

## Cryptology – F08 – Week 4

### **Lecture, February 8**

We covered sections 2.2, 2.3, and 2.7 of chapter 2 and 3.5, and 3.7 of chapter 3 in the textbook (skipping most of the first four sections).

### **Lecture, February 14**

We will cover AES. The original Rijndael specification (which can be found through the course's homepage) will be used as the basis for the description of AES. We will also begin on chapter 5 in the textbook. My plan is to skip section 5.2.1 on the Extended Euclidean Algorithm. Please let me know if you haven't seen it before.

### **Lecture, February 22**

We will continue with chapter 5.

### **No class February 15**

### **No class (or office hours) February 21**

### **Problem session February 18**

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. In Maple, I found it useful to multiply the polynomials, use the right mouse button to find `collect` and `x`, and repeatedly add on appropriate multiples of  $x^4 + 1$ . There might be a better way, but I couldn't get the `modpol` function to do anything in this case.

Similarly, check that the polynomial  $d(x)$  used in `MixColumn` in section 4.2.3 is correct.

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?