Cryptography and Network Security I
Spring 2024
Project Description

This is a group (2-3 students) project and you are free to choose your team mates.

You (as a group) will be implementing your own version of SSH/SSL protocol which supports your own implementation of the ciphers including the symmetric key ones (e.g., DES), PKC under ciphertext only adversary, semantically secure PKC, and homomorphic cipher as we discussed in the class and you implemented in home works. For digital signature schemes use one based on PKC, for MAC use HMAC, for hash functions use SHA1.

The project will be implemented as a client-server protocol to mimic transactions/ebanking between an ATM (client) and the bank (server). Your project will enable banking operations to deposit, withdraw money, and check balance via ATM by accessing the bank.

You are allowed to use sockets programming libraries. Each team will play white hat and black hat roles as described below:

TIME LINE & Grading:
White-hat part [60 points] due 11:59pm, April 14, 2024: The goal is to
(i) [20pnts] negotiate and establish a secure channel using the SSL/SSH handshake protocol.
(ii) [20pnts] pass back and forth messages to implement the banking operations above.
(iii) [20pnts] You will write a document explaining your implementation as a part of *your communication intensive requirement* and pass the code to the TA.

We will assign your code a Black-hat team to analyze and attack. If your code does not run than black-hat will get the full points (since they can claim whatever they want) ☺.

Black-hat part [40 points] due 11:59pm, April 19, 2024: you will receive the source code of the target team on April 15, 2024. Your goal is to find weaknesses in the implementation of (i) cryptographic primitives and protocols [20pnts]; [ii] write a report on your attacks as a *part of your communication intensive requirement.*

In class presentation [100 points] April 22, 2024: we will schedule a time slot for each group for presentations and demos.