Exercise 23. There are four so called *weak* DES keys. One of those is the key

\[ K = 00011111 \ 00011111 \ 00011111 \ 00011111 \ 00001110 \ 00001110 \ 00001110 \ 00001110. \]

What happens if you use this key? Can you find the other three weak keys?

Exercise 24. A block cipher is a cryptosystem where plaintext and ciphertext space are the set \( A^n \) of words of length \( n \) over an alphabet \( A \). The number \( n \) is called the block length.

Show that the encryption functions of block ciphers are permutations. How many different block ciphers exist if \( A = \{0, 1\} \) and the block length is \( n = 6 \)?

Exercise 25. Consider the following AES-128 key given in hexadecimal notation:

\[ K = 2d \ 61 \ 72 \ 69 \ 65 \ 00 \ 76 \ 61 \ 6e \ 00 \ 43 \ 6c \ 65 \ 65 \ 66 \]

a) What is the round key \( K_0 \)?

b) What are the first 4 bytes of round key \( K_1 \)?

Exercise 26. Within the step MixColumns of the AES algorithm a vector \( r \) is given by \( r = Tc \) with \( c = (c_0, c_1, c_2, c_3)' \), \( c_i \in \mathbb{F}_{2^8}[x] \), and

\[
T = \begin{pmatrix}
    x & (x+1) & 1 & 1 \\
    1 & x & (x+1) & 1 \\
    1 & 1 & x & (x+1) \\
    (x+1) & 1 & 1 & x \\
\end{pmatrix}.
\]

Show \((c_3u^3 + c_2u^2 + c_1u + c_0)((x+1)u^3 + u^2 + u + x) = r_3u^3 + r_2u^2 + r_1u + r_0 \ mod \ u^4 + 1.\)