Institut for Matematik og Datalogi
Syddansk Universitet

February 28, 2013
JFB

Cryptology – F13 – Week 5

Lecture, February 21

After discussing some problems, we continued with chapter 5, discussing quadratic residues and nonresidues.

Lecture, February 22

We continued with chapter 5, covering primality testing (the Miller-Rabin algorithm was covered in the problem session on February 25, and a polynomial time primality test will be presented on February 28).

Lecture, February 28

We finished primality testing (the first polytime primality test was presented) and the remainder of chapter 5.

Lecture, March 4

We will cover chapter 6 in the textbook.

Lecture, March 8

We will cover the McEliece Cryptosystem (copied from the earlier edition of the textbook and sent to you via e-mail). You can look at Regev's articles in STOC '05 and CRYPTO 06 for another system secure against quantum attacks, and at Peikert's papers on lattice-based systems: http://eprint.iacr.org. Then we will introduce digital signatures from chapter 7, and start on chapter 4, probably covering through section 4.2. A meet-in-the middle attack will be demonstrated.

Problem session March 7

1. Do problems 5.16 and 5.17 in the textbook.

2. Suppose $n = 11,820,859$ is an RSA modulus. Suppose you know $\phi(n) = 11,813,904$. Find the factors of n. Show your work. (You may use Maple to solve the quadratic equation, but explain how you used it.)

3. Find all square roots of 64 modulo 105.

4. Find a primitive element (generator) in the multiplicative group modulo 103 ($\mathbb{Z}^*_{103}$) and show that it is a primitive element.

5. Consider the following proposal for a primality test for an integer n: Check if $2^n - 2$ is divisible by n. Answer "prime" if it is and "composite" if it is not.

   a. Give an odd prime for which this test works correctly and an odd composite for which it also works correctly.

   b. Prove that the test answers "prime" for all primes.

   c. Show that it answers "prime" incorrectly for $n = 341$. Use Fermat's Little Theorem to compute $2^{341} \pmod{p}$ for each prime factor of 341. Then use the Chinese Remainder Theorem, to compute $2^{341} \pmod{341}$.

6. Suppose the Solovay-Strassen Primality Test is used to find the primes p and q for use in the RSA cryptosystem. (Assume that random integers of the required length are chosen and tested for primality until two are found where the test does not discover that they are composite.) Even assuming that the primality test is executed several times, there is still a small probability of choosing a number which is not prime. Suppose the p chosen is prime, but q is not.

   a. Suppose q is a Carmichael number. (Recall that a *Carmichael number* is a composite integer n such that for all $x \in Z^*_n$, $x^{n-1} \equiv 1 \pmod{n}$.) Would encryption and decryption still work properly? Prove your answer. (Hint: try using the Chinese Remainder Theorem.)

b. Suppose q is a not a Carmichael number. Would encryption and decryption still work properly? Prove your answer. (Hint: try using the Chinese Remainder Theorem.)

c. What other problem could exist if q is a composite number?

7. I may lecture at the end.

Assignment due Friday, March 22, 10:00

Note that this is part of your exam project, so it must be approved in order for you to take the exam in June, and you may not work with others not in your group. If it is late, it will not be accepted (though it could become the assignment you redo). You may work in groups of two (or three). Turn in the assignment through the SDU Assignment system in Blackboard, and remember to keep your receipt. Turn in one PDF file per group.

1. Suppose that two parties, Alice and Bob, possess integers p_A, q_A and p_B, q_B, and they have used a protocol to compute an $N = (p_A+p_B)(q_A+q_B)$, without revealing their own integers to the other party. Now they use the following protocol (repeated many times) to check that N is the product of two primes $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$.

   (a) Bob and Alice agree on a random $g \in Z_N^*$. (In practice, they could alternate who chooses g, but do not worry about that.)

   (b) Both players compute the Jacobi symbol $\left(\frac{g}{N}\right)$. If the result is not 1, they restart at step 1.

   (c) Alice computes $v_A = g^{(N-p_A-q_A+1)/4} \pmod N$, and Bob $v_B = g^{-(p_B+q_B)/4} \pmod N$. They exchange these values and check that $v_A v_B = \pm 1 \pmod N$. If this fails, then both parties output that N is not product of two primes of the correct form. Otherwise they output that N probably is the product of two primes of the correct form.

      i. Show that if $N = pq$, where p and q are both prime, $p \equiv q \equiv 3 \pmod 4$, $p = p_A + p_B$, and $q = q_A + q_B$, then both parties will accept. Hint: Consider the Legendre symbols of g mod p and g mod q.

ii. Suppose that $N = pq$, where p and q are both prime, $p \equiv 3 \pmod 4$, $q \equiv 1 \pmod 4$, $p = p_A + p_B$, and $q = q_A + q_B$. Consider a value g which is a quadratic nonresidue modulo both p and q. Will it pass this test? What does this say about the probability of Alice and Bob incorrectly outputting that N is the product of two primes of the correct form?

2. Consider the ElGamal Public-key Cryptosystem in Z_p^*.

   (a) Suppose that Bob encrypted several messages, $x_1, x_2, ..., x_n$, to send to Alice using Alice's public key, but used the same value k in every encryption. Thus, the encryptions are

   $$(\alpha^k, x_1\beta^k), (\alpha^k, x_2\beta^k), ..., (\alpha^k, x_n\beta^k),$$

   where all operations are performed modulo p. Suppose that x_5 was also sent to the eavesdropper, Eve. How can Eve determine the other x_i's?

   (b) Suppose that, instead of using the same value k, Bob used consecutive values of k. Thus, for some k the encryptions are

   $$(\alpha^k, x_1\beta^k), (\alpha^{k+1}, x_2\beta^{k+1}), ..., (\alpha^{k+n-1}, x_n\beta^{k+n-1}),$$

   where all operations are performed modulo p. How can Eve still determine the other x_i's if she is sent x_5?

3. 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:

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

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? Explain how you got that result.

4. Show all steps in the calculations of the Jacobi symbol $\left(\frac{34}{77}\right)$, using the standard algorithm (using the four properties of the Jacobi symbol given in the textbook).

5. Suppose that a cryptanalyst discovered that some groups of companies had the same public key for RSA and some groups of companies had RSA keys which had exactly one factor in common. Suppose that these companies had not planned for this to happen.

   (a) How could it have happened anyway?

   (b) Why is it a problem for these companies that it happened?

   (c) Suppose that their RSA keys have length 1024 bits. What is the (approximate) probability of two random RSA keys being the same?