Ceng471 HW2 Report

Ali Görkem Yalçın

December 28, 2019

Introduction to used classes

The classes in the solution includes:

User -> which has name, domainParameters, privateKey, publicKey which is calculated from the privateKey($g^{privateKey} modp$) and a secretKey which is a random BigInteger between 0 and p-1.

CertificationAuthority -> which has name, domainParameters, privateKey and the publicKey which is calculated in the same way as the User's.

The other 3 classes except the App class are wrapper classes for values.

App class includes the main scenario.

Main scenario

After creating the players of the scenario, each user will create their own secret key to be used for creating a shared secret between each other.

Creating a secretValue is done by $g^{secretKey}(modp)$

Then CA creates the certificates for the users by signing the content of the file.
I took the whole file contents as a string and signed it by:
$s1 = g^k modp$ where k is a random number
$s2 = (H(m) - privateKey * s1) * k{-}1(modp - 1)$

The signature is (s1,s2)

Then the users verify each other's certificate using the publicKey of the CA. First user checks if the data in the certificate is correct, if so by validating the signature by calculating the:

$v1 = g^H(m) modp$
$v2 = (publicKey^{s1}) * s1^{s2} modp$
if v1=v2 then the signature holds.

Then the users create a shared key by $g^{ab} modp$ where a is the Alice's private value, b is Bob's private value.

Then Alice signs a message in the same way CA signed the certificate

Then Alice encrytps the signed message using the secret value between her and Bob as a key in AES encryption system.

Then Bob decrypts the message using the same shared secret between him and Alice.

Then Bob validates the signature in the message by using Alice's public key.

If the signature holds message is valid.

Additional Information

By increasing the values in domainParameters in the App class we can have a more secure cryptosystem. DomainParameter variable supports multi precision numbers, we can achieve it by changing the values in the parameter.