MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2007
May 30, 2007

Cryptography

Problem Sheet #7

Problem 25

a) Let x, y be two randomly and independently chosen elements of $\mathbb{Z}_2^{64}$ (we assume uniform distribution). Estimate the probabilty that there exists a DES-key K such that $\mathrm{DES}_K(x) = y$.

b) $\mathbb{Z}_2^8$ can be identified with the field $\mathbb{F}_{256}$ of $2^8 = 256$ elements, hence $\mathbb{Z}_2^{64}$ can be identified with the 8-dimensional vector space $\mathbb{F}_{256}^8$ over $\mathbb{F}_{256}$. Determine the number of bijective linear maps $f : \mathbb{F}_{256}^8 \to \mathbb{F}_{256}^8$ and compare it with the number of bijective maps $\mathbb{Z}_2^{64} \to \mathbb{Z}_2^{64}$ which are induced by DES.

Problem 26

Let K be a field and let R be the ring $R := K[T]/(T^4 - 1)$. This is a 4-dimensinal vector space over K. Multiplication by a polynomial

$$a(T) := a_3T^3 + a_2T^2 + a_1T + a_0 \in K[T]$$

induces a K-linear map

$$a : R \to R, \quad g(T) \bmod (T^4 - 1) \mapsto a(T)g(T) \bmod (T^4 - 1).$$

a) Calculate the matrix $C = C(a_0, a_3, a_2, a_1) \in M(4 \times 4, K)$ of the map a with respect to the basis $(\overline{1}, \overline{T}, \overline{T^2}, \overline{T^3})$ of R over K.
Remark. A matrix of the form $C(a_0, a_3, a_2, a_1)$ is called a *circulant* matrix. Such a matrix occurs in the `MixColumns` operation of AES.

b) Show that the matrix C is invertible if and only if the polynomials $a(T)$ and $T^4 - 1$ are relatively prime. In this case the inverse of C is also a circulant matrix.

c) As an example consider the field $K = \mathbb{F}_{16}$ as defined in problem 21. Let

$$a(T) = \texttt{'3'} \cdot T^3 + T^2 + T + \texttt{'2'} \in \mathbb{F}_{16}[T]$$

Calculate the matrix $C(a_0, a_3, a_2, a_1)^{-1}$ in this case.

---

p.t.o.

Problem 27

Alice uses a block cipher system $E : \mathbb{Z}_2^b \to \mathbb{Z}_2^b$ in CBC mode with an initial vector $y_0 \in \mathbb{Z}_2^b$,

$$y_i := E(x_i \oplus y_{i-1}), \quad \text{for all } i \geq 1,$$

and sends Bob (who knows E^{-1}) the cipher text $(y_0, y_1, y_2, \ldots)$, where $(x_1, x_2, \ldots)$ is the plaintext.

a) An error occurs during the transmission of the block y_1, so that Bob receives an incorrect block y_1' instead of y_1. Which blocks of the plaintext can Bob decrypt correctly?

b) Assume that an error occurs in Alice's computer during the encryption of the second block and she gets an incorrect block $\tilde{y}_2$ instead of y_2. Which blocks of the ciphertext are affected by this error? Which blocks of the plaintext can Bob decrypt correctly, if no error occurs during transmission?

Problem 28

a) Prove that for an odd integer K the map

$$f_K : \mathbb{Z}_{2^m} \longrightarrow \mathbb{Z}_{2^m}, \quad x \mapsto x(2x + K) \bmod 2^m,$$

is bijective.

b) Let $m = 16$. We identify $\mathbb{Z}_{2^{16}}$ with $\mathbb{Z}_2^{16}$ by

$$x = \sum_{i=0}^{15} b_i \, 2^i \mapsto (b_{15}, b_{14}, \ldots, b_1, b_0) \in \mathbb{Z}_2^{16}$$

and use f_K as a block cipher $\mathbb{Z}_2^{16} \to \mathbb{Z}_2^{16}$. Encrypt the text "`CFB mode`", hexadecimal

```
4346 4220 6D6F 6465
```

by the 8-bit variant of CFB mode of f_K with initial vector $iv =$ `AB56` and key $K =$ `8BED` (hexadecimal notation).
A specification of the r-bit variant of CFB mode can be found on page 3.

c)* The following ciphertext has been obtained by encrypting an English ASCII text in 8-bit CFB mode of f_K with the same initial vector as in b) but with an unknown key K

```
C9CF D081 7360 286E 9EAE A550 4328 1955 A09C AE7E 886D 6EAB
68ED FBD4 3FCA 4061 A19B 0303 7F54 2333 431D FA7B 050F 1A
```

Find the key K and the plaintext.

Problems marked by an asterisk * are not obligatory, but solutions get extra points.

Due: Friday, June 8, 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.

Specification of the r-bit variant of CFB mode

Suppose given a block cipher

$$E_K : \mathbb{Z}_2^m \longrightarrow \mathbb{Z}_2^m$$

and a positive integer $r \leq m$. Then the r-bit variant of CFB encrypts a plaintext

$$x = (x_1, x_2, \ldots, x_N), \quad x_i \in \mathbb{Z}_2^r,$$

to a ciphertext

$$y = (y_1, y_2, \ldots, y_n), \quad y_i \in \mathbb{Z}_2^r,$$

depending on an initial vector $iv \in \mathbb{Z}_2^m$, in the following way:

We construct recursively a sequence of blocks $z_i \in \mathbb{Z}_2^m$, $i \geq 1$. Let $z_1 := iv$. For $i \geq 2$, the block z_i is formed by shifting z_{i-1} by r bit positions to the left and feeding the previous ciphertext block y_{i-1} into the free positions on the right. More precisely: Let

$$z_{i-1} = (b_{m-1}, \ldots, b_1, b_0) \in \mathbb{Z}_2^m \quad \text{and} \quad y_{i-1} = (c_{r-1}, \ldots, c_1, c_0) \in \mathbb{Z}_2^r.$$

Then

$$z_i := (b_{m-r-1}, \ldots, b_1, b_0, c_{r-1}, \ldots, c_1, c_0) \in \mathbb{Z}_2^m.$$

Now define $u_i := E_K(z_i) \in \mathbb{Z}_2^m$. Let $t_i \in \mathbb{Z}_2^r$ consist of the r leftmost bits of u_i, i.e. for

$$u_i = (a_{m-1}, \ldots, a_1, a_0) \in \mathbb{Z}_2^m \quad \text{set} \quad t_i := (a_{m-1}, \ldots, a_{m-r}) \in \mathbb{Z}_2^r.$$

The i-th ciphertext block y_i is defined by `XOR`ing the plaintext block x_i with t_i,

$$y_i := x_i \oplus t_i \in \mathbb{Z}_2^r.$$

In applications usually m is a multiple of r. Often $r = 8$, i.e. the plaintext and ciphertext blocks are single bytes. The case $r = m$ reduces to the ordinary CFB mode:

$$y_0 := iv, \quad y_i := x_i \oplus E_K(y_{i-1}) \text{ for } i \geq 1.$$