

128-bit constant

Padded message (multiple of 512 bits)

Digest

512 bits

Digest

512 bits

Message digest

