1. Consider a cryptosystem where the key $k$, the message $m$, and the ciphertext $c$ are each $n$ bits long. Each bit of the ciphertext is given as follows:

\[
\begin{align*}
    c_1 &= k_1m_1 + k_2m_2 + \cdots + k_nm_n \\
    c_2 &= k_nm_1 + k_1m_2 + \cdots + k_{n-1}m_n \\
    c_3 &= k_{n-1}m_1 + k_nm_2 + \cdots + k_{n-2}m_n \\
    &\vdots \\
    c_n &= k_2m_1 + k_3m_2 + \cdots + k_1m_n
\end{align*}
\]

Is this cryptosystem secure? Justify your answer.

2. Prove or disprove that each of the following functions is linear over the field $GF(2)$ (i.e., the set $\{0, 1\}$ along with $+$ and $\cdot$, where $+$ is defined as XOR and $\cdot$ is defined as AND).

(a) The parity function on $n$ bits, i.e. $p : \{0, 1\}^n \rightarrow \{0, 1\}$ where

\[
p(b_1, \ldots, b_n) = \begin{cases} 
    0 & \text{if } (b_1, \ldots, b_n) \text{ has an even number of 1's}, \\
    1 & \text{otherwise}. 
\end{cases}
\]

(b) The function $f_q : \{0, 1\}^n \rightarrow \{0, 1\}$, where

\[
f_q(x_1, x_2, \ldots, x_n) = q(x_1 + x_2 + \cdots + x_n)
\]

and $q$ is any polynomial with coefficients in $\{0, 1\}$.

(c) The S-box $S_1$ used in the DES.

3. Describe the meet-in-the-middle (MITM) attack on 2DES where the attacker has three pairs of plaintexts and corresponding ciphertexts. What is the probability that the attack will succeed? Justify your answer in detail.

4. Let $DES(x, K)$ represent the encryption of plaintext $x$ with key $K$ using the DES cryptosystem. Suppose $y = DES(x, K)$ and $y' = DES(c(x), c(K))$, where $c(\cdot)$ denotes the bitwise complement of its argument. Prove that $y' = c(y)$ (i.e., if we complement the plaintext and the key, then the ciphertext is also complemented). Note that this can be proved using only the “high-level” description of DES – the actual structure of $S$-boxes and other components are irrelevant.