6213133

From the Hash function shown in figure 1, the size of input is 1 block (9 bits in length). The input (1 block) will be separated into 3 words which have 3 bits per 1 word. Assume that the rule of word expansion is that

The 4th word will be $W_3 = (W_0$ *ex-or* **RotShift** $_{2\text{-}2}(W_1)$ *ex-or* $W_2)$

where

RotShift $_{x\text{-}y}(W_i)$ is the x-bit Right Rotatation of W_i and then follow by Ex-or with the y-bit Left Shift of W_i

Find the output (Message Digest) of the Hash function when the input is "**001 111 101**"

000

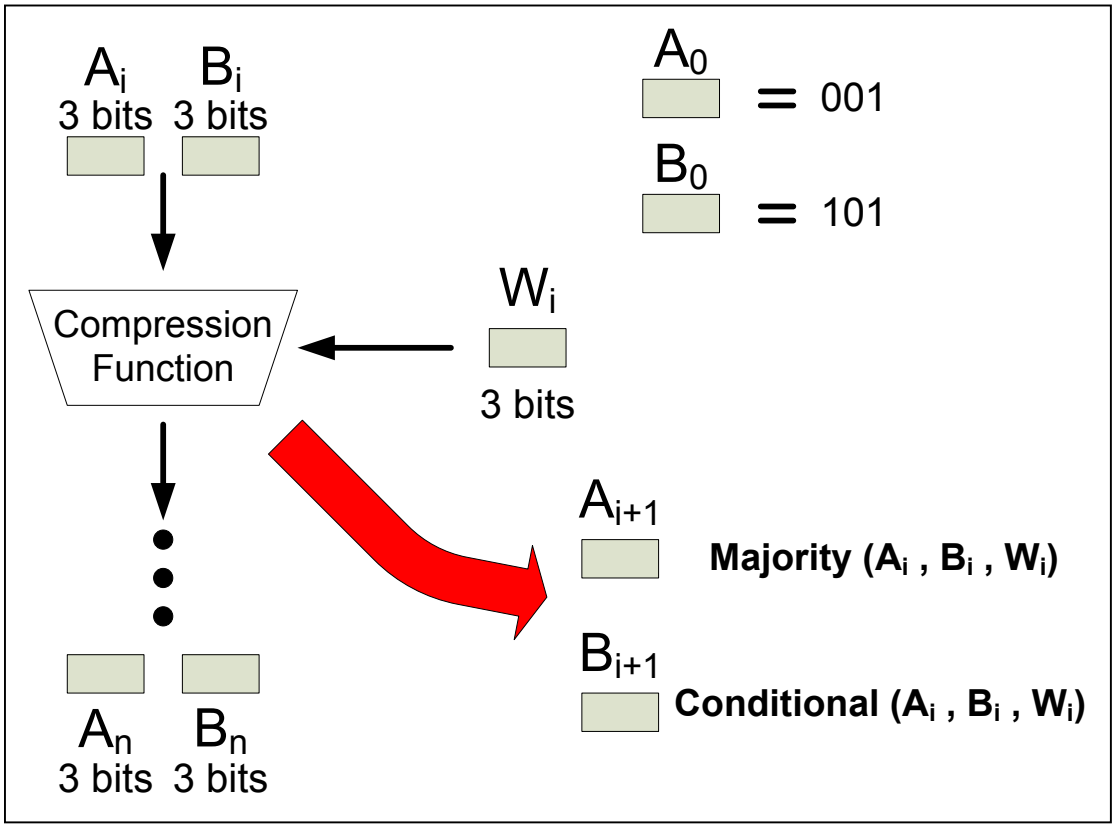

Figure 1 Hash Function

$A_0 = 001$, $B_0 = 101$, $W_0 = 001$

$A_1 = 001$, $B_1 = 001$, $W_1 = 111$

$A_2 = 001$, $B_2 = 111$, $W_2 = 101$

$W_3 = 001 \oplus \text{leftshift}_2(111) \oplus 101$

$= 001 \oplus (100) \oplus (101)$

$= 000$

$\text{Rot}_2(111)$
$= 111$
$\text{shift}_2(111)$
$= 100$

$A_3 = 101$, $B_3 = 001$, $W_3 = 000$ ✗

$A_4 = 001$, $B_4 = 000$

$\therefore$ Input $= 001 \quad 111 \quad 101$

output $= 001\ 000$ ✗