```
$length(a)$: $\mathbb{Z} \to \mathbb{Z}_8^1$
    $r \in \mathbb{Z}_8^1$
    $r_i \mid i : 0 \leq i \leq 7 \leftarrow 0$
    $n \leftarrow 256^{\lfloor \log_{256}(a) \rfloor}$
    $n^{[0]} \leftarrow n$
    $r_i^{[i]} \leftarrow \frac{a}{n^{[i]}}$
    $n^{[i]} \leftarrow \frac{n^{[i-1]}}{256}$
    return $(\textbf{filter}(r^{[i]} \mid i : i = shape(a)_0))$
```

```
$divide(w)$: $\mathbb{Z}^1 \to \mathbb{Z}_{64}^1$
    $l \leftarrow length(shape(w)_0)$
    $a_i \, | i : 0 \leq i \leq 63 \ \leftarrow \begin{cases} w_i & i : i \leq shape(w) \\ \text{0x80} & i : i = shape(w) \\ l_{i-56} & i : i \geq 56 \\ 0 & \textbf{otherwise} \end{cases}$
    return $(a)$
```

```
$T(i)$: $\mathbb{Z} \to \mathbb{Z}$
    return $(\lfloor \text{0x100000000} \cdot |\sin i| \rfloor)$
```

```
$F(i, x, y, z)$: $\mathbb{B}, \mathbb{B}, \mathbb{B}, \mathbb{B} \to \mathbb{Z}$
    if $i < 16$ then
        return $((x \land y) \lor (\neg x \land z))$
    else if $i < 32$ then
        return $((x \land z) \lor (y \land \neg z))$
    else if $i < 48$ then
        return $(x \oplus y \oplus z)$
    else if $i < 64$ then
        return $(y \oplus (x \lor \neg z))$
    end if
```

```
$P(a, b, c, d, k, s, i, W, X)$: $\mathbb{Z}, \mathbb{Z}, \mathbb{Z}, \mathbb{Z}, \mathbb{Z}, \mathbb{Z}, \mathbb{Z}, \mathbb{Z}_4^1, \mathbb{Z}_{16}^1 \to \mathbb{Z}_4^1$
    $W_a \leftarrow W_b + W_a + X_k + T(i+1) + F(i, b, c, d) \lll s$
    **return** $(W)$
```

```
$transform(a)$: $\mathbb{Z}_{64}^1 \to \mathbb{Z}_{16}^1$
    $r \in \mathbb{Z}_{16}^1$
    $r_i \mid \forall i \leftarrow a_{4 \cdot i} \lll 24$
    $r_i \mid \forall i \leftarrow r_i + a_{4 \cdot i+1} \lll 16$
    $r_i \mid \forall i \leftarrow r_i + a_{4 \cdot i+2} \lll 8$
    $r_i \mid \forall i \leftarrow r_i + a_{4 \cdot i+3}$
    **return** $(r)$
```

```
$transform\_back(a)$: $\mathbb{Z}_4^1 \to \mathbb{Z}_{16}^1$
    $r \in \mathbb{Z}_{16}^1$
    $r_i \mid i : 0 \leq i \leq 15 \leftarrow \frac{a_{\frac{i}{4}}}{2^{8 \cdot (3 - \frac{i}{4})}} \mod 2^{8 \cdot (4 - \frac{i}{4})}$
    **return** $(r)$
```

```
$process(A)$: $\mathbb{Z}^1_{64} \to \mathbb{Z}^1_{16}$
    $W \leftarrow \begin{pmatrix} \text{0x01234567} \\ \text{0x89ABCDEF} \\ \text{0xFEDCBA98} \\ \text{0x76543210} \end{pmatrix}$
    $Q \leftarrow transform(A)$
    $W \leftarrow P(0,1,2,3,0,7,0,W,Q)$
       $W \leftarrow P(3,0,1,2,1,12,1,W,Q)$
    $W \leftarrow P(2,3,0,1,2,17,2,W,Q)$,    $W \leftarrow P(1,2,3,0,3,22,3,W,Q)$
    $W \leftarrow P(0,1,2,3,4,7,4,W,Q)$,    $W \leftarrow P(3,0,1,2,5,12,5,W,Q)$
    $W \leftarrow P(2,3,1,0,6,17,6,W,Q)$,    $W \leftarrow P(1,2,3,0,7,22,7,W,Q)$
    $W \leftarrow P(0,1,2,3,8,7,8,W,Q)$,    $W \leftarrow P(3,0,1,2,9,12,9,W,Q)$
    $W \leftarrow P(2,3,0,1,10,17,10,W,Q)$,    $W \leftarrow P(1,2,3,0,11,22,11,W,Q)$
    $W \leftarrow P(0,1,2,3,12,7,12,W,Q)$,    $W \leftarrow P(3,0,1,2,13,12,13,W,Q)$
    $W \leftarrow P(2,3,0,1,14,17,14,W,Q)$,    $W \leftarrow P(1,2,3,0,15,22,15,W,Q)$
    $W \leftarrow P(0,1,2,3,1,5,16,W,Q)$,    $W \leftarrow P(3,0,1,2,6,9,17,W,Q)$
    $W \leftarrow P(2,3,1,0,11,14,18,W,Q)$,    $W \leftarrow P(1,2,3,0,0,20,19,W,Q)$
    $W \leftarrow P(0,1,2,3,5,5,20,W,Q)$,    $W \leftarrow P(3,0,1,2,10,9,21,W,Q)$
    $W \leftarrow P(2,3,1,0,15,14,22,W,Q)$,    $W \leftarrow P(1,2,3,0,4,20,23,W,Q)$
    $W \leftarrow P(0,1,2,3,9,5,24,W,Q)$,    $W \leftarrow P(3,0,1,2,14,9,25,W,Q)$
    $W \leftarrow P(2,3,1,0,3,14,26,W,Q)$,    $W \leftarrow P(1,2,3,0,8,20,27,W,Q)$
    $W \leftarrow P(0,1,2,3,13,5,28,W,Q)$,    $W \leftarrow P(3,0,1,2,2,9,29,W,Q)$
    $W \leftarrow P(2,3,1,0,7,14,30,W,Q)$,    $W \leftarrow P(1,2,3,0,12,20,31,W,Q)$
    $W \leftarrow P(0,1,2,3,5,4,32,W,Q)$,    $W \leftarrow P(3,0,1,2,8,11,33,W,Q)$
    $W \leftarrow P(2,3,0,1,11,16,34,W,Q)$,    $W \leftarrow P(1,2,3,0,14,23,35,W,Q)$
    $W \leftarrow P(0,1,2,3,1,4,36,W,Q)$,    $W \leftarrow P(3,0,1,2,4,11,37,W,Q)$
    $W \leftarrow P(2,3,0,1,7,16,38,W,Q)$,    $W \leftarrow P(1,2,3,0,10,23,39,W,Q)$
    $W \leftarrow P(0,1,2,3,13,4,40,W,Q)$,    $W \leftarrow P(3,0,1,2,0,11,41,W,Q)$
    $W \leftarrow P(2,3,1,0,3,16,42,W,Q)$,    $W \leftarrow P(1,2,3,0,6,23,43,W,Q)$
    $W \leftarrow P(0,1,2,3,9,4,44,W,Q)$,    $W \leftarrow P(3,0,1,2,12,11,45,W,Q)$
    $W \leftarrow P(2,3,1,0,15,16,46,W,Q)$,    $W \leftarrow P(1,2,3,0,2,23,47,W,Q)$
    $W \leftarrow P(0,1,2,3,0,6,48,W,Q)$,    $W \leftarrow P(3,0,1,2,7,10,49,W,Q)$
    $W \leftarrow P(2,3,1,0,14,15,50,W,Q)$,    $W \leftarrow P(1,2,3,0,5,21,51,W,Q)$
    $W \leftarrow P(0,1,2,3,12,6,52,W,Q)$,    $W \leftarrow P(3,0,1,2,3,10,53,W,Q)$
    $W \leftarrow P(2,3,1,0,10,15,54,W,Q)$,    $W \leftarrow P(1,2,3,0,1,21,55,W,Q)$
    $W \leftarrow P(0,1,2,3,8,6,56,W,Q)$,    $W \leftarrow P(3,0,1,2,15,10,57,W,Q)$
    $W \leftarrow P(2,3,1,0,6,15,58,W,Q)$,    $W \leftarrow P(1,2,3,0,13,21,59,W,Q)$
    $W \leftarrow P(0,1,2,3,4,6,60,W,Q)$,    $W \leftarrow P(3,0,1,2,11,10,61,W,Q)$
    $W \leftarrow P(2,3,1,0,2,15,62,W,Q)$,    $W \leftarrow P(1,2,3,0,9,21,63,W,Q)$
    $W \leftarrow W + Q$
    return $(transform\_back(W))$
```

```
$main(\ ){:}\ \rightarrow \mathbb{Z}$
    $w \in \mathbb{Z}^1$
    $w \leftarrow \begin{pmatrix} 68 \\ 61 \\ 62 \\ 72 \\ 61 \\ 68 \\ 62 \\ 72 \end{pmatrix}$
    $a \leftarrow divide(w)$
    **return** $(0)$
```