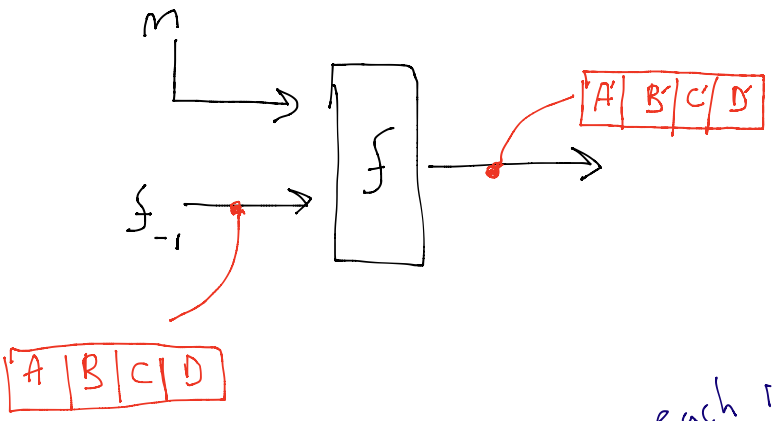
MD4 Compression function

↳ old and insecure → Don't use!



$$t = A + g_i(B, C, D) + M + const.$$

changes each round

changes each time

$$(A', B', C', D') = (D, t \lll const., B, C)$$

Repeat 15 times

Repeat 3 Rounds

bit rotation

changes each time

Each round:

bitwise AND

OR

not

$$g_1 = (B \wedge C) \vee (\neg B \wedge D)$$

$$g_2 = (B \wedge C) \vee (B \wedge D) \vee (C \wedge D)$$

$$g_3 = B \oplus C \oplus D$$

↳ Xor

Sponge (SHA3-256)