Math 319 Problem Set #8 Due 25 April 2002

Instructions: These problems have to do with public-key cryptography and with ways to defeat it. The numbers in the examples are unrealistically small, and are easy to factor using Maple, *Mathematica*, or even a TI-89. You should pretend that this factoring capability is not available – in real-world cryptography it wouldn't be – and try to do each problem with the smallest amount of computer power necessary. I suggest a hand calculator and the Euclidean Algorithm and PowerMod routines on the course website.

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.

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.

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?

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?

(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?

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?

(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.

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

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.)

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?

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.

Cultural aside:

"This is the fellow we've been waiting for," Chattan says to Robson. "The one we could have used in Algiers."

"Yes!" Robson says. "Welcome to Detachment 2701, Captain Waterhouse."

"2702," Waterhouse says.

Chattan and Robson look every so mildly startled.

"We can't use 2701 because it is the product of two primes."

"I beg your pardon?" Robson says.

One thing Waterhouse likes about these Brits is that when they don't know what the hell you are talking about, they are at least open to the possibility that it might be their fault. Robson has the look of a man who has come up through the ranks. A Yank of that type would already be scornful and blustery.

"Which ones?" Chattan says. That is encouraging; he at least knows what a prime number is.

"73 and 37," Waterhouse says.

This makes a profound impression on Chattan. "Ah, yes, I see." He shakes his head. "I shall have to give the Prof a good chaffing about this."

Robson has cocked his head far to one side so that it is almost resting upon the thick woolly beret chucked into his epaulet. He is squinting, and has an aghast look about him. His hypothetical Yank counterpart would probably demand, at this point, a complete explanation of prime number theory, and when it was finished, denounce it as horseshit.

Neal Stephenson, *Cryptonomicon*