Outlook

Re: SE3082 – Assignment Proposal

From Nuwan Kodagoda <nuwan.k@sliit.lk>
Date Wed 05/11/2025 07:27
To OSHAN D A S it23281950 <it23281950@my.sliit.lk>

[EXTERNAL EMAIL] ***This email has been received from an external source – please review before actioning, clicking on links, or opening attachments.***

Approved. Please proceed.

Best Regards

Nuwan

From: OSHAN D A S it23281950 <it23281950@my.sliit.lk>
Date: Tuesday, 4 November 2025 at 5:22 pm
To: Nuwan Kodagoda <nuwan.k@sliit.lk>
Subject: SE3082 – Assignment Proposal

Dear Prof. Nuwan,

I am submitting my algorithm proposal for the SE3082 assignment.

a) Title of the Algorithm - Brute Force Password Cracking using MD5 Hash Comparison

b) Problem Domain - Cryptography and Security.

c) Description - The brute force password cracking algorithm tries every possible password until it finds one that matches a given MD5 hash. It does this by turning numbers into password strings using base-26, where each number represents a different mix of lowercase letters (a–z).

In the serial version, the program first figures out how many passwords it needs to check (26^n for passwords of length n). Then, it creates the MD5 hash of the real password to use for comparison. In the main loop, it goes through all possible passwords one by one, changes each number into a password string, calculates its MD5 hash, and checks if it matches the target hash.

This algorithm is easy to run in parallel because each password check is independent. The total number of passwords can be divided among multiple threads or processes, with each one working on a separate range. Since each thread only needs to check its own passwords and doesn't share data with others, no communication or waiting is needed.

Each part of the work takes about the same amount of time, so the load is evenly spread out. Adding more CPU cores makes the process faster almost in direct proportion. Also, each thread uses very little memory—just enough for its own password string and hash—so it works well on multi-core or distributed systems.

Because of how independent each task is, this problem is perfect for showing how parallel programming improves speed and efficiency, especially in password-cracking or cryptography examples.

d) C code - Please find the attached C file for the source code.

I believe this algorithm shows excellent parallelization potential and would appreciate your approval to proceed with the parallel implementation for the assignment.

Best Regards,

Sithija Oshan,

IT23281950.

Disclaimer : This email and any attachment transmitted herewith are confidential and is intended solely for the use of the individual or entity to which they are addressed and may contain information that is privileged or otherwise protected from disclosure. If you are not the intended recipient, you are hereby notified that disclosing, copying, distributing, or taking any action in reliance on this email and the information it contains is strictly prohibited. If you have received this email in error, please notify the sender immediately by reply email and discard all of its contents by deleting this email and the attachment, if any, from your system.

Disclaimer : This email and any attachment transmitted herewith are confidential and is intended solely for the use of the individual or entity to which they are addressed and may contain information that is privileged or otherwise protected from disclosure. If you are not the intended recipient, you are hereby notified that disclosing, copying, distributing, or taking any action in reliance on this email and the information it contains is strictly prohibited. If you have received this email in error, please notify the sender immediately by reply email and discard all of its contents by deleting this email and the attachment, if any, from your system.

Disclaimer : This email and any attachment transmitted herewith are confidential and is intended solely for the use of the individual or entity to which they are addressed and may contain information that is privileged or otherwise protected from disclosure. If you are not the intended recipient, you are hereby notified that disclosing, copying, distributing, or taking any action in reliance on this email and the information it contains is strictly prohibited. If you have received this email in error, please notify the sender immediately by reply email and discard all of its contents by deleting this email and the attachment, if any, from your system.