Homework Set 9 (Lecture 31)

Problem 1

Example 24. Consider the following compression function $C(x)$ which takes three bits input and outputs two bits:

x	000	001	010	011	100	101	110	111
$C(x)$	10	00	11	01	01	10	00	11

Let $H(x)$ be the hash function obtained from $C(x)$ using the Merkle–Damgård construction (using initial value $h_1 = 0$). Compute $H(11000)$.

Solution. Here, $b = 2$ and $c = 1$, so that each x_i is 1 bit: $x_1x_2x_3x_4x_5 = 11000$.
$h_1 = 00$
$h_2 = C(h_1, x_1) = C(001) = 00$
$h_3 = C(h_2, x_2) = C(001) = 00$
$h_4 = C(h_3, x_3) = C(000) = 10$
$h_5 = C(h_4, x_4) = C(100) = 01$
$h_6 = C(h_5, x_5) = C(010) = 11$
Hence, $H(11000) = h_6 = 11$.