

Grading Scale – Encrypted Sockets

The scoring of this exercise consists of two parts; first - going through the code and making sure that all the requirements are met, and second - running the code and testing.

Item	Details	Score
Creating symmetric key-based encryption	protocol.symmetric_encryption properly coded Implemented on both client and server on sending and receiving	20
Diffie-Helman Key Exchange	Implementing three functions to calculate DF Calculating shared secret on client and server	30
Hashing Function	Implement a 16-bit hash function	20
Signature and MAC generation using hash and private key	Implement the RSA algorithm and find two public and private key pairs Exchange of public keys between the sides Generating a MAC and checking for authenticity on the server and client	30
Tests	Send a few messages and see that it goes well.	-30 If there is a crash
	Change the MAC only on one side and see that there is an error (the check will only be performed assuming that the normal health check is successful)	-10 If no message