İSTANBUL SABAHATTIN ZAİM ÜNİVERSİTESİ

BIM 437 - Bilgisayar ve Ağ Güvenliği

TERM PROJECT

Dr. ARTRIM KJAMILJI

Although Socket Programmin in C# is adviced, yet you can use any programming language for your term project. The term project should contain GUI.

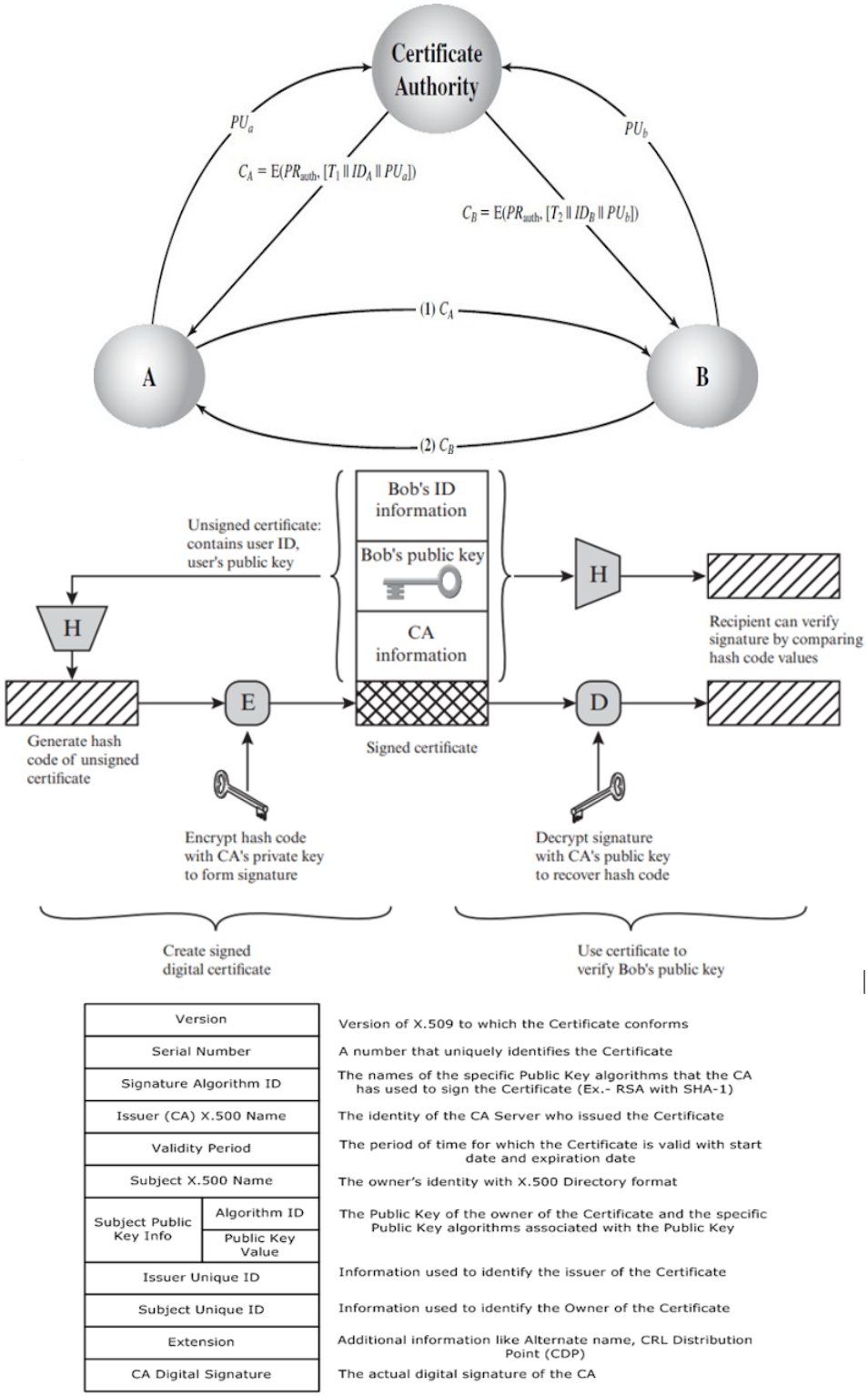
In your term project you should write the codes for 3 entities, which are as follows:

1. **Ceritificate Authority (CA):** It provides digital certificates to clients for their public keys
2. **Client 1:** Takes a public certificate from CA for its public key and sends it to Client 2. Afterwards with Client 2 they derive a master symmetric key using the public keys. Finally, using the master symmetric key they derive a secret key together.
3. **Client 2:** Takes a public certificate from CA for its public key and sends it to Client 1. Afterwards with Client 2 they derive a master symmetric key using the public keys. Finally, using the master symmetric key they derive a secret key together.

This means that when presenting the term project you should use 3 laptops, one for each entity.

The details (protocols) for the steps are illustrated below:

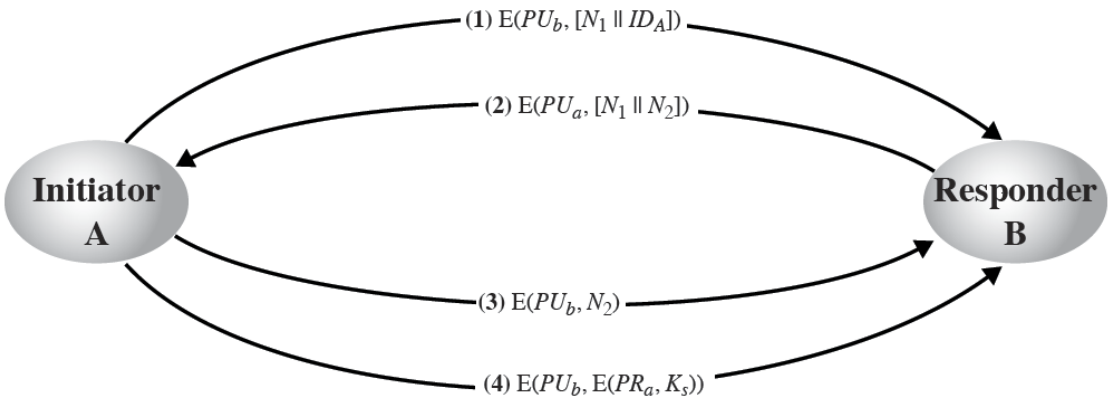
1. Obtaining the public key certificate using oversimplified X.509 certificates from CA and exchanging the public key certificates between Client 1&2



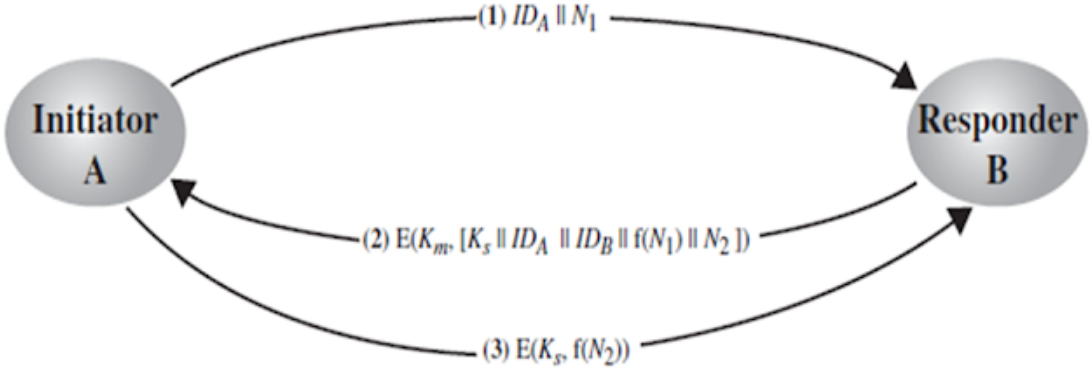
Version		Version of X.509 to which the Certificate conforms
Serial Number		A number that uniquely identifies the Certificate
Signature Algorithm ID		The names of the specific Public Key algorithms that the CA has used to sign the Certificate (Ex.- RSA with SHA-1)
Issuer (CA) X.500 Name		The identity of the CA Server who issued the Certificate
Validity Period		The period of time for which the Certificate is valid with start date and expiration date
Subject X.500 Name		The owner's identity with X.500 Directory format
Subject Public Key Info	Algorithm ID	The Public Key of the owner of the Certificate and the specific Public Key algorithms associated with the Public Key
	Public Key Value	
Issuer Unique ID		Information used to identify the issuer of the Certificate
Subject Unique ID		Information used to identify the Owner of the Certificate
Extension		Additional information like Alternate name, CRL Distribution Point (CDP)
CA Digital Signature		The actual digital signature of the CA

Here from the X.509 certificates only the most important fields should be used, such as Subject ID, Subject Public Key Info (Algorithm ID, Public Key Value), Validity Period, Serial Number and CA Digital Signature. You can add other fields if you want.

2. Obtaining the symmetric master key Ks using the public keys



3. Obtaining a symmetric session key Ks using the symmetric master key Km



You should decide on and generate all the other details such as, which is the public key cryptosystem that the CA uses (RSA, el-Gamal, etc.) and its public and secret key, which is the public key cryptosystems that the clients will use and their corresponding public and secret key, as well as **other details**.

Notes:

1. You can work in group with 1-4 students and all should upload the same term project (codes) to LMS (OYS).
2. The term projects should be presented in front of the class during the last week of the semester.
3. The term project is mandatory and it weights at least 10% of your course grade.
4. You can use generative AI to write the project, but should understand all the code when presenting.

Good luck!