a1 b1 c1 d1a2 b2 c2 d2

a3 b3 c3 d3

a4 b4 c4 d4

a1 \* a2 = a1,2 (acтарші 64 + aмолодші 64) mod 264 a1,2 \* a3 = a1,2,3 (acтарші 64 + aмолодші 64) mod 264a1,2,3 \* a4 = a1,2,3,4 (acтарші 64 + aмолодші 64) mod 264

a1 \* b2

a1 b1 c1 d1

a2 b2 c2 d2a3 b3 c3 d3 a4 b4 c4 d4

a1 \* a2 \*b2 \*c2 \*d2\*a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4

b1\* a2 \*b2 \*c2 \*d2\*a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4

c1\* a2 \*b2 \*c2 \*d2\*a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4

d1\* a2 \*b2 \*c2 \*d2\*a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4

a1 b1 c1 d1 a2 b2 c2 d2

a3 b3 c3 d3 a4 b4 c4 d4

----------------------------------------------------------

a1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4

b1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4

c1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4

d1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4

a2 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4

b2 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4

c2 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4

d2 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4

-------------------------------------------------------------

a1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4

b1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4

c1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4

d1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4

**Realizyvatu**

a1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4 \* a2

a1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4 \* b2

a1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4 \* c2

a1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4 \* d2

b1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4 \* a2

b1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4 \* b2

b1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4 \* c2

b1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4 \* d2

c1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4\* a2

c1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4\* b2

c1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4\* c2

c1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4\* d2

--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

d1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4\* a2

d1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4\* b2

d1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4\* c2

d1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4\* d2

a1 \* a3 \*b3 \*c3 \*d3 \*a4 \*b4 \*c4 \*d4 \* a2

a1 \* a2 \* a3 \* a4

a1 \* b2 \* b3 \* b4

a1 \* c2 \* c3 \* c4

a1 \* d2 \* d3 \* d4

a1 \* a2 \* b3

a1 \* a2\* c3 a1 \* a2 \* (b3 + c3 + d3)

a1 \* a2\* d3a1 \* a2 \* b4 a1 \* a2 \* (b4 + c4 + d4)

~~a~~~~1 \*~~ ~~a~~~~2\*~~ ~~c~~~~4~~

~~a~~~~1 \*~~ ~~a~~~~2\*~~ ~~d~~~~4~~a1 \* a2 \* a3\* b4 a1 \* a2 \* a3 \* (b4+ c4 + d4~~)~~

~~a~~~~1 \*~~ ~~a~~~~2~~~~\*~~ ~~a~~~~3\*~~ ~~c~~~~4~~

~~a~~~~1 \*~~ ~~a~~~~2~~~~\*~~ ~~a~~~~3\*~~ ~~d~~~~4~~

A1 = a1 b1 c1 d1

A2 = a2 b2 c2 d2

A3 = a3 b3 c3d3

A4 = a4 b4 c4 d4

---

A1 \* A2 =A1,2

A3 \* A4 =A3,4A1,2 \*A3,4 =A1,2,3,4

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| a1\* a2 | a3\* a4 | a1\* a2 \* (a3\*( a4+ b4+ c4+ d4) | a1\* b2 \*( a3\*( a4+ b4+ c4+ d4)) |  |
| a1\* b2 | a3\* b4 | ~~a~~~~1~~~~\* a~~~~2~~ ~~\* a~~~~3~~~~\* b~~~~4~~ | ~~a~~~~1~~~~\* b~~~~2~~ ~~\* a~~~~3~~~~\* b~~~~4~~ |  |
| a1\* c2 | a3\* c4 | ~~a~~~~1~~~~\* a~~~~2~~ ~~\* a~~~~3~~~~\* c~~~~4~~ | ~~a~~~~1~~~~\* b~~~~2~~ ~~\* a~~~~3~~~~\* c~~~~4~~ |  |
| a1\* d2 | a3\* d4 | ~~a~~~~1~~~~\* a~~~~2~~ ~~\* a~~~~3~~~~\* d~~~~4~~ | ~~a~~~~1~~~~\* b~~~~2~~ ~~\* a~~~~3~~~~\* d~~~~4~~ |  |
| b1\* a2 | b3\* a4 | a1\* a2 \* b3\* a4 | a1\* b2 \* b3\* a4 |  |
| b1\* b2 | b3\* b4 | a1\* a2 \* b3\* b4 | a1\* b2 \* b3\* b4 |  |
| b1\* c2 | b3\* c4 | a1\* a2 \* b3\* c4 | a1\* b2 \* b3\* c4 |  |
| b1\* d2 | b3\* d4 | a1\* a2 \* b3\* d4 | a1\* b2 \* b3\* d4 |  |

a1 b1 c1 d1

a2 b2 c2 d2

a3 b3 c3 d3

a4 b4 c4 d4

a1 \* a2