

Lecture 12  
 Copyright © Sue Geller 2006

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  $d = 13 = 8 + 4 + 1$ . So  $13_{\text{base } 10} = 1101_{\text{base } 2}$ . So  $13^{13} \bmod 55 = (13^8)(13^4)(13^1) \bmod 55 = (13^8 \bmod 55)(13^4 \bmod 55)(13) \bmod 55 = (((13^2 \bmod 55)^2 \bmod 55)^2 \bmod 55)((13^2 \bmod 55)^2 \bmod 55)(13) \bmod 55$ . 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  $\bmod 55$ . 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.

$i$	$e_i$	$M$	$M^2$	$M^2 \bmod 55$	$C^{e_i}(M^2 \bmod 55)$	$C^{e_i}(M^2 \bmod 55) \bmod 55 = \text{new } M$
3	1	1	1	1	13	13
2	1	13	169	4	52	-3
1	0	-3	9	9	9	9
0	1	9	81	26	338	8

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

$i$	$e_i$	$M$	$M^2$	$M^2 \bmod 55$	$C^{e_i}(M^2 \bmod 55)$	$C^{e_i}(M^2 \bmod 55) \bmod 55 = \text{new } M$
3	1	1	1	1	5	5
2	1	5	25	25	125	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.