# Mac Attack HW

Jackson Mowry

Tue Sep 16 09:15:56 2025

## Contents

1. How are $p_1$ and $l_1$ calculated?
    - Padding is calculated based on the fact that we need to produce a message with a round number of bits (relative to 512 bit blocks), the message needs to have a single `1` bit added, and finally the message needs to include a 64-bit integer of the message length. We can solve this equation by solving for k in `l + 1 + k = 448mod512` where `l` is the length of $m_1$ in bits.
    - $l_1$ is calculated by adding the original message length and the required padding togther to give the final length before hashing is performed.
2. What are the contents of m'?
    - m' would be Alice's original message $m_1$, concatenated with the original padding $p_1$, and finally Malory's message $m_2$.
    - My only question here is: Assuming this was originally a text based ascii message, wouldn't the padding $p_1$ show up as a section of NULL bytes, thus effectively ending the string? If it was some other binary format with variable length data I assume these NULL bytes would simply be ignored.
3. How are $p_2$ and $l_2$ calculated?
    - The padding and length are calculated based only on the text that Malory wants to add. This is performed in the same way as $m_1$, just with the new information.
4. What are the inputs to SHA-1'?

- Malory would input both the original message digest (as internal state) from Alice's message and $m_2$ (the piece she is adding).
- SHA-1' takes 2 inputs (message and dynamic IV), as opposed to SHA-1 which only takes the message as input.

5. How is SHA-1' used to calculate $MAC_2$

   - SHA-1' is initialized with $MAC_1$ to be its IV. This way we have a known "good" starting point that was already computed using the concatenation of Bob/Alice's shared key and Alices original message. Then Malory will input $m_2$ and receive the final digest that will be sent to bob along with m'.
   - The output from the previous step is fed into SHA-1 at the beginning of each step, so we are effectively changing out the IV that is used by default in SHA-1 to be $MAC_1$
   - SHA-1 uses a fixed IV, whereas SHA-1' uses a dynamic value based on the message we are trying to maliciously modify