File Transfer System using Elliptic Curve Cryptography

With the advent of the Internet and associated technologies, millions of data in the form of text and images are transferred every day across the network. It is essential to ensure the confidentiality and integrity of the data being transferred.

Security of data can be enhanced by using techniques like cryptography, and steganography on data to be transferred. The cryptographic technique which we have used in our project is Elliptic Curve Cryptography (ECC). Various study on ECC has concluded that the difficulty to solve an Elliptic Curve Discrete Logarithmic Problem is exponentially hard with respect to the key size used. This property makes ECC a very good choice for the encryption/decryption process compared to other cryptographic techniques which are linearly difﬁcult or sub exponentially difﬁcult.

This python-based project comprises only 1 module: User. The user would be required to register themselves to log into the system. After registering, they can log in using their credentials. They can also manage their profile. Through the system, they can send files and view files with total security.

The Hill Cipher algorithm is one of the algorithms used in this project. It is one of the symmetric key algorithms that have several advantages in data encryption as well as decryptions. It has a simple structure and fast computations. The other algorithm used is DCT for images. DCT stands for Discrete Cosine Transform. It is a type of fast-computing Fourier transform which maps real signals to corresponding values in the frequency domain.

In this project, the front end involves Html, CSS and JavaScript and the back end involves Python. The database used is MySQL Database and Django is used for the framework.

**Advantages**

* The system is easy to maintain.
* It is user-friendly.
* The main advantage of elliptic curve cryptography is that it offers higher security with a smaller key size in comparison with other existing schemes.
* It requires less computing power than other first-generation encryption public key algorithms.