Cryptography

* Elliptic Curve Cryptography

Overall Program

* Random Key generation using Elliptic curve cryptography

Requirements for ECC

* Using non-singular elliptic
* Interaction with the keys and files
* Discrete log

This project is a key generation program that creates a private key and public key using elliptic curve cryptography. The key size is unknown but likely to be low. It will be able to print the keys onto a text file for transport. After generation there will an encryption option in the menu which also prints to a text file

Stages

* Research elliptic curves over finite fields
* Start creation of first functions
* Key Generation
* Saving Key pair’s into text files

The program's main menu will have

An option to generate a new key pair

An option to save key pair into a text file

An option to encrypt ascii using a key pair

An option to decrypt ascii using a key pair

First Week

Start the function that generates key pairs

Second Week

Finish the functions that generates key pairs

Third Week

Finish function that saves key pairs into .txt

Start Encrypt ascii using a key pair function

Fourth Week

Finish encrypt ascii using a key pair function

Start decrypt ascii function using a key pair

Fifth Week

Finish decrypt function and do graphic work with

Console graphic work for menu