W9. The Preprocessing Unit for the Secure Hash Algorithm – 256

1) Theoretical Background

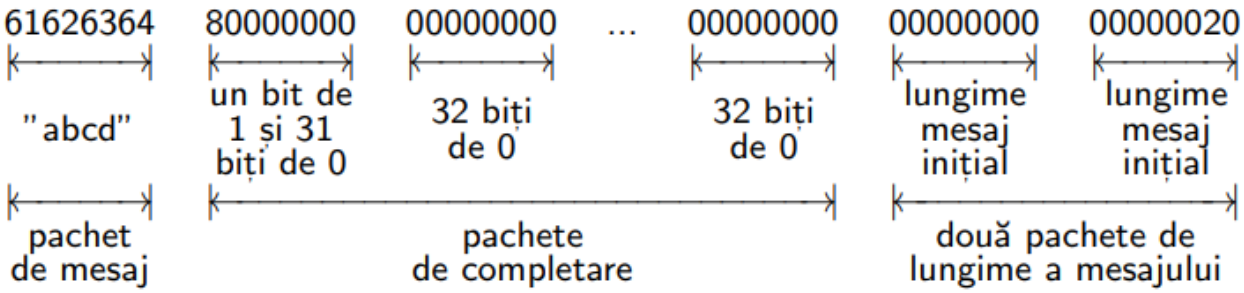
The 256-bit SHA-2 input preprocessing unit implements the preprocessing phase, described in ["FIPS PUB 180-4: Secure Hash Standard," Gaithersburg, MD 20899-8900, USA, Tech. Rep., Aug. 2015] (section 5.1.1) consisting of completing and dividing the message.

Completing the message: For an initial message of length ***l***, the completion adds a bit of 1 and ***k*** bits of 0, so that **l** + ***1*** + ***k*** = 448 (mode 512). At the end, the length of the initial message is attached as a 64-bit unsigned number.

Dividing the message: The initial message with the completed bits above is divided into 512-bit blocks, which are delivered to the unit's output. For brevity, the unit receives the initial message in 32-bit packets and the initial message has a length ***l***, multiple of 32.

The message "abcd", represented in 8-bit ASCII code, is considered to be processed. The length of the message is ***l*** = 32 bits and it will be completed with 1 bit of 1 followed by ***k*** = 415 bits of 0 (k is obtained from the equation ***l + 1 + k*** = 448 (mode 512)). Then attach the initial length, in bits, of the message, represented as a 64-bit unsigned number.

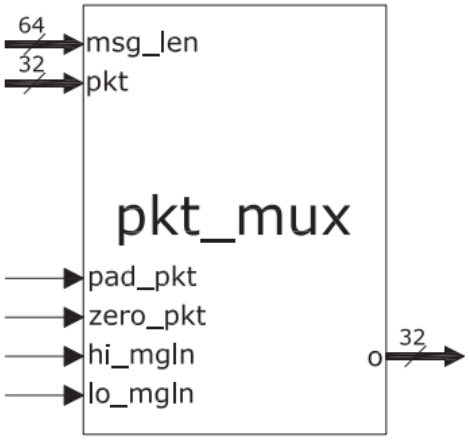
The 512-bit block generated by the input module for this example is detailed below (fields are represented in hexadecimal):



The preprocessing unit operates with 5 types of packages:

- ***message***: packets in which the initial message is divided and which are delivered at the entrance of the unit, one or more such packets may be received
- ***padding***: a packet with the most significant bit of 1 and 31 bits of 0, groups the first 32 bits attached in the completion phase, a single packet of this type is generated
- ***zero***: 32-bit packet of 0, group bits successively, attached in the completion phase. One or more such packets can be generated
- ***the superior half of the message***: a packet containing the most significant 32 bits of the initial length of the message. A single packet of this type is generated
- ***the inferior half of the message***: a packet containing the least significant 32 bits of the initial length of the message. A single packet of this type is generated.

The preprocessing unit will divide the entire binary sequence (initial message + completion bits + length of the initial message) into 512-bit blocks. In each clock cycle, the input processing unit receives a new packet from the initial message and after receiving 16 consecutive packets a new 512-bit block will be delivered to the output.



A dedicated ***pkt_mux*** multiplexer provides the data packets at its output. Its data entries are ***pkt***, for message packets and ***msg_len***, for the length of the original message. Output ***o*** is controlled by the following selection lines:

- ***pad_pkt*** – provides a padding package
- ***zero_pkt*** – provides a zero package
- ***hi_msgln*** – provides the most significant half of the message length (received at msg_len entry)
- ***lo_msgln*** – provides the least significant half of the message length

Two or more selection entries cannot be active at the same time. If none of the 4 selection inputs is active, the current message packet received at the ***pkt*** input is provided at the output.

2) Laboratory Task

Design, using Verilog language, the data path of the input preprocessing unit of a cryptographic application as illustrated below. The processing unit will divide the entire binary sequence (initial message + completion bits + length of the initial message) into ***512-bit blocks***. At each clock cycle, the input processing unit receives a new packet from the initial message and after receiving ***16 consecutive packets*** a new ***512-bit block*** will be delivered to the output.