Institut for Matematik og Datalogi
Syddansk Universitet

February 18, 2008
JFB

Cryptology – F08 – Week 5

Lecture, February 14

We covered AES. The original Rijndael specification (which can be found through the course's homepage, which I updated on February 15) will be used as the basis for the description of AES. We also began on chapter 5 in the textbook.

Lecture, February 22

We will continue with chapter 5.

Lecture, February 28

We will finish chapter 5 and possibly begin on chapter 6.

No class (or office hours) February 21

Problem sessions February 25 and 29

1. With RSA, there are often recommendations to use a public exponent $e = 3$.

   a. What would the advantage to this be?

   b. If $e = 3$, the two prime factors dividing the modulus, p and q, must be such that $p \equiv q \equiv 2 \pmod{3}$. Why is it impossible to have one or both of p and q congruent to 0 or 1 modulo 3?

   c. Suppose that $e = 3$, $p = 3r + 2$ and $q = 3s + 2$. What would the decryption exponent d be?

2. Suppose we have a set of blocks encoded with the RSA algorithm and we do not have the private key. Assume $(n = pq, e)$ is the public key. Suppose also that someone tells us they know one of the plaintext blocks has a common factor with n. Does this help us find the plaintext used to produce these blocks? If so, how? If not, why not?

3. Suppose the modulus used in RSA has 1024 bits. What is the unicity distance of this RSA cryptosystem? Why?

4. Suppose that user A wants to send a message $s \in \{s_1, s_2, ..., s_k\}$ to user B, where $s_i < 1024$ for $1 \leq i \leq k$. Assume that RSA is secure (when the modulus is large enough and is the product of two equal length prime factors).

   a Why would you still advise user A not to use RSA directly?

   b What would you recommend instead, if you still wanted to use RSA?

5. Show all steps in the calculations of the Jacobi symbol $\left(\frac{29}{35}\right)$, using the standard algorithm (using the four properties of the Jacobi symbol given in the textbook).

6. Show all steps of the execution of one call to the Solovay-Strassen Primality Test, checking if 35 is prime. Assume that the random integer a chosen is 19.

7. A *Carmichael number* is a composite integer n such that for all $x \in Z_n^*$, $x^{n-1} \equiv 1 \pmod{n}$.

   a Explain why the existence of Carmichael numbers (there are in fact infinitely many of them) make primality testing more difficult.

   b Explain why Carmichael numbers are easy to factor using intermediate calculations from the Miller–Rabin primality test.

   c Show that 561 is a Carmichael number. Try to do it without explicitly checking all elements of $\mathbb{Z}_{561}^*$.

8. Suppose that $n = pq$ is odd, and p and q are prime. Suppose that 3 divides $(p-1)$, but not $(q-1)$.

   a How many cubed roots of 1 are there, i.e. how many x are there such that $x^3 \equiv 1 \pmod{n}$? Why?

b Suppose you had a probabilistic polynomial time algorithm for finding sixth roots of 1 in Z_n^*, i.e. x such that $x^6 \equiv 1 \pmod{n}$. How would you use this algorithm to factor n?

9. Do problems 5.9, 5.13, 5.16 and 5.17 in the textbook.

10. 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.)

11. Find all square roots of 64 modulo 105.

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

Assignment due Friday, March 14, 12:15

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. You may write in either English or Danish.

1. 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 $2^{341} \pmod{341}$.

2. 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?

3. In the RSA cryptosystem, the public key consists of the modulus n and the exponent b, while the decryption exponent a is kept secret. Suppose a user U leaks his secret key a. Suppose further that when creating a new key pair, for efficiency reasons, he keeps the same modulus, but finds new exponents a' and b'. Is this secure? Why or why not?

4. On page 212 of the textbook, there is a formula for computing square roots modulo a prime p where $p \equiv 1 \pmod{4}$. One can also deterministically compute a square root when $p \equiv 5 \pmod{8}$, using a similar idea and the fact that you know a quadratic nonresidue modulo such values of p. Explain how to do this and why it works.