CSE350/550: Network Security

Programming assignment no. 4 (due date Thursday, Apr 20, 2023, 11.55 pm)

Listed below, you will find brief description of 3 projects, numbered 0 through 2. In groups of 2, you are required to pick one (see algorithm to pick a project), complete that project and submit a report (with a working system) on or before April 20, 2023. The outcome will be evaluated by me and the TAs.

Algorithm to pick a project: you are required to pick project numbered 0, 1, or 2 as determined by k = A1 + A2 mod 3, where
A1 = last_4_digits_of_entry_no_of_first_student, and
A2 = last_4_digits_of_entry_no_of_second_student.

The submission will consist of three parts:

1. a 2 to 4 page document describing the system you have designed, together with sample outputs from the code you have written,
2. the code as a separate file, and
3. 5 to 8 slides that you will use to present your work.

Project 0 Securely time-stamping a document: This application relates to securely time-stamping a document that one may have prepared some moments ago. The process envisaged is: upload the document to the date/time stamping server (or perhaps some version of the document) and expect to receive the same but with the current date and time stamped onto the document. Thus, there must exist a "GMT date &time-stamping server" which has the correct GMT date and time. It uses that to time-stamp documents (in some standard format) with the current GMT data/time and a digital signature. At any time, it should be possible to establish the fact that the document existed at the date/time stamped, and that the document has not been modified.
Before moving forward, try answer these questions:

1. How and where do you get the correct GMT date and time? And when is the correct GMT date/time obtained?
2. Is the source reliable? Is the GMT date and time obtained in a secure manner?
3. How do you ensure privacy, in that the server does not see/keep the original document?
4. How do you share the document with others in a secure manner with the GMT date/time preserved, and its integrity un-disturbed?
5. How does one ensure that the user (both the owner and anyone verifying the date/time) uses the correct "public-key" of the server stamping/signing the "GMT date/time".

Project 1 Digitally signed degree certificates: This application relates to building a web server that responds with a degree-certificate and grade-card whenever someone requests for it. The request must contain the graduate's name & unique roll-number. The degree-certificate and grade-card (possibly in PDF format) is suitably digitally signed by the university authorities, together with the current (and correct) date & time.

1. How and where do you get the correct GMT date and time? Is the source reliable and the GMT date and time obtained in a secure manner?
2. How do you ensure that only the graduate is able to download it (by providing information beyond the roll no, such as date of birth, home pin code, etc.?

3. Should the graduate decide to share the document with others, how can one trace the origin of the document (could watermarks be useful?)?
4. Do we need to have access to public-keys, and if so how?

Bonus points if you address this issue: How do you get the document to be digitally signed by two persons (say the Registrar and the Director?

Project 3 On-the-go verification of Driver's License: This project has to do with verifying a document such as a "driver's license". (Truly this holds good for any "identity card" or any official document such as a passport or birth certificate.) Typically, and currently, a police officer looks at the physical driver's license card and simply assumes that the license, together with the information it contains, was issued by the "transport authority", and none else. Given that it is not difficult to copy, alter or produce afresh a plastic card, how can one use technology to verify **on the go** a driver license card, when shown to a police officer on the road or elsewhere. (Recall: today cellular based access to Internet-connected servers from smart cell phones is readily available, in almost all parts of India.)
Questions:

1. What is the information to be supplied by the driver to the police officer? And what information is sought and obtained by the police officer from the server in the transport authority?
2. Would you need a central server that has the correct and complete information on all drivers and the licenses issued to them?
3. In what way are digital signatures relevant?
4. Does one need to ensure that information is kept confidential? Or not altered during 2-way communication?
5. Which of these, viz. confidentiality, authentication, integrity and non-repudiation is/are relevant?

Bonus points if you address this issue: Is date and time of communication important? If so how can that be obtained from a well-known server in a secure manner?