SIL765: Network & System Security

Programming assignment no. 3 (due date Monday, March 18, 2019)

Listed below, you will find brief description of 4 projects, numbered 0 through 3. 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 March 18. The outcome will be evaluated by me.

Algorithm to pick a project: you are required to pick project numbered 0, 1, 2, or 3 as determined by k = A1+A2 mod 4, 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: This application relates to time-stamping a document that one may have prepared some moments ago. The process envisaged is: upload the document to server (or some version thereof) 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 document (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.
Further:

1. How and where do you get the correct GMT date and time? And how often?
2. Is the source reliable and 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 date/time preserved, and integrity un-disturbed?
5. Also ensure that the user has (and uses) the correct "public-key" of the "GMT date/time stamping server".

Project 1: 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 unique entry-number. The degree-certificate (possibly in PDF format) is suitably digitally signed by the university authorities, together with the current (and correct) 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 get the document to be signed by more than one individual (say two persons)?
3. How do you ensure that only the graduate is able to download it (by providing information beyond the entry_no, such as date of birth, home pin code, etc.?
4. Should the graduate decide to share the document with others, how can one trace the origin of the document (could watermarks be useful?)?
5. Do we need to have access to public-keys, and if so how?

Project 2: The origin of this lies in UID project of GoI, where a central server can be accessed to determine whether some information on an individual is correct or not, but without divulging the information itself. For instance, the database will help determine whether BNJ's DoB is xxx or not, but without the database server itself volunteering such information. How can we do this in a secure and trusted manner.

1. One question that arises is: how does one ensure that information is not altered during the 2-way communication between the client and server?
2. How could one be sure that the reply from UID server "Yes" or "No" is related to the question being asked?
3. In what way are digital signatures relevant?
4. Would access to "public-key certificate" issued by a certification authority be an issue?

Project 3: 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". Given that it is not so difficult to copy, alter or produce afresh a plastic card, how can one use technology to verify on the go the veracity of 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, 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 from 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. Is date and time of communication important?
4. In what way are digital signatures relevant?
5. How does one ensure that information is not altered during the 2-way communication?
6. Which of these, viz. confidentiality, authentication, integrity and non-repudiation relevant?