Problem Q-1. Hash functions from symmetric block ciphers

In this problem we will consider two proposals to construct hash functions from symmetric block encryption schemes as DES and RC5.

Let E denote a symmetric block encryption scheme. Let $E_k(M)$ denote the encryption of the 1–block message M under key k. Let $M = M_0 \circ M_1 \circ M_2 \circ \ldots \circ M_n$ denote a message of $n+1$ blocks.

The first proposed hash function h_1 works as follows: let $H_0 = M_0$ and then define

$$H_i = E_{M_i}(H_{i-1}) \oplus H_{i-1} \quad \text{for} \quad i = 1, \ldots, n.$$

The value of the hash function is defined as

$$h_1(M) = H_n$$

The second proposed hash function h_2 is similar. Again $H_0 = M_0$ and then

$$H_i = E_{H_{i-1}}(M_i) \oplus M_i \quad \text{for} \quad i = 1, \ldots, n.$$

The value of the hash function is defined as

$$h_2(M) = H_n$$

For both proposals, show how to find collisions if the encryption scheme E is chosen to be DES.