$T(i)$: $\mathbb{R} \to \mathbb{Z}$

return $(\lfloor 0\text{x}100000000 \cdot \mid sin(i) \mid \rfloor)$

$F(i, x, y, z)$: $\mathbb{Z}, \mathbb{Z}, \mathbb{Z}, \mathbb{Z} \to \mathbb{Z}$

if $i < 16$ **then**

return $((x \wedge y) \vee (\neg x \wedge z))$

else if $i < 32$ **then**

return $((x \wedge z) \vee (y \wedge \neg z))$

else if $i < 48$ **then**

return $(x \oplus y \oplus z)$

else if $i < 64$ **then**

return $(y \oplus (x \vee \neg z))$

end if

"Circular shift of a number"

$rol(val, s)$: $\mathbb{Z}, \mathbb{Z} \to \mathbb{Z}$

$r \in \mathbb{Z}$

$r^{[0]} \leftarrow val$

$r^{[\mathbf{i}]} \leftarrow (r^{[\mathbf{i}-1]} \ll 1) + ((r^{[\mathbf{i}-1]} \wedge 0\text{x}80000000) \gg 31)$

return $(r^{[s]})$

$P(a, b, c, d, k, s, i, W, X)$: $\mathbb{Z}, \mathbb{Z}, \mathbb{Z}, \mathbb{Z}, \mathbb{Z}, \mathbb{Z}, \mathbb{Z}, ([0, 4] \Rightarrow \mathbb{Z}), ([0, 4] \times [0, 16] \Rightarrow \mathbb{Z}) \to ([0, 4] \times [0, 16] \times [0, 4] \Rightarrow \mathbb{Z})$

$r \in \mathbb{Z}$

$tmp \leftarrow W_a + X_k + T(i + 1) + F(i, W_b, W_c, W_d)$

$W_a \leftarrow (W_b + rol(tmp, s)) \wedge 0\text{xFFFFFFFF}$

return (W)

"Transform a byte array with 64 elements into a 4 byte array with 16 elements"

$transform(a)$: $([0,64] \Rightarrow \mathbb{Z}) \to ([0,64] \times [0,16] \Rightarrow \mathbb{Z})$

$r \in ([0,16] \Rightarrow \mathbb{Z})$

$r_i \mid \forall i \leftarrow a_{4 \cdot i}$

$r_i \mid \forall i \leftarrow r_i + (a_{4 \cdot i+1} \ll 8)$

$r_i \mid \forall i \leftarrow r_i + (a_{4 \cdot i+2} \ll 16)$

$r_i \mid \forall i \leftarrow r_i + (a_{4 \cdot i+3} \ll 24)$

return (r)

$transform\_back(a)$: $([0,4] \Rightarrow \mathbb{Z}) \to ([0,4] \times [0,16] \Rightarrow \mathbb{Z})$

$r \in ([0,16] \Rightarrow \mathbb{Z})$

$$r_i|\forall i \leftarrow \begin{cases} (a_{\lfloor \frac{i}{4} \rfloor} \wedge \text{0xFF000000}) \gg 24 & i : i \mod 4 = 3 \\ (a_{\lfloor \frac{i}{4} \rfloor} \wedge \text{0x00FF0000}) \gg 16 & i : i \mod 4 = 2 \\ (a_{\lfloor \frac{i}{4} \rfloor} \wedge \text{0x0000FF00}) \gg 8 & i : i \mod 4 = 1 \\ (a_{\lfloor \frac{i}{4} \rfloor} \wedge \text{0x000000FF}) & \textbf{otherwise} \end{cases}$$

return (r)

$process(A)$: $([0,64] \Rightarrow \mathbb{Z}) \to ([0,64] \times [0,16] \Rightarrow \mathbb{Z})$

$W \leftarrow \begin{pmatrix} \text{0x67452301} \\ \text{0xEFCDAB89} \\ \text{0x98BADCFE} \\ \text{0x10325476} \end{pmatrix}$

$Q \leftarrow list(W)$

$X \leftarrow transform(A)$

$W \leftarrow P(0,1,2,3,0,7,0,W,X)$; $W \leftarrow P(3,0,1,2,1,12,1,W,X)$

$W \leftarrow P(2,3,0,1,2,17,2,W,X)$; $W \leftarrow P(1,2,3,0,3,22,3,W,X)$

$W \leftarrow P(0,1,2,3,4,7,4,W,X)$; $W \leftarrow P(3,0,1,2,5,12,5,W,X)$

$W \leftarrow P(2,3,0,1,6,17,6,W,X)$; $W \leftarrow P(1,2,3,0,7,22,7,W,X)$

$W \leftarrow P(0,1,2,3,8,7,8,W,X)$; $W \leftarrow P(3,0,1,2,9,12,9,W,X)$

$W \leftarrow P(2,3,0,1,10,17,10,W,X)$; $W \leftarrow P(1,2,3,0,11,22,11,W,X)$

$W \leftarrow P(0,1,2,3,12,7,12,W,X)$; $W \leftarrow P(3,0,1,2,13,12,13,W,X)$

$W \leftarrow P(2,3,0,1,14,17,14,W,X)$; $W \leftarrow P(1,2,3,0,15,22,15,W,X)$

$W \leftarrow P(0,1,2,3,1,5,16,W,X)$; $W \leftarrow P(3,0,1,2,6,9,17,W,X)$

$W \leftarrow P(2,3,0,1,11,14,18,W,X)$; $W \leftarrow P(1,2,3,0,0,20,19,W,X)$

$W \leftarrow P(0,1,2,3,5,5,20,W,X)$; $W \leftarrow P(3,0,1,2,10,9,21,W,X)$

$W \leftarrow P(2,3,0,1,15,14,22,W,X)$; $W \leftarrow P(1,2,3,0,4,20,23,W,X)$

$W \leftarrow P(0,1,2,3,9,5,24,W,X)$; $W \leftarrow P(3,0,1,2,14,9,25,W,X)$

$W \leftarrow P(2,3,0,1,3,14,26,W,X)$; $W \leftarrow P(1,2,3,0,8,20,27,W,X)$

$W \leftarrow P(0,1,2,3,13,5,28,W,X)$; $W \leftarrow P(3,0,1,2,2,9,29,W,X)$

$W \leftarrow P(2,3,0,1,7,14,30,W,X)$; $W \leftarrow P(1,2,3,0,12,20,31,W,X)$

$W \leftarrow P(0,1,2,3,5,4,32,W,X)$; $W \leftarrow P(3,0,1,2,8,11,33,W,X)$

$W \leftarrow P(2,3,0,1,11,16,34,W,X)$; $W \leftarrow P(1,2,3,0,14,23,35,W,X)$

$W \leftarrow P(0,1,2,3,1,4,36,W,X)$; $W \leftarrow P(3,0,1,2,4,11,37,W,X)$

$W \leftarrow P(2,3,0,1,7,16,38,W,X)$; $W \leftarrow P(1,2,3,0,10,23,39,W,X)$

$W \leftarrow P(0,1,2,3,13,4,40,W,X)$; $W \leftarrow P(3,0,1,2,0,11,41,W,X)$

$W \leftarrow P(2,3,0,1,3,16,42,W,X)$; $W \leftarrow P(1,2,3,0,6,23,43,W,X)$

$W \leftarrow P(0,1,2,3,9,4,44,W,X)$; $W \leftarrow P(3,0,1,2,12,11,45,W,X)$

$W \leftarrow P(2,3,0,1,15,16,46,W,X)$; $W \leftarrow P(1,2,3,0,2,23,47,W,X)$

$W \leftarrow P(0,1,2,3,0,6,48,W,X)$; $W \leftarrow P(3,0,1,2,7,10,49,W,X)$

$W \leftarrow P(2,3,0,1,14,15,50,W,X)$; $W \leftarrow P(1,2,3,0,5,21,51,W,X)$

$W \leftarrow P(0,1,2,3,12,6,52,W,X)$; $W \leftarrow P(3,0,1,2,3,10,53,W,X)$

$W \leftarrow P(2,3,0,1,10,15,54,W,X)$; $W \leftarrow P(1,2,3,0,1,21,55,W,X)$

$W \leftarrow P(0,1,2,3,8,6,56,W,X)$; $W \leftarrow P(3,0,1,2,15,10,57,W,X)$

$W \leftarrow P(2,3,0,1,6,15,58,W,X)$; $W \leftarrow P(1,2,3,0,13,21,59,W,X)$

$W \leftarrow P(0,1,2,3,4,6,60,W,X)$; $W \leftarrow P(3,0,1,2,11,10,61,W,X)$

$W \leftarrow P(2,3,0,1,2,15,62,W,X)$; $W \leftarrow P(1,2,3,0,9,21,63,W,X)$

$W \leftarrow W + Q$

return $(transform\_back(W))$

$divide(w)$: $([0,\ldots] \Rightarrow \mathbb{Z}) \to ([0,\ldots] \times [0,64] \Rightarrow \mathbb{Z})$

$ret \in ([0,64] \Rightarrow \mathbb{Z})$

$$ret_i|\forall i \leftarrow \begin{cases} w_i & i : i < len(w) \\ 0\text{x}80 & i : i = len(w) \\ 8 \cdot len(w) & i : i = 56 \\ 0 & \textbf{otherwise} \end{cases}$$

return (ret)

$\mu(\ )$: $\to ([0,16] \Rightarrow \mathbb{Z})$

"An input string stored as a vector, where symbols are ASCII numbers"

$$w \leftarrow \begin{pmatrix} 97 \\ 98 \\ 99 \\ 100 \\ 101 \\ 101 \\ 100 \\ 99 \\ 98 \\ 97 \end{pmatrix}$$

$a \leftarrow divide(w)$

return $(process(a))$