MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2005
May 26, 2005

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

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

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

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

Problem 23

With $F(X), G(X) \in \mathbb{F}_2[X]$ as in problem 22, show that $\gcd(F, G) = 1$ and calculate the inverse of G mod F in the ring $\mathbb{F}_2[X]/(F(X))$, i.e. determine a polynomial $H(X) \in \mathbb{F}_2[X]$ such that

$$G(X)H(X) \equiv 1 \bmod F(X).$$

Hint: Use the extended euclidean algorithm.

Problem 24

Using problem 23, calculate the inverse of the matrix $M \in \mathrm{M}(8 \times 8, \mathbb{F}_2)$ of problem 22.

Due: Thursday, June 2, 2005, 14:10 h