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 $\mathbb{Z}_pq$ 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, $M^{ED} \equiv M \mod pq$.

The RSA Encryption Algorithm

Suppose Alice wants to send Bob a secret message.
Bob picks two prime numbers, p and q. Bob also picks an encoding number, E, from $Z_{(p-1)(q-1)}$ that is relatively prime to $(p-1)(q-1)$. Bob then makes pq and E public.
Alice converts her number to a message M (M must be less than pq, but this can be achieved by breaking the message into segments). To encode this message, she calculates $M^E \mod pq$.

For these problems, suppose Bob picks $p = 3, q = 97$. Thus, $pq = 291$ and $(p-1)(q-1) = 192$. He also chooses $E = 5$.

1. Suppose Alice's message is the number $M = 2$. What number does she send Bob? Describe in your own words how you found this number.
   First, I calculated M^E. $2^5 = 32$. $32 \mod 291 = 32$, so she will send Bob 32.

2. Suppose that Alice's secret message is the number M = 150. What number does she send Bob?
   Again, Alice will send Bob $M^E \mod pq$, so $150^5 \mod 291$. By modular multiplication rules, $150^5 \mod 291 = (150^2)^2 * 150 = 22500^2 * 150 = (291 * 77 + 93)^2 * 150 \equiv 93^2 * 150 = 8649 * 150 \equiv 210 * 150 = 31500 \equiv 72 \mod 291$. Alice sends 72 to Bob.

To decode the message, Bob must find D, the multiplicative inverse of E in $\mathbb{Z}_{(p-1)(q-1)}$. A computer can easily compute modular inverses with the Euclidean algorithm; in this case $D = 77$.

3. Bob can now decode Alice's message.

   (a) Verify that 77 is indeed the multiplicative inverse of 5 in $\mathbb{Z}_{192}$. Explain in your own words how you know that you are correct.
   To verify, I will find $77 * 5 \mod 192$. $77 * 5 = 385 = 192 * 2 + 1$, so $77 * 5 \equiv 1 \mod 192$, so $5^{-1} \mod 192$ is indeed 77.

   (b) Using the RSA Cryptosystem Crux Theorem, explain how Bob can use the number D to decode Alice's encoded message M^E and recover her original message M.
   By the Crux Theorem, $M^{ED} = M \mod pq$. The encoded message Bob receives from Alice is M^E. To find M and decode the message, Bob should calculate $(M^E)^D \mod pq$.

Why RSA Encryption is Useful

1. Suppose that you are listening in on Bob's public transmission and you hear that $pq = 21$ and $E = 5$. Recover $(p-1)(q-1)$ and D. You have broken Bob's code!
   $pq = 21$, where both p and q are prime. Either $p = 1, q = 21$ (which would be stupid), or $p = 3, q = 7$. Thus, $(p-1)(q-1) = 2 \times 6 = 12$. $D = E^{-1} \mod 12$, so $D = 5^{-1} \mod 12 = 5$. Thus, $(p-1)(q-1) = 12, D = 5$.

2. You are a secret agent. An evil spy with shallow number theory skills uses the RSA Public Key Coding System in which the public modulus is $n = 1537$, and the encoding exponent is $E = 47$. You intercept one of the encoded secret messages being sent to the evil spy, namely the number 570. Using your superior number theory skills, decode this message, thereby saving countless people from the fiendish plot of the evil spy.
   By brute-force testing increasing prime numbers, $p = 29, q = 53$. Thus, $(p-1)(q-1) = 28 \times 52 = 1456$. $D = 31$. $M = M^{ED} \mod pq = 570^D \mod pq = 570^{31} \mod 1537 = (570^3)^{10} \times 570 = (120490 \cdot 1537 - 130)^{10} \times 570 \equiv (-130)^{10} \times 570 = ((-130)^2)^5 \times 570 \equiv (-7)^5 \times 570 = -16807 \times 570 \equiv 100 \times 570 = 57000 \equiv 131 \mod 1537$.

These codes are easy to break because the chosen values of pq are relatively small. In practice, pqs are hundreds of digits long, making them effectively impossible to factor, even for a computer (though choosing numbers too large can make encoding and decoding difficult).
This is a public key encryption algorithm: Bob can make the encoding key, E, available to anyone, but only he has the decoding key D.

3. Summarize RSA encryption and the advantages it offers in your own words.
   In RSA encryption, a person publicly releases an encrypting key and a modulus. Anyone sending them a message uses those two things to encrypt the message, but only the original person has the decrypting key. This allows messages to be encrypted and decrypted without ever needing to transmit a decoding key, eliminating the possibility of interception.

4. Can you see any weaknesses in RSA? There are a couple and one has to make a few simple modifications to the messages being sent and the algorithm to avoid them. For the sake of simplicity, the method discussed here is the simplest version and in practice more sophisticated methods (based on the same idea) are used.
   When implemented correctly, RSA encryption has no weaknesses, barring quantum computers, because being able to efficiently factor large numbers allows for breaking the encryption.
   However, due to a couple of mathematical quirks, the following properties should be ensured:

   - p and q are both sufficiently large, to ensure a sufficiently large pq
   - $p-1$ and $q-1$ each have at least one prime factor that is sufficiently large
   - E and D are sufficiently large

   Other weaknesses of RSA come from its implementation, not the mathematical principles.