1125-VC-801 **Samundra Regmi*** (samundra.regmi@cameron.edu), 2800 W Gore Blvd, Lawton, OK 73505,
and **Parshuram Budhathoki** (pbudhath@cameron.edu), 2800 W. Gore Blvd, Lawton, OK 73505.
Diffie-Hellman key exchange protocol and its software implementation. Preliminary report.

In 1976, Whitefield Diffie and Martin Hellman introduced the first practical method for stablishing a common key between two parties over an unsecured communication channel, which is also known as Diffie-Hellman key exchange protocol. This is one of the widely used protocols in different cryptographic algorithms (ex. DES, AES, HMAC). So, implementation of this protocol is of high interest. In this project we are primarily focused on software implementation of Diffie-Hellman key exchange protocol using Python. We can find many work related to this area in the literature. We will also study these existing implementations and will try to optimize software implementation of this protocol using Python. (Received September 12, 2016)