# M 375 – Homework 2

**10.2.1**

The polynomial encoding function has six input variables and three output variables:

$$f : F_2^6 \longrightarrow F_2^3$$

$$f(x_1, x_2, x_3, y_1, y_2, y_3) = (x_1x_2y_1y_2, x_2x_3y_3y_1, (x_1 + x_2)y_1y_3) .$$

The keys are $k_1 = (1,0,1)$ and $k_2 = (0,1,1)$. The message $M = (1,1,1,1,1,1)$ is broken into two pieces $m_0 = (1,1,1)$ and $m_1 = (1,1,1)$.

Encryption procedure:

$$m_2 = m_0 + f(k_1, m_1) = (1,1,1) + f((1,0,1),(1,1,1)) = (1,1,1) + (0,0,1) = (1,1,0)$$
$$m_3 = m_1 + f(k_2, m_2) = (1,1,1) + f((0,1,1),(1,1,0)) = (1,1,1) + (0,0,0) = (1,1,1)$$

The cyphertext consists of $C = (m_2, m_3) = (1,1,0,1,1,1)$.

**10.2.2**

Again the encryption function has six input and three output variables:

$$f : F_2^6 \longrightarrow F_2^3$$

$f$ permutes the elements of the message $m_i$ with the keys $k_1 = (1,2,3)$, $k_2 = (2,1,3)$, $k_3 = (3,2,1)$, and $k_4 = (2,3,1)$.

The message is $M = (1,0,1,01,1)$, $m_0 = (1,0,1)$ and $m_1 = (0,1,1)$.

$$m_2 = m_0 + f(k_1, m_1) = (1,0,1) + (0,1,1) = (1,1,0)$$
$$m_3 = m_1 + f(k_2, m_2) = (0,1,1) + (1,1,0) = (1,0,1)$$
$$m_4 = m_2 + f(k_3, m_3) = (1,1,0) + (1,0,1) = (0,1,1)$$
$$m_5 = m_3 + f(k_4, m_4) = (1,0,1) + (1,1,0) = (0,1,1)$$

Thus, the message $M$ is encrypted as $C = (m_4, m_5) = (0,1,1,0,1,1)$.

In order to get the plaintext message from the cyphertext $C = (1,0,1,0,1,1)$ one has to apply the inversion of the encryption algorithm. Since we are operating on the field modulo 2 ‘minus’ is equal to ‘plus’.

$$m_3 = m_5 - f(k_4, m_4) = m_5 + f(k_4, m_4) = (0,1,1) + (0,1,1) = (0,0,0)$$
$$m_2 = m_4 + f(k_3, m_3) = (1,0,1) + (0,0,0) = (1,0,1)$$
$$m_1 = m_3 + f(k_2, m_2) = (0,0,0) + (0,1,1) = (0,1,1)$$
$$m_0 = m_2 + f(k_1, m_1) = (1,0,1) + (0,1,1) = (1,1,0)$$

Therefore, the original message was $M = (1,1,0,0,1,1)$.

**10.3.1**

Each bit string has $2^n$ permutations and there are $2^n$ mapping function

$$f : (b_1, ..., b_n) \longrightarrow (b_1, ..., b_n).$$

So we have $\underbrace{2^n \cdot 2^n \cdot ... \cdot 2^n}_{2^n \text{ times}} = \left(2^n\right)^{2^n} = 2^{n2^n}$ elements in $F^n$.

**p. 176, problem 2**

Given is a function $f : V_n \longrightarrow V_n$ which maps a binary vector to another binary vector and $f(f(x)) = x$ (involution) $\forall x \in A$ then this involution is a 1-1 mapping.

Assume that the involution is not a one-to-one mapping $\Rightarrow$

$$|A| > |f(A)|$$

Apply function *f* again:

$$|f(A)| > |f(f(A))|.$$

Because of the involution property and transitivity:

$$|A| > |A|.$$

This is false, thus the assumption is wrong and the opposite is true.

**p. 176, problem 6**

Push $2^{2^n}$ different message through the encryption algorithm and one gets a mapping of the entire encryption function (plaintext and cyphertext).

This is the reason why the DES encryption is no longer considered to be safe. An exhaustive search for keys ($2^{56}$) can be accomplished within a few hours and at reasonable low costs (see Douglas R. Stinson, CRYPTOGRAPHY: THEORY AND PRACTICE, CRC Press, Boca Raton, FL, et al., 1995, pp. 82).