# Computer Networking: Security

## (CSE 3752)

## Experiment 7

## Aim:

Implementation of secure key exchange and source authentication process using both symmetric and asymmetric cryptography in computer networking.

## Objectives:

1. An overview on Diffie-Helman algorithm.
2. Execution of Diffie-Helman algorithm for key exchange between a source and destination host.
3. Execution of public key crypto-system for authentication verification of source using digital signature in cryptography process.

## Exercises:

1. Given the following parameters for Diffie-Helman algorithm used by A and B for key exchange.
   - The shared prime q=157 and the primitive root p=5.

   Calculate: (a) The value of $Y_A$ and $Y_B$ transmitted by both A and B.
   (b) The value of secured key (K) shared by both A and B.
2. Given a scenario, where B has received a document from A through internet. Explain, how B confirms that the document has been transmitted by A only (not any adversary) using the concept of digital signature as an use of public key cryptosystem.