1. The number $m = 89\,336\,978\,293$ is the product of two primes. Suppose it is somehow discovered that $\varphi(m) = 89\,336\,174\,400$. Use this information to factor m.

Solution: Write $m = pq$. Then $\varphi(m) = (p-1)(q-1) = pq - (p+q) + 1$, so that

$$m - \varphi(m) + 1 = p + q.$$

Using a calculator, we determine that

$$p + q = 803\,894.$$

Next we recall that $(p+q)^2 - 4pq = (p-q)^2$. Since we know pq (it's m), and we know $p+q$, we can find $(p-q)^2$. The calculator says

$$(p-q)^2 = 288\,897\,650\,064.$$

Taking the square root, we find that $p - q = 537\,492$. Finally, we have

$$p = \frac{1}{2}((p+q) + (p-q)) = 670693$$
$$q = \frac{1}{2}((p+1) - (p-q)) = 133201.$$

2. Suppose the numbers $m = 61\,138\,711$ (a product of two primes) and $k = 4571$ are given as an encryption key. By means of a bit of virtual breaking and entering, a number theory student at MIT discovers that the corresponding $\overline{k}$ is equal to $1\,618\,003$. Use this information to factor m.

Solution: We know that $k\overline{k} = 7\,395\,891\,713$ is congruent to 1 modulo $\varphi(m)$, so any integer raised to the power $k\overline{k} - 1$ will be congruent to 1 modulo m.

We search for a witness to m's compositeness. We find that

$$\begin{aligned} 2^{\frac{k\overline{k}}{2}} &\equiv 1 \pmod{m} \\ 2^{\frac{k\overline{k}}{4}} &\equiv 1 \pmod{m} \\ 2^{\frac{k\overline{k}}{8}} &\equiv 19\,334\,531 \pmod{m} \end{aligned}$$

From the last result, we know that $x = 19\,334\,531$ satisfies $x^2 - 1 \equiv 0 \pmod{m}$, but $x \not\equiv \pm 1 \pmod{m}$. Thus one of the prime factors of m must divide $19\,334\,530$ and the other must divide $19\,334\,532$. Using the Euclidean algorithm, we find that

$$\begin{aligned}(19\,334\,530, m) &= 7\,703\\ (19\,334\,532, m) &= 7\,937.\end{aligned}$$

These are the prime factors of m.

3. Suppose $m = p_1p_2p_3$ is a product of three (distinct) primes, and suppose we know a pair of integers k and $\overline{k}$ such that $k\overline{k} \equiv 1 \pmod{\varphi(m)}$. How can we use this information to factor m?

Solution: As with products of two primes, we look for witnesses to the compositeness of m. That is, we try to find a number x such that $x^2 \equiv 1 \pmod{m}$ but $x \not\equiv \pm 1 \pmod{m}$. Having found such a number x, we know that

$$m | (x-1)(x+1)$$

but $m \not| (x-1)$ and $m \not| (x+1)$. The only way this can occur is if one of the prime factors of m divides one of the factors $(x-1)$, $(x+1)$, and the other two factors of m divide the other.

We compute $((x-1), m)$ and $((x+1), m)$. One of these will be prime; the other will be a product of two primes. We have thus reduced this to a simpler problem, which we have already solved.

4. (a) M the spymaster needs to collect status reports from two of her field agents, R and S (code names for Roger and Sean). She finds a number m that is the product of two primes, and finds two numbers k_1 and k_2, that are relatively prime to $\varphi(m)$ and relatively prime to each other.

She sends the encryption key (m, k_1) to agent R and the encryption key (m, k_2) to agent S. The two agents encrypt and send back to M the same message ("`ALL IS WELL PLEASE SEND MORE VERMOUTH`").

Members of SPECTRUM intercept the whole transaction. They suspect that the replies sent by R and S are two different encryptions of the same message. By assuming this is true, they are able to decrypt the reply.

How do they do it?

Solution: Suppose the message is a. Then SPECTRUM has access to m, k_1, k_2, a^{k_1} and a^{k_2}.

Since k_1 and k_2 are relatively prime, there exist integers x and y such that

$$k_1 x + k_2 y = 1.$$

We need only compute

$$(a^{k_1})^x \times (a^{k_2})^y \equiv a^{k_1 x + k_2 y} \equiv a^1 \pmod{m}.$$

The only snag here is that either x or y will be a negative integer, so we need to figure out how to raise either a^{k_1} or a^{k_2} to a negative power. But this is easy; by the Euclidean algorithm, we know how to find multiplicative inverses (modulo m), and a^{-t} is just $\overline{a}^t$.

(b) Your friends in SPECTRUM hire you as a consultant to discover the numerical value of the message that R and S are sending to M. They have the following data:

$$\begin{aligned} m &= 6\,070\,619 \\ k_1 &= 541 \\ k_2 &= 491. \end{aligned}$$

The encrypted message returned by R (using k_1) is 2 637 195. The encrypted message returned by S (using k_2) is 3 177 151.

What is the number that both R and S have encrypted?

Solution: Let a denote the unknown message, b_1 denote R's encryption of a and b_2 denote S's encryption of a. We use the Euclidean algorithm to find that

$$119 \times k_2 - 108 \times k_1 = 1.$$

We need to find x satisfying

$$x \equiv b_1^{119} \times b_2^{-108} \pmod{6\,070\,619}.$$

To compute this, we'll need the multiplicative inverse of b_2 modulo 6070619. Using the Euclidean algorithm again, we find that

$$\overline{b_1} \equiv -1\,111\,999 \equiv 4\,958\,620 \pmod{6\,070\,619}.$$

Using a calculator and the PowerMod routine on the website, we find that

$$b_1^{119} \times \overline{b_2}^{108} \equiv 246 \pmod{6\,070\,619}.$$

The original message was 246.

5. (a) Spymaster M now needs to collect status reports from agents R, S, and T (Timothy, of course). This time, she finds three different moduli, m_1, m_2, and m_3, each a product of two primes. She sends the encryption key $(m_1, 3)$ to R, $(m_2, 3)$ to S, and $(m_2, 3)$ to T.

As before, agents R, S, and T encrypt and return identical messages.

Members of SPECTRUM use this unfortunate habit to break the code once again. How do they do it?

Solution: First of all, they check to see that all the m's are relatively prime in pairs. If not, then the GCD of any two of them (say m_1 and m_2) is a prime factor of both m_1 and m_2, so SPECTRUM can then factor either m_1 or m_2 to crack the code.

Here's how they proceed in the case where all the moduli are relatively prime in pairs. Let x be the secret message. Then SPECTRUM has numbers b_1, b_2, and b_3 such that

$$\begin{aligned} x^3 &\equiv b_1 \pmod{m_1} \\ x^3 &\equiv b_2 \pmod{m_2} \\ x^3 &\equiv b_3 \pmod{m_3}. \end{aligned}$$

Furthermore, since x is in the interval $0 \le x < \min\{m_1, m_2, m_3\}$, we know that x^3 satisfies $0 \le x^3 < m_1 m_2 m_3$.

By the Chinese Remainder Theorem, there is a unique integer y in the interval $0 \le y < m_1 m_2 m_3$ satisfying

$$\begin{aligned} y &\equiv b_1 \pmod{m_1} \\ y &\equiv b_2 \pmod{m_2} \\ y &\equiv b_3 \pmod{m_3}. \end{aligned}$$

If we find such a y, it must be equal to x^3. In fact, it's not difficult to determine a solution to a CRT problem, so this is probably what the SPECTRUM people do: they find a solution y to the system above, and take its cube root to recover x.

(b) Here's some more consulting work. The good folks at SPECTRUM intercept the following data. For each i, b_i is the encoded reply sent back to M.

$$\begin{aligned} m_1 &= 206\,837; & b_1 &= 26\,458 \\ m_2 &= 205\,811; & b_2 &= 97\,814 \\ m_3 &= 244\,523; & b_3 &= 223\,073 \end{aligned}$$

In each case, the secret message is the same, and the value of k is 3. What was the secret message? (For this one, you'll need Mathematica, Maple, or a TI-89, because the numbers are too big for a hand calculator. Do it without factoring any of the m_i.)

Solution: We set up the Chinese Remainder Theorem problem

$$\begin{aligned} y &\equiv 26\,458 \pmod{206\,837} \\ y &\equiv 97\,814 \pmod{205\,811} \\ y &\equiv 223\,073 \pmod{244\,523} \end{aligned}$$

We find the multiplicative inverses $\overline{m_1}$ (modulo m_2m_3), $\overline{m_2}$ (modulo m_1m_3), and $\overline{m_3}$ (modulo m_1m_2) using the Euclidean algorithm. They are

$$\begin{aligned} \overline{m_1} &= 2\,368\,866\,757 \\ \overline{m_2} &= 20\,173\,451\,063 \\ \overline{m_3} &= 23\,585\,890\,907 \end{aligned}$$

We use the usual method for solving CRT problems to find a solution Y to the system above. We get

$$\begin{aligned} Y &= m_2\overline{m_2}m_3\overline{m_3}b_1 + m_1\overline{m_1}m_3\overline{m_3}b_2 + m_1\overline{m_1}m_2\overline{m_2}b_3 \\ &= 1\,363\,748\,093\,360\,796\,644\,969\,631\,310\,441\,506\,021. \end{aligned}$$

This is congruent modulo $m_1m_2m_3$ to 691 745 275 584. We take the cube root of this last number to find the secret message: 8844.

6. On an earlier problem set, we showed that in the unlikely event that the message a turns out not to be relatively prime to m, the RSA encryption and decryption process still works.

However, from a security standpoint, transmitting such a message (even encrypted) is very dangerous. Why?

Solution: Suppose $(a, m) > 1$. Then $(a, m) = p$ or $(a, m) = q$. That is, either p or q divides a. Since the encrypted form of a is simply a^k for some (positive) k, we know that either p or q divides a^k as well.

A spy intercepting a^k and m can quickly compute their GCD, which will be either p or q. In either case, the spy will be able to factor m, and thus discover the contents of this message and all future messages sent with the same m.

7. Describe a modified RSA system in which each of three people has a key. Each person can encrypt a message with his or her key, and the message can be read only if both of the other two keys are used.

Solution: Here's one way to do it: Let m be a product of two large primes, and let k_1, k_2, and k_3 be positive integers such that

$$k_1 k_2 k_3 \equiv 1 \pmod{\varphi(m)}.$$

Let the three agents be called A_1, A_2, and A_3. Give the key k_1 to agent A_1, the key k_2 to agent A_2, and the key k_3 to agent A_3.

Now suppose A_1 encrypts a message using the key k_1. That is, A_1 takes the secret message a and finds a number b such that

$$b \equiv a^{k_1} \pmod{m}.$$

Agent A_1 transmits the number b to A_2 and A_3. Can A_2 and A_3 decrypt the message? The obvious way to do it is for A_2 and A_3 to use their keys, k_2 and k_3, to form $b^{k_2 k_3}$, which will then be congruent to

$$a^{k_1 k_2 k_3} \equiv a \pmod{m}.$$

So by working together, A_2 and A_3 can decrypt A_1's message.

Could either A_2 or A_3 decrypt the message without help from the other? Decrypting the message is equivalent to finding $\overline{k_1}$ modulo $\varphi(m)$. But A_2 doesn't know either k_1 or $\varphi(m)$. Even if A_2 could factor m (and thus determine $\varphi(m)$), she would not have enough information to decrypt the message.

The same scheme can be used in another way: the agent receiving a (pre-arranged) message can verify that the message has been seen by both of the other two agents. Suppose agent A_1 wants to know that both A_2 and A_3 have seen the message a. She instructs A_2 to encode the message – that is, to find b such that

$$b \equiv a^{k_2} \pmod{m}$$

and send the result to A_3. Agent A_3 then finds c such that

$$c \equiv b^{k_3} \pmod{m}$$

and relays it to A_1. Agent A_1 decrypts c by finding

$$c^{k_1} \equiv b^{k_1 k_3} \equiv a^{k_1 k_2 k_3} \equiv a \pmod{m}.$$

Since the pre-arranged answer pops out, A_1 knows that the number c must have been congruent to $a^{k_2 k_3}$ modulo m. Could either of A_2 or A_3 formed this number without the help of the other? Again, that would require finding $\overline{k_1}$ modulo $\varphi(m)$, and since neither A_2 nor A_3 knows k_1 or $\varphi(m)$, neither agent could have successfully faked this "digital signature."