DFSM Design:

The DFSM has two state machines acting in parallel:

1. Producer
2. Consumer

The producer will continuously read 128-bit words from the OCM using the AXI master and feed the bus output to a 64-bit wide FIFO of depth 64 (64 x 64 bits). If the FIFO is half-full, the AXI master read data ready signal will be low, and reading will pause until data from the FIFO is consumed. The master bus is reading at a burst size of 1 word, and the DFSM is providing the AXI master with what address to read from.

The consumer will continuously attempt to read 64-bit words from the FIFO and handle all Keccak signals. These signals include in_ready, is_last, and byte_num. The state machine will pause whenever the Keccak buffer is empty, and feed 64-bit words to the Keccak module as words are read from the FIFO. The consumer will keep track of how many bytes it has written into the Keccak module, and assert is_last when appropriate.

Timer Design:

The timer is the same as the timer used in Lab 2, except the timer starts with SHA_START and ends with SHA_DONE.

Testing:

The SHA3 accelerator is tested manually with different inputs and compared using the online Keccak-512 tool. These are the edge cases I tested to validate the accelerator:

1. Simple string: “The quick brown fox jumps over the lazy dog”
2. Zero length: “”
3. String of length that is a multiple of 8
4. Very long string to check for full FIFO pausing (length 3000)

All test cases passed.