Project P2: MD5 Cracker

MD5 (= Message Digest algorithm 5) is an algorithm that computes for a given string (e.g., a file, a part of a file, or a password) a 128-bit hash value.

The purpose of this project is to write a distributed MD5 cracker. Given a MD5 hash value the software should be able to find an (alphanumeric) argument key leading to that value by using a simple brute-force approach. The software should, however, be able to take advantage of multiple, networked computers to distribute the compute load.
The software should be written in Java. You may choose to implement the network comunication using one of Java RMI, TCP sockets or HTTP (using the appropriate Java API).
Minimum requirements are:

- Computer A is given the MD5 hash value and the maximum key length.
- A number of other computers connect to computer A, request part of the work (for example the brute-forcing of all keys starting with the given 2 characters) and push the result back to computer A. The result is the key found or the information that the key was not within the searched space. The comunication should follow a simple text-based protocol (when using sockets or HTTP) or method signatures (when using Java RMI). Designing an appropriate protocol or method signature is an important part of your task.
- As soon as the key is found or after all other computer finish searching without success, computer A outputs the result to the user

Your project submission will be graded by additional features. Recommended features are:

- Computer A is not special: all computers use a leader election scheme to decide which computer will take the master role (distributing the work and collecting the results);

- Robustness: make all parts of the system fail-proof (i.e. deal with network time-outs; make work packages available again if the client does not call back, etc, ...);
- Liar detection: device a scheme to deal with clients that poison the network by accepting work without actually performing the brute-forcing (this way a key might not be discovered);
- your own ideas.

Your project submission must include:

- the source code of the software;
- a short description (in ASCII text format) of the software.

Be prepared to be able to answer questions about the source code (i.e., all group members must know all parts of the code).

Team size

The default team size is two. Single person teams are acceptable. If you feel you absolutely need to be more than two persons in a team, please ask and explain why you want to be a larger team.

Deadline

The deadline for project submission is 8 February, 2010. Please send files via email to `nutt@inf.unibz.it` no later than that date.

Acknowledgment: This project has originally been designed by Chris Mair for the labs in 2008/09.