Math 328K (Daniel Allcock)
Homework 13, due Friday April 28, 2017

Caution: at the bottom of p. 323 in the text there is an extremely confusing typo. The right side should be $C^d$ not $P^d$.

Problem 1. Encrypt the message “BESTWISHES” using RSA with modulus $n = 2669$ and encrypting exponent $e = 3$. (This is problem 5 from section 8.4 of the book, so you can check in the back to see you did it right. Of course you have to show your work. The book adds extra copies of the letter X at the end of the message to make the length of the message be a multiple of 4, and converts from letters to numbers using $A \rightarrow 00$, $B \rightarrow 01$, etc. See the examples in the book for more on this. This is the only time this course where you will have to do the conversion between letters and numbers.)

Problem 2. Suppose the RSA setup you are using takes the modulus to be some huge 100’s-of-digits number $n$, and that the encrypting exponent $e$ is some large number too. Their exact details don’t matter here.

Say the message is “WINTER IS COMING”. You and a friendly spy have secretly agreed beforehand on a correspondence between letters and numbers, $W \leftrightarrow P_W$, $I \leftrightarrow P_I$, etc. The numbers are integers in the range $2, \ldots, n - 1$. He encrypts the first number by applying RSA to the number $P_W$, and sends the result to you. Then he applies RSA to $P_I$, and sends the result to you, and so on. There is a pause between numbers so you can tell where each piece of the message ends and the next one begins.

Explain why this communication is insecure, no matter how well $n$ is chosen.

Problem 3. You intercept a message “2206 0755 0436 1165 1737”, which you know was encrypted using RSA with modulus $n = 2747$ and encrypting exponent $e = 13$. Crack the message. (This is number 7 in the same section of the text, again so you can check your work. But of course you still have to show your work. You do NOT need to bother converting it into letters or anything.)

Problem 4. Suppose another incompetent spy has a long list of numbers, say $2, \ldots, 1000000$, representing common words like “rendevous” or “subversive” and so forth. He uses a huge modulus $n$, say a 100-digit number, but a small encrypting exponent, say $e \leq 16$. Explain why someone listening to his communications can read his messages, without having to factor $n$.

Problem 5. Suppose that Bob, very concerned with security, selects an encrypting modulus $n = pq$ where $p$ and $q$ are large primes. Suppose he also chooses two encrypting exponents $e_1$ and $e_2$. He asks people sending him messages to “double encrypt” their messages as follows. For each plaintext (an element of $\mathbb{Z}_n$), he asks them to encrypt it using RSA with modulus $n$ and encrypting exponent $e_1$, and then encrypt the result of that using RSA with modulus $n$ and encrypting exponent $e_2$. He thinks he’s getting twice as much security this way. Explain why he is wrong.

Problem 6. This problem highlights what looks like an obscure attack on RSA. But this kind of attack is actually a big deal, because espionage is full of people cracking codes by clever tricks like this. For example, it is a common tactic to try tricking an opposing radio operator (or a more-modern equivalent) into encrypting some known plaintext, so the result of the encryption can be compared with the known original.
Now, on to the specific attack:

You are eavesdropping on Alice’s communications. You know she received a message sent to her using her public key: modulus $n$ and encrypting exponent $e$. So you know what the ciphertext $C$ is and you want to know the original plaintext $P$. You choose a number $r$ and send her the message “$Cr^e$”. Expecting that the incoming message has been encrypted with her public key, Alice decrypts it, but finds no intelligible message, so she carelessly discards the result. You dig through her trash and find the decrypted-but-seemingly-nonsense result. Then you laugh maniacally (cue sound effect) because now you can recover the original plaintext $P$. Explain, including discussing what properties you should choose $r$ to have.

*Problem 7.* Three military commanders want to set things up so that if any two of them send a message “attack” then their forces will attack, but no one commander has that power. And no one should be able to impersonate them, not even the people at the base who must be prepared to receive the message. Discuss how one might use public-key encryption for this.