Problem 9): We can calculate the probability of finding a collision here. There are $N_{TOT} = \prod_{i=1}^{l} \{2^n\} = (2^n)^l$ total possible messages with l blocks and block-length n. Out of these, there are $N_{NO-COL} = \prod_{i=1}^{l} \{2^n - i + 1\}$ messages that will have no collisions because one message is removed from the number available for each subsequent block. Therefore, the number of messages with collisions in the *must* be

$$\begin{aligned} N_{COL} = N_{TOT} - N_{NO-COL} &= \prod_{i=1}^{l} \{2^n\} - \prod_{i=1}^{l} \{2^n - i + 1\} \\ &= (2^n)^l - \prod_{i=1}^{l} \{2^n - i + 1\} \end{aligned} \tag{9.1}$$

This allows the probability