

BigNumMul

Multiply two 128 bit, unsigned numbers a, b

Input

a is passed through 2 registers **RDI** and **RSI**. The **RDI** contains the lower 64bits, the **RSI** contains the upper 64bits.

b is passed through 2 registers **RDX** and **RCX**. The **RDX** contains the lower 64bits, the **RCX** contains the upper 64bits.

On the other hand,

a = (**RDI**) | (**RSI**<<64)

b = (**RDX**) | (**RCX**<<64)

Output

The result, modulo (2^{128}), should be splited into 2 registers **RAX** and **RDX**, where **RAX** contains the lower 64bits of the answer, **RDX** contains the upper 64bits of the answer.