Institut for Matematik og Datalogi
Syddansk Universitet

March 5, 2003
JFB

Cryptology – F03 – Note 6

Lecture, March 4

We continued with chapter 5, covering up through Theorem 5.10.

Lecture, March 11

We will continue with chapter 5.

Lecture, March 18

We will begin on chapter 6.

Problems for Thursday, March 20

1. There is an iterated attack on RSA which proceeds as follows: Set f equal to the ciphertext c. Repeatedly encrypt f using the public key to get a new value for f ($f \leftarrow f^e \pmod N$) until $f = c$. The last value of f before it became the ciphertext is the original message.

   This attack is usually not efficient, but is occasionally. When it works relatively quickly, what are the likely explanations?

2. Do problem 5.9 in the textbook.

3. Do problem 5.15 in the textbook.

4. Do problem 5.16 in the textbook.

5. Do problem 5.17 in the textbook.

6. Suppose that RSA is implemented using the public keys, $N = 221$ and $e = 77$.

   a. While encrypting the plaintext 160, repeated squaring was used, and the following results were obtained:

$$\begin{array}{lll} 160^2 \mod 221 & = & 185 \\ 160^4 \mod 221 & = & 191 \\ 160^8 \mod 221 & = & 16 \\ 160^{16} \mod 221 & = & 35 \\ 160^{32} \mod 221 & = & 120 \\ 160^{64} \mod 221 & = & 35 \\ 160^{72} \mod 221 & = & 118 \\ 160^{76} \mod 221 & = & 217 \\ 160^{77} \mod 221 & = & 23 \end{array}$$

   The intermediate results which were obtained give a cryptanalyst some very useful information for factoring the modulus. What was so interesting? (Hint: Look at the results of the different squarings.) Show how to use this information to factor 221.

   b. What is the decryption exponent d?

7. Do problem 5.22 in the textbook. Skip part (b), but assume the result there for the later subquestions.

8. Calculate the Jacobi symbols $\left(\frac{16}{57}\right)$, $\left(\frac{20}{59}\right)$, and $\left(\frac{23}{59}\right)$.