Computer Security — Fall 2019
CS 4351 — Professor L. Longpré

Assignment 2 addendum

Introduction

The purpose of this assignment is to gain experience in implementing a cryptographic protocol that involves key exchange, digital signatures and encryption.

Crypto client and server files

The files `CryptoMultiEchoServer.java` and `CryptoEchoClient.java` distributed earlier were supposed to read from the file `randomBytes`. However, each of the two programs were missing a read statement. They worked, because they shared the zeroes secret. However, it could be a disaster if this went into real use. I have included the corrected versions in the .zip.

Server running our protocol

We now have a server that runs our protocol. You can test your client program by running it with host `cspl000.utep.edu` instead of localhost.
We also provided the java program `EchoClientSkeleton.java`. This can work as a skeleton for writing your own program. However, it does not perform any public key algorithms. Instead, it sends hard-coded data for encryption and signature of zeroed random bytes. The server shifts to testing mode when receiving random bytes all zeroes from the client. In this case, both client and server can generate the same (unsafe) AES key based on zeroes. The `client2Certificate.txt` is also provided.
Once your client program works using the certificates you generated in Part 2 with our server, typing the message "flag" will cause the server to give you a flag string. Provide this flag string in your report as evidence of your success.