Cairo University
Faculty of Engineering

Computer Engineering Department

Cryptography and Network Security- CMP 404**
Spring 2019

Security Project 3: Key Management through Certificates

Project Objectives:

1. Apply security concepts you study in the course to a real world problem.
2. Enhance student's understanding of different encryption algorithms.
3. Enhance student's understanding of Key management and distribution و and public key certificates.
4. Implement one of the digital signature algorithms (ElGamal).

Project Requirement:

You are required to develop an application that simulates key management and distribution.

The Detailed Steps of the application are as follows:

Suppose Alice wants to send a secure and signed message to Bob. She will encrypt the message using asymmetric encryption algorithm (public key) for confidentiality and with her private key for signature. Accordingly, Alice should do the following steps:

1. Assign Ids for Alice and Bob, generate private/public key pairs for the certificate authority.
2. Initially generate some X509 certificates for random public keys, for random ids and store them in a suitable format (a file or a database).
3. Sign the encrypted message using Alice private key using El-Gamal Signature Algorithm, **implement El-Gamal digital signature by yourself.**
4. Get public key of Bob by contacting certificate authority (searching the database/the file of certificates) and getting Bob's certificate, verify certificate by decrypting it with authority public key.
5. Encrypt the message to be sent using Bob's public key using RSA algorithm.
6. Send the signed encrypted message to Bob.

On the receiver side, Bob should do the following steps upon receiving an-email from Alice:

1. Decrypt the ciphertext resulting from step (2) using Bob's private key.
2. Verify that the message is from Alice by contacting certificate authority and check Alice public key.
3. Verify the received signed ciphertext using Alice retrieved public key from certificate.

Important Notes

- **Copied projects from each other/from the internet will get zero!**
- **The sender and receiver should be two separate modules (2 programs), communication can be done using files, or network (socket programming).**
- You can use a cryptography library, but you should implement ElGamal algorithm by yourself.
- You should work in group of size 2 students.

Deliverables:

- You should deliver all your code and a detailed report about your project, how you implemented it and the analysis results and your conclusions.

Project Due Date:

Tuesday, April 30th, 2019.