The RSA Cryptosystem

The Theoretical Basis for RSA Encryption

The RSA algorithm involves 5 numbers: p, q, E, D, and M. As a brief introduction, they are:

- two different prime numbers, p and q
- two numbers in $\mathbb{Z}_{(p-1)(q-1)}$:
  - the "encoding number", E, which is relatively prime to $(p-1)(q-1)$
  - the "decoding number", D, which is the multiplicative inverse of E in $\mathbb{Z}_{(p-1)(q-1)}$
- a number in $\mathbb{Z}_p q$ known as the "message number", M

1. Do the activity Modular Inverses
   E must be relatively prime to $(p-1)(q-1)$ in order to have a multiplicative inverse in the system.

2. Let $p = 3$ and $q = 5$. Then $(p-1)(q-1) = 8$ and $pq = 15$. Suppose that we choose E to be 3. (We could choose any number that didn't have a factor of 2 since 2 is the only factor in 8). Find D.
   D is the multiplicative inverse of E in $\mathbb{Z}_8$. Thus, $D = 3$.

3. Sticking with the same p, q, and E (and therefore the same D), complete the table below using the rules of $\mathbb{Z}_{15}$. What do you notice about the entries of the last row?

$M \mod pq$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$M^E \mod pq$	1	8	12	4	5	6	13	2	9	10	11	3	7	14
$M^{ED} \mod pq$	1	2	3	4	5	6	7	8	9	10	11	12	13	14

   The last row is the same as the first row.

4. Google Sheets RSA Cryptosystem Crux Theorem Activity
   From the activity, it seems that raising a number to a power, then raising that to the multiplicative inverse of the previous power, produces the original number.

Theorem 5.1 (RSA Cryptosystem Crux): Suppose that p and q are two distinct prime numbers. Let E be relatively prime to $(p-1)(q-1)$. Then if D is the multiplicative inverse of E in $\mathbb{Z}_{(p-1)(q-1)}$ and if M is any number in $\mathbb{Z}_{pq}$, it will always be that $M^{ED} \equiv M \mod pq$.
Theorem 5.2: If p and q are distinct prime numbers and M is a positive integer with $\gcd(M, pq) = 1$, then $M^{(p-1)(q-1)} \equiv 1 \mod pq$.
Theorem 5.3: Let p and q be distinct prime numbers, k be a positive integer, and M be a number in $\mathbb{Z}_{pq}$ with $\gcd(M, pq) = 1$. Then $M^{1+k(p-1)(q-1)} \equiv M \mod pq$.
Theorem 5.4: Let p and q be distinct primes and E be a number in $\mathbb{Z}_{(p-1)(q-1)}$ such that E is relatively prime to $(p-1)(q-1)$. Then E has a multiplicative inverse in $\mathbb{Z}_{(p-1)(q-1)}$. That is, there exists some D in $\mathbb{Z}_{(p-1)(q-1)}$ such that $D \equiv E^{-1} \mod (p-1)(q-1)$.

5. Find the primes p and q if $pq = 14,647$ and $\phi(pq) = 14,400$. p and q must be distinct, since pq is not a square. Thus, $\phi(pq) = (p-1)(q-1) = pq - p - q + 1 = 14,400$. Thus, we can make a system of equations to solve for p and q:
   $$\begin{cases} pq &= 14,647 \\ pq - p - q + 1 &= 14,400 \end{cases}$$
   Thus, $p + q - 1 = 247$, so $p + q = 248$, so $p = 248 - q$. We can plug this back into the first equation, so $(248 - q)q = 14,647 \rightarrow 248q - q^2 = 14,647 \rightarrow 0 = q^2 - 248q + 14,647$. I put this into the quadratic equation to get $q = 97$ or 151. p and q are interchangeable in this equation, so either $p = 151, q = 97$, or $p = 97, q = 151$.

6. Prove Theorem 5.2 based on what you have already learned (perhaps in a previous section).
   Let p and q be distinct prime numbers, and let M be a positive integer with $\gcd(M, pq) = 1$. According to Euler's Theorem, if m is a positive integer and a is a positive integer with $\gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \mod m$. By setting $a = M$ and $m = pq$, we get $M^{\phi(pq)} \equiv 1 \mod pq$. In the previous section, we also determined that where p and q are distinct primes, $\phi(pq) = (p-1)(q-1)$. Thus, $M^{(p-1)(q-1)} \equiv 1 \mod pq$.

7. Prove Theorem 5.3 based on what you have already learned.
   Let p and q be distinct prime numbers, k be a positive integer, and M be a number in $\mathbb{Z}_{pq}$ with $\gcd(M, pq) = 1$. $M^{1+k(p-1)(q-1)} = M \times M^{k(p-1)(q-1)} = M \times (M^{(p-1)(q-1)})^k \mod pq$. By theorem 5.2, $M^{(p-1)(q-1)} \equiv 1 \mod pq$, so $M \times (M^{(p-1)(q-1)})^k \equiv M \times 1^k \equiv M \mod pq$. Thus, $M^{1+k(p-1)(q-1)} \equiv M \mod pq$.

8. Prove Theorem 5.1 (RSA Cryptosystem Crux) based on what you have already learned.
   Let p and q be two distinct prime numbers, and let E be relatively prime to $(p-1)(q-1)$. By theorem 5.4, there exists a number D that is the multiplicative inverse of E modulo $(p-1)(q-1)$. This means $ED \equiv 1 \mod (p-1)(q-1)$, or $ED = k(p-1)(q-1)+1$ for some integer k. Thus, $M^{ED} = M^{k(p-1)(q-1)+1} \equiv M \mod pq$ by theorem 5.3. Thus, $M^{ED} \equiv M \mod pq$.