ASN4 – CMPT 471

Joshua Campbell

301266191

Part A:

Encryption Scheme – Data is encrypted by:

1. XOR the contents of the data (each character) using the secret key generated in the Diffie-Hellman scheme
2. Increase the numerical value of the contents of a character by (2 \* secret-key)

Decryption Scheme – Data is decrypted by:

1. Subtract (2 \* secret-key) from each received character
2. XOR each of the received characters with the secret key generated in the Diffie-Hellman scheme

Program Files:

* ASN4-a-client.cpp – compile the program using g++ -o asn4-a-client ASN4-a-client.cpp, run using ./asn4-a-client 172.16.1.16 (server’s address)
* ASN4-a-server.cpp – compile the program using g++ -o asn4-a-server ASN4-a-server.cpp, run using ./asn-a-server