

SHA-256 Ronda #1

[illegible]

Diagram illustrating the execution of the SHA-256 algorithm, showing the state of the registers (Σ0, Maj, aux) and the output (new A, new B, new C, new D, new E, new F, new G, new H) after each iteration (0 to 15).

The initial state of the registers is shown in the top row (Iteration 0):

- Σ0: 0 0
- Maj: 1 1
- aux: 2 2

The subsequent iterations (1 to 15) show the state of the registers and the output after each iteration:

- Iteration 1: new A: 3 3
- Iteration 2: new B: 4 4
- Iteration 3: new C: 5 5
- Iteration 4: new D: 6 6
- Iteration 5: new E: 7 7
- Iteration 6: new F: 8 8
- Iteration 7: new G: 9 9
- Iteration 8: new H: 10 a
- Iteration 9: new A: 11 b
- Iteration 10: new B: 12 c
- Iteration 11: new C: 13 d
- Iteration 12: new D: 14 e
- Iteration 13: new E: 15 f
- Iteration 14: new F: 16 g
- Iteration 15: new G: 17 h
- Iteration 16: new H: 18 i

The final state of the registers after 16 iterations is shown in the bottom row (Iteration 16):

- Σ1: 19 19
- Ch: 20 20
- H: 21 21
- K: 22 22
- Σ1: 23 23
- aux: 24 24