MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2005
May 31, 2005

Cryptography

Problem Sheet #7

Problem 25

Let $f : \mathbb{Z}_{2^m} \to \mathbb{Z}_{2^m}$ be defined by $x \mapsto x(2x+1) \bmod 2^m$.

a) Show that f is a bijection.

b) Work out an algorithm which computes the inverse of f.
Hint: Induction on m.

Problem 26

The following byte string $y = (y_0, y_1, y_2, \ldots, y_{52})$ was obtained from an English ASCII plaintext $x = (x_1, \ldots, x_{52})$ using the function $f : \mathbb{Z}_{256} \to \mathbb{Z}_{256}$ from problem 25 in the following way: $y_i := f(x_i \oplus y_{i-1})$ for all $i \geq 1$.

```
3AC5 1D4F A81F 331E 8CBF A52B FDC6 A4C9 0BAE C389 0C4C 414B 44F3 2177
79CD 2888 78D2 5941 44FE AC6B D1B3 298E 36C5 CEAC ACC3 CC28 9F
```

Find the plaintext!

Problem 27

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

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

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

a) An error occurs during the transmission of the first 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

Discuss a scenario analogous to problem 27, when Alice uses the k-bit variant of CFB mode. Assume that $s = rk$ with an integer $r > 1$.

Due: Thursday, June 9, 2005, 14:10 h