Calcolo del checksum MD5 di un file in C

Il checksum MD5 è un algoritmo di hash comunemente usato per verificare l'integrità dei file e dei dati. In C, calcolare il checksum MD5 di un file implica utilizzare una libreria di crittografia, come la libreria OpenSSL, che offre strumenti per generare hash MD5. Vediamo insieme come possiamo calcolare l'MD5 di un file in C utilizzando OpenSSL.

Per poter seguire questo esempio, assicurati di avere installata la libreria OpenSSL. La maggior parte dei sistemi Unix, come Linux e macOS, la includono già. Su Windows potrebbe essere necessario installarla separatamente.

Di seguito, vedremo come implementare il calcolo dell’MD5 di un file utilizzando le funzioni di OpenSSL.

```
#include <stdio.h>
#include <stdlib.h>
#include <openssl/md5.h>

// Dimensione del buffer di lettura
#define BUFFER_SIZE 1024

void calculate_md5(FILE *file, unsigned char *result)
{
    MD5_CTX md5Context;
    unsigned char buffer[BUFFER_SIZE];
    int bytesRead;

    // Inizializza il contesto MD5
```

```
    MD5_Init(&md5Context);

    // Legge il file a blocchi e aggiorna il contesto
MD5
    while ((bytesRead = fread(buffer, 1, BUFFER_SIZE,
file)) != 0) {
        MD5_Update(&md5Context, buffer, bytesRead);
    }

    // Completa il calcolo MD5 e scrive il risultato
nel buffer
    MD5_Final(result, &md5Context);
}

void print_md5(unsigned char *md5Result) {
    for (int i = 0; i < MD5_DIGEST_LENGTH; i++) {
        printf("%02x", md5Result[i]);
    }
    printf("\n");
}

int main(int argc, char *argv[]) {
    if (argc != 2) {
        fprintf(stderr, "Utilizzo: %s <file>\n",
argv[0]);
        return 1;
    }

    // Apri il file in modalità lettura binaria
    FILE *file = fopen(argv[1], "rb");
    if (!file) {
        perror("Errore apertura file");
        return 1;
    }
```

```
    unsigned char md5Result[MD5_DIGEST_LENGTH];
    calculate_md5(file, md5Result);
    fclose(file);

    printf("Checksum MD5: ");
    print_md5(md5Result);

    return 0;
}
```

Spiegazione del codice:

- **Inclusione delle librerie**: La libreria `<openssl/md5.h>` contiene le dichiarazioni necessarie per utilizzare le funzioni MD5 di OpenSSL.
- **Funzione `calculate_md5`**:
  - Inizializza un contesto MD5 con `MD5_Init`.
  - Legge il file a blocchi (buffer di 1024 byte) e aggiorna il contesto con `MD5_Update`.
  - Quando tutti i dati del file sono stati letti, `MD5_Final` calcola il risultato finale e lo salva nel buffer `result`.
- **Funzione `print_md5`**:
  - Stampa il risultato dell'MD5 in formato esadecimale.
- **Funzione `main`**:
  - Controlla gli argomenti della riga di comando per assicurarsi che l’utente abbia specificato un file.
  - Apre il file in modalità binaria, calcola l'MD5 e stampa il checksum.

Conclusione

L'algoritmo MD5, pur avendo alcune limitazioni di sicurezza, è un metodo veloce e semplice per verificare l'integrità dei file. Questo programma può essere usato per calcolare rapidamente il checksum MD5 di qualsiasi file, rendendo facile verificare l'integrità di dati trasferiti o scaricati. Se hai bisogno di calcolare hash più sicuri, potresti considerare di utilizzare SHA-256 o altre funzioni di hash più moderne e sicure.