(This document will be re-uploaded several times. Version 05/05/2021)

Dear students,
In this document you will find the most frequently (and relevant) asked question about this year FoC project. If you have any question, please **first** thoroughly read this document, **then** email me at michele.lamanna@phd.unipi.it if you still have any doubts.

Sincerely,
Michele La Manna.

Q, Is this project mandatory?

A. Yes, and **PLEASE READ THIS ANSWER UNTIL THE END**. In order to take the written exam, you have to request first a meeting with me, in which you will discuss your work. If your project satisfies the requirements, I will notify Prof. Dini, and then you will be able to take the written exam. Please, if you want to take an exam on a specific date (let's say July 19th), send the email in which you request the meeting **at least** a week before. To be perfectly clear, if you send a meeting request on July 12th you are guaranteed to have a meeting **before** the written exam, but if you send the meeting request on July 13th you are **not guaranteed** to have a meeting before the written exam, so you risk losing the chance of taking the written exam on July 19th.

Q. How many people should participate in the group project?

A. The maximum (and recommended) number of people contributing to a single project is 3 (three). Clearly, two-members groups or singles project are allowed. If you want to develop your project in groups of 4 (four) or more, please contact me via e-mail, and we will discuss extra feature to add to you assignment.

Q. How many meetings can my group request?

A. As many as you want. You are here to learn something, and we are here to teach. However, please keep in mind that you are almost 100 students, so before asking for a meeting, please try your hardest to solve by yourselves the issue you are facing.

Q. What can I request a meeting for?

A. You can request the meeting if you have doubts on some theory concepts, over how OpenSSL works, or simply if you need a confrontation over your design choices for the project. Indeed, it is recommended to request a meeting before you start programming the client/server application. In this way, if you overlooked something inside your design, you can correct it **before** actually implementing it.
I CANNOT DEBUG YOUR CODE. So, please, do not send me emails like "I'm having trouble with this piece of code and my program crashes, what did I do wrong?".

Q. Is the project mandatory for foreign students and applied crypto students?

A. Yes.

Q. Can Students from different curricula participate in the same group?

A. Yes, however in that case secure coding must be implemented also if one group member is from AC.

Q. Are there any specific version of the language, tool chain or OS to use?

A. You must use C++/C, using the OpenSSL library. You can develop your code on any OS you prefer, however Ubuntu is recommended.

Q. What kind of communication medium must use? Sockets, files, ecc.?

A. You have to use sockets. You don't have to solve issues caused by NAT, but the final demo must run on your localhost as if clients and serves run on different machines (no shared resources like files or memory).

Q. do we have to use TCP or UDP? Do we have to implement a challenge response-protocol? Do we have to use AES_CBC or AES_ECB? Do we have to use…

A. Technical implementations are your design choices that must be motivated inside your final report. There is not a single way in which this project can be designed and developed, so choose freely but put some think in it! Refer to the guidelines to check all the requirements.

Q. Can we decide a limit on the amount of characters send from a client in one message?

A. Yes, but it must be higher or equal than 10.000 characters.