**Security Algorithm and Protocols Project Proposal**

1. **Principal Investigator**

Deeksha Sudini - [deeksha.sudini1@marist.edu](mailto:saraa1@hawkmail.newpaltz.edu)

**2. Title of Project**

SeMA - A messaging app using AES

**3. Mentoring**

Professor Pablo Rivas, Department of Computer Science, Marist College

Pablo.Rivas@marist.edu

**4. Objective of Project**

The main motto of this project is to secure messages coming from different sources using Advanced Encryption System.

**5. Background/History of the Study**

Before the cryptography came into power or usage, the data sharing and messaging through any source has been not secured and anyone can access the data and one can modify the data. There is no proper protection for the data. Since data plays a vital role it should be secured so that only authorized person can only use it. Now a days cryptography is playing a vital role in securing the data. It provides confidentiality, authentication,data Integrity and non repudiation. These services offered security for the computer systems in extremely efficient and effective manner.

**6. Approach to the Study**

Considering this problem statement of data security, this project is trying to secure messages by using Advanced Encryption Systems . In this approach the sender decides whom he wants to share messages with and encrypts it by using a pattern and sends it over a network and receiver will decrypt the message using a shared key.

**Modules:**

1. **Data Encryption:** Data encryption translates data into another form of data. In this step data is commonly referred as cipher text. If a user wants to use the data he should have authentication to access it. A Secret key is needed to decrypt the data.
2. **Data Decryption:** Data can be decrypted by using a secret key shared among the user so that third party will not be able to access it.

**3) Validation:** Validation is always considered important as it shows how accurate and effective the built model is. Efforts to make the improvisation is promised until the quality is obtained.

**7. References**

https://www.schneier.com/essays/archives/2004/08/cryptanalysis\_of\_md5.html

https://www.tutorialspoint.com/cryptography/advanced\_encryption\_standard.htm

http://www.axantum.com/AxCrypt/etc/seagate128vs256.pdf

http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard

https://www.packetlight.com/innovations/layer-1-encryption-over-dwdm-and-cwdm?gclid=CjwKCAiA5OrTBRBlEiwAXXhT6Cimb34Wl8XOf9KKIDjROIixAngVwRYbSESc5cq\_cBfm4UenjTz8PhoC-zQQAvD\_BwE