## GABRIELE ROMANATO

### MD5 (Message Digest Algorithm 5)

MD5 (Message Digest Algorithm 5) è una funzione di hash crittografica sviluppata da Ronald Rivest nel 1991. È progettata per convertire un input di lunghezza arbitraria in un valore di hash di 128 bit, rappresentato comunemente come una stringa esadecimale di 32 caratteri.

# Come funziona MD5

L'algoritmo MD5 opera suddividendo l'input in blocchi di 512 bit e processandoli attraverso una serie di trasformazioni matematiche. Il processo avviene in diversi passaggi:

- **Padding:** Il messaggio originale viene esteso con un bit 1 seguito da zeri fino a raggiungere una lunghezza congruente a 448 mod 512. A questo viene aggiunta una rappresentazione a 64 bit della lunghezza originaria del messaggio.
- **Inizializzazione:** Vengono definiti quattro registri a 32 bit con valori iniziali fissi.
- **Elaborazione per blocchi:** Il messaggio suddiviso in blocchi da 512 bit viene elaborato in 64 round, ciascuno dei quali utilizza operazioni logiche booleane, rotazioni bit a bit e somme modulari.
- **Produzione dell'hash:** Dopo l'elaborazione di tutti i blocchi, i quattro registri vengono concatenati per ottenere il valore di hash finale.

# Vulnerabilità di MD5

Nonostante la sua popolarità iniziale, MD5 è oggi considerato insicuro per applicazioni crittografiche. Le principali vulnerabilità includono:

- **Collisioni:** È possibile trovare due input diversi che producono lo stesso hash MD5, rendendolo vulnerabile ad attacchi di collisione.

- **Velocità di calcolo:** La rapidità con cui un hash MD5 può essere calcolato lo rende suscettibile agli attacchi di forza bruta e agli attacchi con tabelle arcobaleno.

## Utilizzi attuali

Nonostante le sue debolezze, MD5 è ancora usato in scenari non critici per la sicurezza, come il controllo di integrità dei file e la generazione di checksum.

## Alternative sicure

Per applicazioni che richiedono una sicurezza maggiore, è consigliato l'uso di algoritmi di hashing più robusti come SHA-256 o SHA-3, che offrono una protezione migliore contro attacchi crittografici.