

# Hw3

Jackson Mowry

Wed Sep 3 09:33:29 2025

1. Pseudocode for the padding function described in Section 5.1.1.

```
# Equation we're trying to solve  $1 + 1 + k == 448 \bmod 512$   
# Simplifies to  $448 - (1 + 1) = k$ 
```

```
def pad_message(message: u1[]) -> void:  
    message_len: u64 = length of message in bits  
    k = 448 - (message_len + 1)  
  
    message += 1  
    for 0 to k:  
        message += 0  
    end  
  
    message += message_len as u1[]
```

1. Pseudocode for calculating the messaging schedule ( $W_t$ ) described in Section 6.1.2.

```
def message_schedule(message: u1[], block: u32) -> u32[]:  
    current_block = message[(block * 512)..(block * 512 + 512)]  
    w: u32[] = []  
  
    for i = 0 to 80:  
        if i >= 0 && i <= 15:  
            w += current_block[(i * 32)..(i * 32 + 32)]  
        else  
            w += rotl(w[i-3] ^ w[i-8] ^ w[t-14] ^ w[t-16])  
        fi
```

```
end
```

```
return w
```