Institut for Matematik og Datalogi
Syddansk Universitet

February 21, 2013
JFB

Cryptology – F13 – Week 4

Lecture, February 11

We covered most of chapter 3 in the textbook, skipping most of the first four sections. The original Rijndael specification (which can be found through the course's homepage) was used as the basis for the description of AES.

Lecture, February 18

We briefly covered differential and linear cryptanalysis, plus modes of operation for block cyphers from chapter 3 in the textbook. We began on chapter 5 in the textbook, skipping the Extended Euclidean Algorithm. We covered RSA, except for showing how to find primes. We showed that factoring was polynomial time equivalent to finding square roots modulo a composite (though still need to show how to find square roots modulo primes or prime powers).

Lecture, February 21

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

Lecture, February 22

We will continue with chapter 5, covering primality testing.

Lecture, February 28

We will begin on chapter 6.

Problem session February 25

1. In the original description of Rijndael, it says that x^4+1 (which is used to create the matrix for the MixColumn operation) is not irreducible over $GF(2^8)$. What are its factors? Try the function `Factor` in Maple, using `mod 2`. Check that the `mod 2` makes a difference by also trying to factor it with `factor`.

   Check that $x^8 + x^4 + x^3 + x + 1$ is irreducible over $GF(2)$. Check the multiplication done in the example in section 2.1.2 using the `modpol` function in Maple.

   Find the inverse of $x^7 + x^5 + x^3 + 1$ modulo $x^8 + x^4 + x^3 + x + 1$. Try the function `powmod` using the exponent -1. Check that your answer is correct using `modpol`.

2. Why do you think $x^4 + 1$ was used, rather than an irreducible polynomial? Why are there no problems that it is not irreducible?

3. Check that the definition given for the polynomial $d(x)$ in section 2.2 is correct (for multiplication). Try using `powmod` with the exponent 1 in Maple.

   Similarly, check that the polynomial $d(x)$ used in MixColumn in section This problem is probably just about as easy to do by hand.

4. Find the inverse transformation for ByteSub in section 4.2.1. To find the inverse modulo 2 of the matrix, you can use the `Inverse` function in Maple. To create the matrix, you can use the function `Matrix` (in the LinearAlgebra package, so you have to type `with(LinearAlgebra);` first) and list the matrix row by row. For example, to create the matrix $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, you can type `A:=Matrix([[1,2],[3,4]]);`. To check the result, you can multiply two matrices, A and B using `C:=A.B;`. To reduce all the elements of the matrix modulo 2, you can use the `Map` function, for example as `Map(modp,C,2);`.

5. Why doesn't the last round of AES have the MixColumn operation?

6. Look at problems 5.3, 5.6, and 5.7 in the textbook. If you are at all unsure of how to do them, please do them. Even if you are not unsure, you might consider this an opportunity to try using Maple.

The following Maple functions should be useful: `igcdex` (extended Euclidean algorithm for integers), `mod` (where the operation `&^` should be used for more efficient modular exponentiation - try them both to compare), `msolve` (solve equations in $\mathbb{Z}_m$), and `chrem` (Chinese Remainder Algorithm).

7. Another easy problem. Let $n = 143$ be a modulus for use in RSA. Choose a public encryption exponent e and a private decryption exponent d which can be used with this modulus. Try encrypting and decrypting some value to see that the exponents you have chosen work.

8. Suppose you as a cryptanalyst intercept the ciphertext $C = 10$ which was encrypted using RSA with public key $(n = 35, e = 5)$. What is the plaintext M? How can you calculate it?

9. In an RSA system, the public key of a given user is $(n = 3599, e = 31)$. What is this user's private key?

10. I may lecture at the end.

Problem session March 1

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

3. 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?

4. 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).

5. 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.

6. 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 $\mathbb{Z}_{561}^*$.

7. Do problems 5.9 and 5.13 in the textbook.

8. I may lecture at the end.