Parallel Project 1 Part 2 - 8 ascii Password Cracker

Instructions: (Those that are not struck out are for the report)

1. ~~Generate a 1-8 ascii password~~
2. ~~Convert it to hash~~
3. Do hash/password/generation research, list on report
4. What is a hash function? Properties? Can he directly know that the h func is? Or can he retrieve or investigate the hash? How does the attacker eventually obtain the hash so that the attacker can brute-force or even use a rainbow table to try any combination of characters through the hash in order to obtain the same hash value?
5. ~~Convert each permutation into hash and compare it with provided hash.~~
6. When to use Dictionary attack vs. Rainbow Table attck? What are the resource requirements for each type of attack? Which uses more storage? Which requires more pre-computation? Which requires more analysis time? (per-hash vs. batch cracking)
7. ~~Select various and diverse ways of problem decomposition and assignment with the goal to achieve optimal workload utilization.~~
8. ~~Consider a scenario for which thread 1 thecks only combinations of length 1, thread 2 does that for 2 letter words, thread 3 for 3 letter words etc. So, first generate hashes and matching them in bulk via your dedicated hardware.~~
9. What is the ISPC implementation speedup for single CPU core (no tasks launched) and when using multiple cores (with tasks)? What is the speedup due to SIMD parallelization? What is the speedup due to multi-core parallelization? Extend your code to utilize 2, 3, 4, 5, 6, 7, 8 threads, partitioning the computation accordingly. In your write-up, produce a graph of speedup compared to a sequential implementation (which you need to implement as well) as a function

of the number of cores and threads used. Is speedup linear in the number of cores used? In the number of threads used? Please justify why yes or why not.

10. You may also conduct some search on the web and utilize in addition an existing software toolfor password cracking. Does your tool lend itself easily to parallel execution? You are expected to do some research and find one that does.
11. Conduct a similar experiment as the one with your own password cracker. Compare the results and discuss them in your report. Note: Also experiment with a number of different password characters and report thedifference in the timing results. All groups in addition to your own imaginary passwords, also use the following to compareagainst all groups and all varying implementations: bv37qi#f. Apply a number of popular hashesand obtain a number of versions of the password. And you take it from there...