Lecture 12

This week your challenge is to read a paper and understand it, namely, the paper on RSA codes. I'm going to leave most of it for you to decipher and ask questions if you need to, but I am going to write a bit about the square and multiply method. The basic idea is that to get successive powers of 2 one squares the previous power of 2. So let's assume that you have been given out a public key code of $n = 55$ and $e = 17$ and received the coded message 1305. Of course you wouldn't use such low numbers but I want to do an example whose arithmetic is easy to follow. Since you created the code, you know that your secret decode key is $d = 33 = 32 + 1$. So $33_{\text{base 10}} = 100001_{\text{base 2}}$. So $13^{33} \mod 55 = (13^{32})(13^1) \mod 55 = (13^8 \mod 55)(13^4 \mod 55)(13) \mod 55$. To do this most efficiently we make a chart. Let $d = e_k \cdots e_0$ and C be the code block or M for the message block. Each time we do the indicated operation, we go $\mod 55$. We initialize by starting with M=1 or C=1 depending on whether we have C or M, namely, it is what we are computing. In our case, since we have C, we want to compute M and set $M = 1$ to start. Note that it is easier sometimes to use negative numbers so as to simplify the arithmetic.

i	e_i	M	M^2	$M^2 \mod 55$	$C^{e_i}(M^2 \mod 55)$	$C^{e_i}(M^2 \mod 55) \mod 55 =$ new M
5	1	1	1	1	13	13
4	0	13	169	4	4	4
3	0	4	16	16	16	16
2	0	16	256	36	36	-19
1	0	-19	361	31	31	-24
0	1	-24	576	26	338	8

So the message starts with the eight letter of the alphabet, namely h. Similarly, with $C = 05$

i	e_i	M	M^2	$M^2 \mod 55$	$C^{e_i}(M^2 \mod 55)$	$C^{e_i}(M^2 \mod 55) \mod 55 =$ new M
5	1	1	1	1	5	5
4	0	5	25	25	25	25
3	0	25	625	20	20	20
2	0	20	400	15	15	15
1	0	15	225	5	5	5
0	1	5	25	25	125	15

So the second letter of the message is the fifteenth letter of the alphabet, namely, o. The message is HO, which means amen in a number of Native American languages.

Problem 2 is done using the frequency chart and guessing. Good luck.