Project Overview

This project designs and implements a secure Diffie-Hellman Key Exchange protocol built to be resistant to man-in-the-middle attacks.

The project is supposed to simulate a data-streaming channel between a client and a server. It established a shared session key using Diffie-Hellman (I have used ECDH as I understand this to be more current and optimal version of the exchange), authenticates using RSA signatures and then encrypts all streaming messages using AES-GCM.

The goal is to model a secure client-server channel that streams real-time JSON event messages (like those from real-time sports API's).