

Implementation Secure Hash Standard with AVR Microcontroller

The programmability of the AVR family of microcontroller makes possible the implementation of different data processing algorithm on the same device. We implements SHA-1 on AVR microcontroller. The Delay for SHA-1 Computation is 4.2 milisecond with AT90S8515 and 8MHz XTAL. The Delay is in 1 block SHA-1 Computation with 512 bits messages.

The Secure Hash Algorithm (SHA-1) may be used with the Digital Signature Algorithm (DSA) in electronic mail, electronic funds transfer, software distribution, data storage, and other applications that require data integrity assurance and data origin authentication. The SHA-1 may also be used whenever it is necessary to generate a condensed version of a message.

When a message of any length < 264 bits (for SHA-1 and SHA-256) or < 2128 bits (for SHA-384 and SHA-512) is input to an algorithm, the result is an output called a message digest. The message digests range in length from 160 to 512 bits, depending on algorithm.

A hash function compresses the bits of a message to a fixed-size value in a way that distributes the possible message evenly among the possible hash value. A cryptographic hash function does this in a way that makes it extremely difficult to come up with a message that would hash to a previously computed hash value.

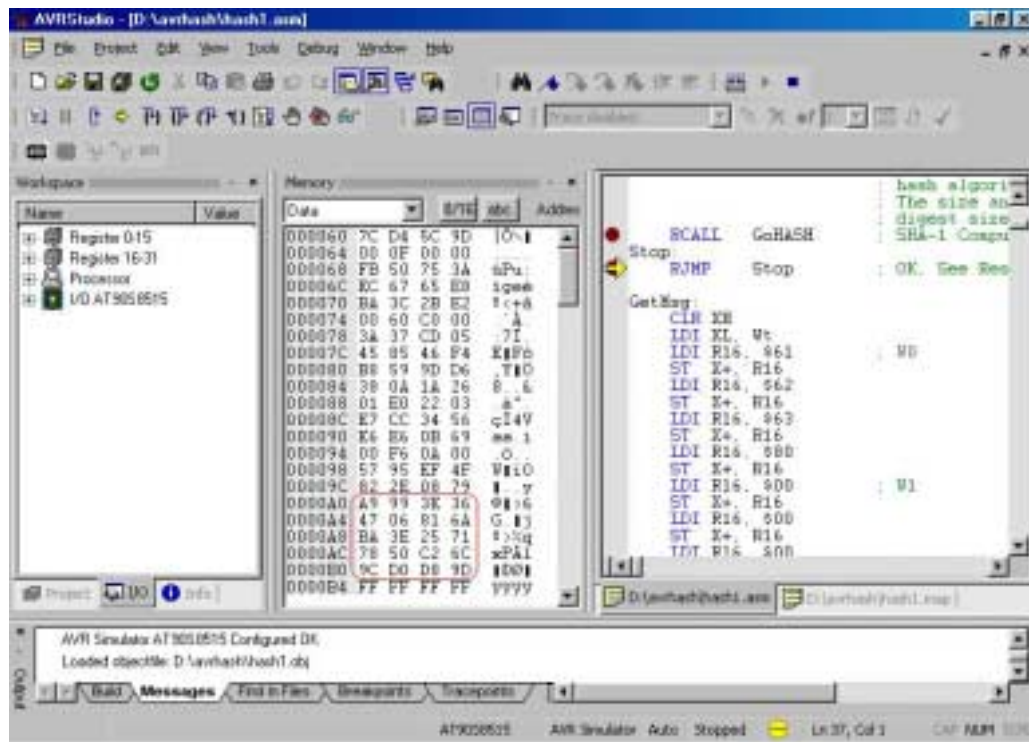


Fig 1, AVR SHA-1 Simulation Result

This is the code sample for SHA-1 Computation

Start:

```
LDI    R16, low(RAMEND)
OUT    SPL, R16
LDI    R16, high(RAMEND)
OUT    SPH, R16
```

```
RCALL  GetMsg      ; Init the message schedule
RCALL  GetInitHash ; Before hash computation begins for each of
                  ; the secure hash algorithm, the initial hash
                  ; value, H must be set
                  ; The size and number of words in H depends on
                  ; the message digest size.
RCALL  GoHASH      ; SHA-1 Computation
```

Stop:

```
RJMP   Stop       ; OK, See Result
```