Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Jose Leon

Exercise 5

Friday, May 27, 2016

Problem 1. *(Perfect secrecy for affine cipher)* Consider affine ciphers on $\mathbb{Z}_{26}$, i.e., $\mathcal{M} = \mathcal{C} = \mathbb{Z}_{26}$ and $\mathcal{K} = \mathbb{Z}_{26}^* \times \mathbb{Z}_{26} = \{(a,b) \mid a, b \in \mathbb{Z}_{26}, \gcd(a, 26) = 1\}$. Select the key $\hat{K}$ uniformly distributed at random and independently from the message $\hat{M}$.

Show that this cryptosystem has perfect secrecy.

Problem 2. *(Demo perfect secrecy)* Let $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ be a cryptosystem. Suppose that $P(\hat{M} = M) > 0$ for all $M \in \mathcal{M}$, $P(\hat{K} = K) > 0$ for all $K \in \mathcal{K}$ and $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$. Show that if $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ has perfect secrecy, then

$$P(\hat{K} = K) = \frac{1}{|\mathcal{K}|} \text{ for all } K \in \mathcal{K} \text{ and}$$

for all $M \in \mathcal{M}, C \in \mathcal{C}$, there is a unique $K \in \mathcal{K}$ such that $e(M, K) = C$.

Problem 3. (*block ciphers are permutations*) A block cipher is a cryptosystem where both plaintext and ciphertext space are the set $\mathcal{A}^n$ of words of length n over an alphabet $\mathcal{A}$.

a) Show that the encryption functions of block ciphers are permutations.

b) How many different block ciphers exist if $\mathcal{A} = \{0, 1\}$ and the block length is $n = 6$?

Problem 4. (*DES Complementation property*) Let M be a block of bits of length 64 and let K be a block of bits of length 56. Let $\text{DES}(M, K)$ denote the encryption of M with key K using the DES cryptosystem. $\overline{x}$ denotes the bitwise complement of a block x.

a) Show that the *complementation property* holds:

$$\text{DES}(M, K) = \overline{\text{DES}(\overline{M}, \overline{K})}$$

b) How does the complementation property help to attack DES?

Problem 5. (*weak DES keys*) There are four so called *weak* DES keys. One of those keys is

$$K = 00011111\ 00011111\ 00011111\ 00011111\ 00001110\ 00001110\ 00001110\ 00001110.$$

a) What happens if you use this key?

b) Can you find the other three weak keys?