MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2007
May 23, 2007

Cryptography

Problem Sheet #6

Problem 21

The elements of the field $\mathbb{F}_{2^4} = \mathbb{F}_2[X]/(\varphi(X))$, where φ is the irreducible polynomial $\varphi(X) = X^4 + X + 1 \in \mathbb{F}_2[X]$, are identified with 4-bit integers, where $\xi = \sum_{i=0}^{3} a_i 2^i$ corresponds to $\sum a_i X^i \bmod \varphi(X)$. We use hexadecimal notation for the 4-bit integers.

a) Let $u :=$ '`2`', $v :=$ '`6`'. Calculate $u + v$, $u \cdot v$, u^3 and u^5.

b) Show that the element $u =$ '`2`' is a primitive root of $\mathbb{F}_{2^4}^*$, i.e. a generator of the multiplicative group $\mathbb{F}_{2^4}^*$.

Problem 22

With $F(X) := X^8 + 1 \in \mathbb{F}_2[X]$ define the ring $R := \mathbb{F}_2[X]/(F(X))$, which is an 8-dimensional vector space over $\mathbb{F}_2$. Let

$$G(X) := X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X].$$

Consider the map

$$\psi : R \to R, \quad f \mapsto \psi(f) := G \cdot f \bmod F.$$

a) Show that the matrix of ψ with respect to the basis $(\overline{1}, \overline{X}, \ldots, \overline{X^7})$ of R over $\mathbb{F}_2$ is

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Remark. This matrix appears in the description of the byte substitution in AES.

b) Show that $\gcd(F, G) = 1$ and calculate the inverse of $G \bmod F$ in the ring R.

c) Show that the matrix $M \in \mathrm{M}(8 \times 8, \mathbb{F}_2)$ is invertible and calculate its inverse.

Problem 23

We define a binary operation $\boxtimes : \mathbb{Z}_{256} \times \mathbb{Z}_{256} \to \mathbb{Z}_{256}$ using the bijective map

$$\phi : \mathbb{Z}_{256} \to \mathbb{F}_{257}^*, \quad x \mapsto \phi(x) := \begin{cases} 256 & \text{if } x = 0, \\ x & \text{if } x \neq 0, \end{cases}$$

as follows: $x \boxtimes y := \phi^{-1}(\phi(x) \cdot \phi(y))$, where '$\cdot$' denotes multiplication in the field $\mathbb{F}_{257}$.

a) Prove that $(\mathbb{Z}_{256}, \boxtimes)$ is a group, which is isomorphic to $(\mathbb{Z}_{256}, +)$.
b) Show that $(\mathbb{Z}_{256}, +, \boxtimes)$ is not a ring.

Problem 24

The following ciphertext was encrypted using a mini-version of a 2-round Feistel network: The block length is $16 = 2 \times 8$ bits $= 2$ bytes. The i-th round transformation is $(L, R) \mapsto (R, L \oplus f(R, K_i))$ with

$$f(x, K_i) := (A_i \boxtimes x + B_i) \bmod 2^8,$$

where $\boxtimes$ was defined in problem 23 and $K_i = (A_i,\, B_i) \in \mathbb{Z}_{2^8}^2$, $i = 1, 2$, are independent round keys. After the last round, the left and right halves are swapped. The plaintext begins with the four bytes "`The `" (hexadecimal `5468 6520`).

```
10B4 D2A9 1F20 75A1 72AF 7371 7B27 9A5F 0CAA FDAD FD4C C62E
767E C1A0 7E64 157B 043A 5CA7 C62E B867 82F3 D0D8 DF6C
```

Determine the keys K_1, K_2 and decrypt the ciphertext.

Due: Wednesday, May 30, 2007, 14:10 h

Solutions should be returned in the Cryptography letter box in the first floor of the Institute in front of the library.