```
In[41]:= p = FromDigits["FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141", 16];

In[52]:= r0 = Mod[2^256 - p, 2^52];

In[55]:= r1 = Mod[Floor[(2^256 - p) / 2^52], 2^52];

In[56]:= r2 = Mod[Floor[(2^256 - p) / 2^104], 2^52];

In[42]:= a = RandomInteger@(p - 1);

In[43]:= b = RandomInteger@(p - 1);

In[44]:= result = Mod[a b, p];

In[45]:= ai[n_] := Mod[Floor@(a / 2^(52 n)), 2^52]

In[46]:= bi[n_] := Mod[Floor@(b / 2^(52 n)), 2^52]

In[47]:= cl[n_] := Mod[Sum[ai[i] bi[n - i], {i, Max[0, n - 4], Min[n, 4]}], 2^52]

In[48]:= cu[n_] := Floor[Sum[ai[i] bi[n - i], {i, Max[0, n - 4], Min[n, 4]}] / 2^52]
```

0

```
In[63]:= res0 = (cl[0] + cu[0] 2^52) + 2^52 (cl[1] + cu[1] 2^52) + 2^104 (cl[2] + cu[2] 2^52) +
           2^156 (cl[3] + cu[3] 2^52) + 2^208 (cl[4] + cu[4] 2^52) + 2^260 (cl[5] + cu[5] 2^52) +
           2^312 (cl[6] + cu[6] 2^52) + 2^364 (cl[7] + cu[7] 2^52) + 2^416 (cl[8] + cu[8] 2^52);

In[65]:= Mod[res0, p] == result
Out[65]= True
```

1

```
In[64]:= res1 = (cl[0] + 16 r0 (cu[4] + cl[5]) + 256 r0 (r1 cu[8] + r2 (cu[7] + cl[8]))) +
           2^52 (cu[0] + cl[1] + 16 r0 (cu[5] + cl[6]) + 16 r1 (cu[4] + cl[5]) + 256 r0 r2 cu[8] + 256 r1 r1 cu[8] +
             256 r1 r2 (cu[7] + cl[8])) + 2^104 (cu[1] + cl[2] + 16 r0 (cu[6] + cl[7]) + 16 r1 (cu[5] + cl[6]) +
             16 r2 (cu[4] + cl[5]) + 256 r1 r2 cu[8] + 256 r2 r1 cu[8] + 256 r2 r2 (cu[7] + cl[8])) +
           2^156 (cu[2] + cl[3] + 16 r0 (cu[7] + cl[8]) + 16 r1 (cu[6] + cl[7]) + 16 r2 (cu[5] + cl[6]) + 256 r2 r2 cu[8]) +
           2^208 (cu[3] + cl[4] + 16 r0 cu[8] + 16 r1 (cu[7] + cl[8]) + 16 r2 (cu[6] + cl[7]));

In[66]:= Mod[res1, p] == result
Out[66]= True
```

2

In[78]:=
```
s01 = r0 r1;
s01l = Mod[s01, 2^52];
s01u = Mod[Floor[s01 / 2^52], 2^52];
```

In[81]:=
```
s02 = r0 r2;
s02l = Mod[s02, 2^52];
s02u = Mod[Floor[s02 / 2^52], 2^52];
```

In[84]:=
```
s11 = r1 r1;
s11l = Mod[s11, 2^52];
s11u = Mod[Floor[s11 / 2^52], 2^52];
```

In[87]:=
```
s12 = r1 r2;
s12l = Mod[s12, 2^52];
s12u = Mod[Floor[s12 / 2^52], 2^52];
```

In[90]:=
```
s22 = r2 r2;
s22l = Mod[s22, 2^52];
s22u = Mod[Floor[s22 / 2^52], 2^52];
```

In[126]:=
```
f0 = r0 cu[8];
f0l = Mod[f0, 2^52];
f0u = Mod[Floor[f0 / 2^52], 2^52];
```

In[105]:=
```
f1 = r1 (cu[7] + cl[8]);
f1l = Mod[f1, 2^52];
f1u = Mod[Floor[f1 / 2^52], 2^52];
```

In[108]:=
```
f2 = r2 (cu[6] + cl[7]);
f2l = Mod[f2, 2^52];
f2u = Mod[Floor[f2 / 2^52], 2^52];
```

In[111]:=
```
f3 = s22u cu[8];
f3l = Mod[f3, 2^52];
f3u = Mod[Floor[f3 / 2^52], 2^52];
```

In[129]:=
```
res2 = (cl[0] + 16 r0 (cu[4] + cl[5]) + 256 s01l cu[8] + 256 s02l (cu[7] + cl[8]) + 256 r0 (f0u + f1u + f2u + 16 f3u)) +
    2^52 (cu[0] + cl[1] + 16 r0 (cu[5] + cl[6]) + 16 r1 (cu[4] + cl[5]) + 256 s02l cu[8] + 256 s11l cu[8] +
        256 s12l (cu[7] + cl[8]) + 256 s01u cu[8] + 256 s02u (cu[7] + cl[8]) + 256 r1 (f0u + f1u + f2u + 16 f3u)) +
    2^104 (cu[1] + cl[2] + 16 r0 (cu[6] + cl[7]) + 16 r1 (cu[5] + cl[6]) + 16 r2 (cu[4] + cl[5]) +
        512 s12l cu[8] + 256 s22l (cu[7] + cl[8]) + 256 s02u cu[8] + 256 s11u cu[8] +
        256 s12u (cu[7] + cl[8]) + 256 r2 (f0u + f1u + f2u + 16 f3u)) +
    2^156 (cu[2] + cl[3] + 16 r0 (cu[7] + cl[8]) + 16 r1 (cu[6] + cl[7]) + 16 r2 (cu[5] + cl[6]) +
        256 s22l cu[8] + 256 s12u cu[8] + 256 s12u cu[8] + 256 s22u (cu[7] + cl[8])) +
    2^208 (cu[3] + cl[4] + 16 (f0l + f1l + f2l + 16 f3l));
```

In[131]:= **Mod[res2, p] == result**

Out[131]= True