \geq 1$.

**Theorem:** For $\ell \geq 1$, $\phi(3^\ell) = 3^\ell - 3^{\ell-1}$.

**Proof:** (Megan) Consider the set of integers from 1 up to $3^\ell$. An integer is relatively prime to $3^\ell$ if and only if it is not a multiple of 3. But every third integer is a multiple of 3. Thus, one-third of the integers from 1 to $3^\ell$ are multiples of 3, leaving two-thirds which are not multiples of 3. Thus, 

$$\phi(3^\ell) = \frac{2}{3}(3^\ell) = (2)(3^{\ell-1}) = (3 - 1)(3^\ell - 1) = 3^\ell - 3^{\ell-1}.$$

**Example:** $\phi(3^5) = 3^5 - 3^4 = 3^4(3 - 1) = 81(2) = 162$. Thus, there are 162 integers between 0 and 242 which are relatively prime to 3.

Actually, as both Gabe and Megan pointed out, it’s easy to see that this proof generalizes to any prime $p$:

**Theorem:** Let $p$ be a positive prime and $\ell \geq 1$. Then 

$$\phi(p^\ell) = p^\ell - p^{\ell-1} = (p - 1)p^{\ell-1}.$$

**Proof:** (Gabe, Megan) We follow the same logic as with the case $p = 3$. We start with the set of integers from 1 up to $p^\ell$. A number in this list is relatively prime to $p^\ell$ if and only if it is not a multiple of $p$. Exactly one out of every $p$ of these numbers is a multiple of $p$, leaving $\frac{(p-1)}{p}(p^\ell) = (p - 1)(p^{\ell-1})$ of the numbers relatively prime to $p$. \[\square\]

Here is your homework for Thursday:

**Homework:** Let $p$ and $q$ be distinct primes. Conjecture a formula for $\phi(pq)$. Then prove your formula is correct.