Remember that the quality of the defenses, hence the quality of the of the school on the labor market depends on you. The remote defences during the Covid crisis allows more flexibility so you can progress into your curriculum, but also brings more risks of cheat, injustice, laziness, that will harm everyone's skills development. We do count on your maturity and wisdom during these remote defenses for the benefits of the entire community.

SCALE FOR PROJECT FT_SSL_MD5 (/PROJECTS /42CURSUS-FT_SSL_MD5)

You should evaluate 1 student in this team

★

Git repository

```
git@vogsphere.msk.21-school.ru:vogsphere/intra-uuid-ef3c884d-4a97-40
```

Introduction

In order to maintain high evaluation standards, you are expected to::

Stay polite, courteous, respectful and constructive at every moment of the discussion. Trust between you and our community depends on your behaviour.

Highlight the flaws and issues you uncover in the turned-in work to the evaluated student or team, and take the time to discuss every aspect extensively.

Please take into account that discrepancies regarding the expected work or functionnalities definitions might occur. Keep an open mind towards the opposite party (is he or she right or wrong?), and grade as honestly as possible. 42's pedagogy only makes sense if peer-evaluations are carried out seriously.

Guidelines

You must grade only what exists in the GiT repository of the student or team.

Be careful to check the GiT repository's ownership:: is it the student's or team's repository, and for the right project?

Check thoroughly that no wicked aliases have been used to trick you into grading something other than the genuine repository.

Any script supposed to ease the evaluation provided by one party must be thoroughly checked by the other party in order to avoid unpleasant situations.

If the student in charge of the grading hasn't done the project yet, it is mandatory that he or she reads it before starting the evaluation.

Use the available flags on this scale to tag an empty work, a non functional work, a coding style ("norm") error if applicable, cheating, and so on. If a flag is set, the grade is 0 (or -42 in case of cheating). However, cheating case excluded, you are encouraged to carry on discussing what went wrong, why, and how to

address it, even if the grading itself is over.

Attachments

subject.pdf (https://cdn.intra.42.fr/pdf/pdf/13242/en.subject.pdf)

Mandatory Part

The basics Without mastering them, you are nothing.

Does FT_SSL handle commands correctly?

It doesn't have to match OpenSSL perfectly here, but it must meet a few basic requirements.

Does ft_ssl handle invalid commands correctly? Does it output an appropriate error message?

Does ft_ssl provide a usage if no arguments are provided OR does it read the command from standard input?

Yes No

Did they implement a function dispatcher?

You're going to have to actually look at the code for this one. How do they determine which command should be run?

Do they set up a function pointer array and have a clever way of dispatching their commands? Or a hideous if/else monstrosity?

Award no points for this question if it's only if/else statments.

Award only 4 points if they have to make a change in more than two places in the code every time they add a new command. Reduce a point for each place they must make a change.

(Example:: a NUM_COMMANDS macro in includes, an extra if/else, or adding another line to their setup_commands or equivalent function)

Rate it from 0 (failed) through 5 (excellent)

5

Can they MD5 a file?

Check that the ft_ssl md5 hashing algorithm implementation is 100% correct. Nothing less than perfect will be accepted.

echo 'is md5("salt") a salted hash? :thonking_face:' > /tmp/file
./ft_ssl md5 /tmp/file md5 /tmp/file openssl md5 /tmp/file

The spacing of the output does not matter as long as it matches either openssl or the md5 standalone.

Yes No

Can they do it quietly?

The following command should have no output::

diff <(md5 -q /tmp/file) <(./ft_ssl md5 -q /tmp/file)

☑ Yes ☒ No

REVERSE REVERSE!

Now you have to test that they implemented the -r flag correctly!

md5 -r /tmp/file ./ft_ssl md5 -r /tmp/file

☑ Yes ☒ No

Print it back now, Y'all!

They had better be able to do this. It's just 1 write() call, seriously.

echo "Magic mirror on the wall, think I wanna smash them all?" | md5 -p echo "Speed up now, Gas Pedal??" | ./ft_ssl md5 -p

My mashup skills are nowhere near as good as MD5's.

Rate it from 0 (failed) through 5 (excellent)

5

SHA (Some Hipster Algorithm)

Enough playing around with the suits let's do something fresh and hip, yeah?

echo "Lorem ipsum dolor amet thundercats letterpress cray portland cornhole coloring book twee prism hexagon mixtape pork belly hell of four dollar toast disrupt. Hammock PBR&B bicycle rights selvage street art, lumbersexual gochujang vegan hot chicken. Meggings drinking vinegar biodiesel poke roof party tote bag cloud bread ethical. Glossier flannel 8-bit hexagon selvage adaptogen farm-to-table offal knausgaard pickled." > some_hipster_ipsum shasum -a 256 some_hipster_ipsum > some_hipster_ipsum_sum ./ft_ssl sha256 some_hipster_ipsum > flip_some_hipsum diff some_hipster_ipsum_sum flip_some_hipsum

☑ Yes ☒ No

Nigel Thornberry

You better be SMASHING the Sha Hashing flags like our favorite documentary filmmaker.

You know what flags need to be tested so I'm going to consolidate all the tests into a single slider and save us both (mostly me) some time.

Rate it from 0 (failed) through 5 (excellent)

4

Bonus Part!

Are they a mere hub2JmdXNjYXRlZCBidXR0cwo=man? Or are they a god?

Are they a perfectionist?

Did they set up their executable to read commands from the STDIN and not just args?

☑ Yes ☒ No

Are they prepared to out-hash the Hash Slinging Slasher?

Did they add bonus hash functions? Can they prove they accurately hash identical to their counterpart? Are they considered stronger than MD5?

(If you're unsure what to rate, the SHA family are similar and around 2 points each, while whirlpool is more oouah and 5 points ;)

Rate it from 0 (failed) through 5 (excellent)

5

Are they a Memer? Do they look like someone who memes?

This question has no effect on your grade, we're just starting our own data-mining personality quiz for the Zucc.

☑ Yes ☒ No

Ratings

Don't forget to check the flag corresponding to the defense

✔ Ok ★ Outstanding project

Empty work Incomplete work No author file Invalid compilation Norme Cheat

Crash Forbidden function

Conclusion

Leave a comment on this evaluation

Finish evaluation