Communication is the process of transmitting data across channel. Whenever data is transmitted across a channel, errors are likely to occur. Coding theory is a stream of science that deals with finding efficient ways to encode and decode data, so that any likely errors can be detected and corrected. There are many methods to achieve coding and decoding. One among them is Algebraic Geometric Codes that can be constructed from curves.

Cryptography is the science of security of transmitting messages from a sender to a receiver. The objective is to encrypt message in such a way that an eavesdropper would not be able to read it. A cryptosystem is a set of algorithms for encrypting and decrypting for the purpose of the process of encryption and decryption. Public key cryptosystem such as RSA and DSS are traditionally being preferred for the purpose of secure communication through the channel. However Elliptic Curve cryptosystem have become a viable alternative since they provide greater security and also because of their usage of key of smaller length compared to other existing crypto systems. Elliptic curve cryptography is based on group of points on an elliptic curve over a finite field.

This thesis deals with Algebraic Geometric codes and their relation to Cryptography using elliptic curves. Here Goppa codes are used and the curves used are elliptic curve over a finite field. We are relating Algebraic Geometric code to Cryptography by developing a cryptographic algorithm, which includes the process of encryption and decryption of messages. We are making use of fundamental properties of Elliptic curve cryptography for generating the algorithm and is used here to relate both.

Concept of secret sharing is applied to the algorithm. Secret sharing is a scientific method for dividing key information into several places and
distributes it among the group of participants. Here we are making use of Shamir secret sharing schemes. In this method we are encrypting information using a secret key where as during the process of decryption, secret can be reconstructed by the shares given by the different participants.

Errors are likely to occur during the process of communications. We can decode an Algebraic Geometric code for the process of error detection and correction. Decoding methods can be applied to this Cryptographic algorithm to find whether any errors had occurred during the process of transmission. Various decoding methods are available that, can be applied to the algorithm to find whether errors have occurred in the information we communicated and can correct it.

In this way we are trying to find a relation between Algebraic Geometric codes to Cryptography. Cryptography provides a secure way of sending messages, while Algebraic Geometric code converts the information to be transmitted, to a code. This code can be decoded to detect or correct errors. By combining these two we are imposing security and error correction or detection over our message that are being transmitted.

In this thesis an algorithm is developed and implementation of the method is done by using MATLAB. A comparative study of the algorithm developed is done with existing public key crypto system, Elliptic Curve crypto system, and cryptosystem using Algebraic Geometric code. It is done to prove the efficiency of the system.

Attacks are common to all crypto systems whenever we develop a system. We should take into consideration of all the possible attacks that is prone to it. In this method various possible attacks is considered and a study is made regarding it.