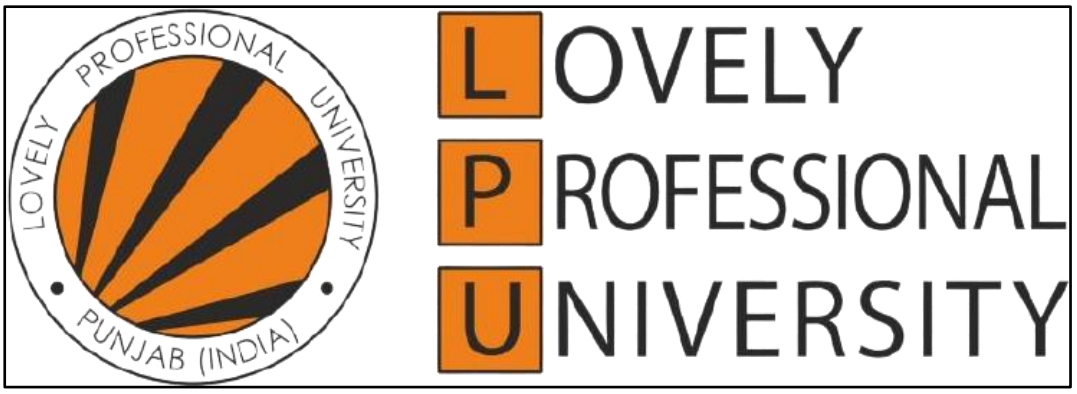
Elliptic Curve Cryptography (ECC) for Secure File Encryption Requirements Specification

Lovely Professional University
Phagwara, Punjab

School of Computer Applications



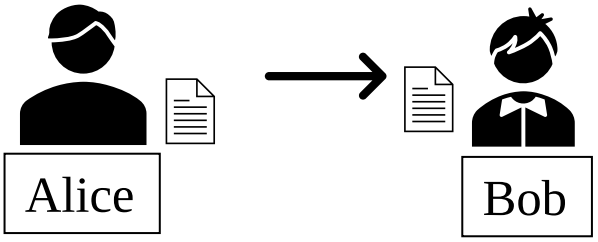
Submitted To: -	**Submitted By: -**
Dr. Sophiya Sheikh (26298)	Name : - Arjun Kumar Section : - DE504 Reg. no : - 11916159 Roll No : - B36

Introduction

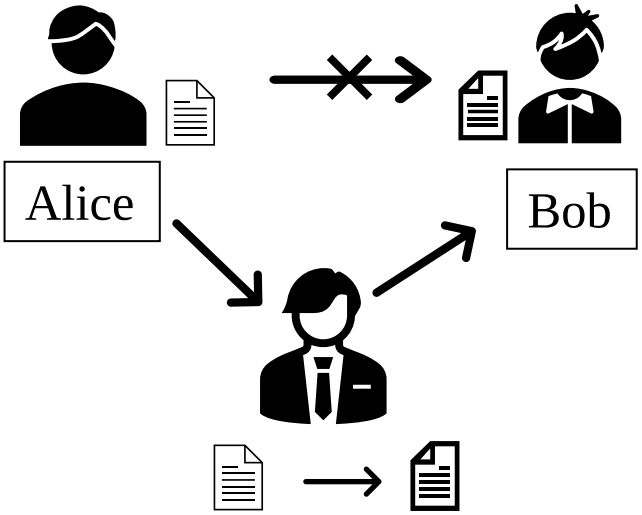
Before diving into the concept of ECC (Elliptical Curve Cryptography), As an individual, we must know "**Why we need cryptography**".

Let us take an example:

Here Alice is the sender which he is sending file over the internet to Alice who is receiver of the file.



So now Bob sent file to an unsecure network and his file got hacked / changed by Man in the middle (MIM) and then transferred to Alice.



(File data changed in between transfer)

In this scenario, Alice got the wrong information which was intended to send him by bob. Therefore, we need to implement the concept of cryptography here.

Cryptography

Cryptography is the art of hiding and securing information by a person or machine, which must be revealed only by an intended person.

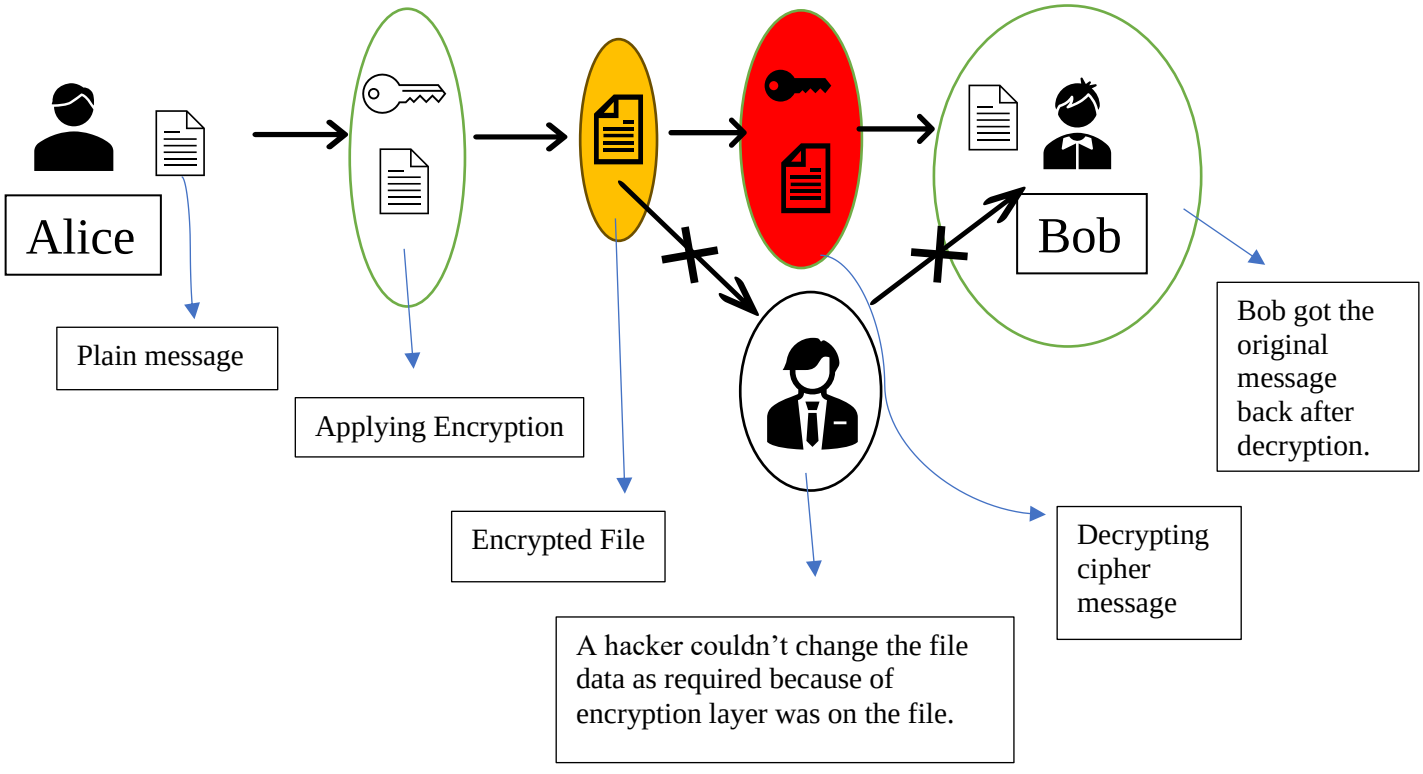
If we trace the history of cryptography, we can see that it was there for more than decades.

In ancient times people used to hide the file inside the sole of shoes or hide under the hat many more. That was more of a Physical war but now the information is in the form of soft copy like a virtual file which is located into your computer system.

The information before the transfer must be encrypted by small yet complex coding so no one can see or travers the data through within the file itself.

Again, if we take the same example.

Alice must use encryption before sending the file to bob and bob must decrypt the file with some key to decipher the cipher text.

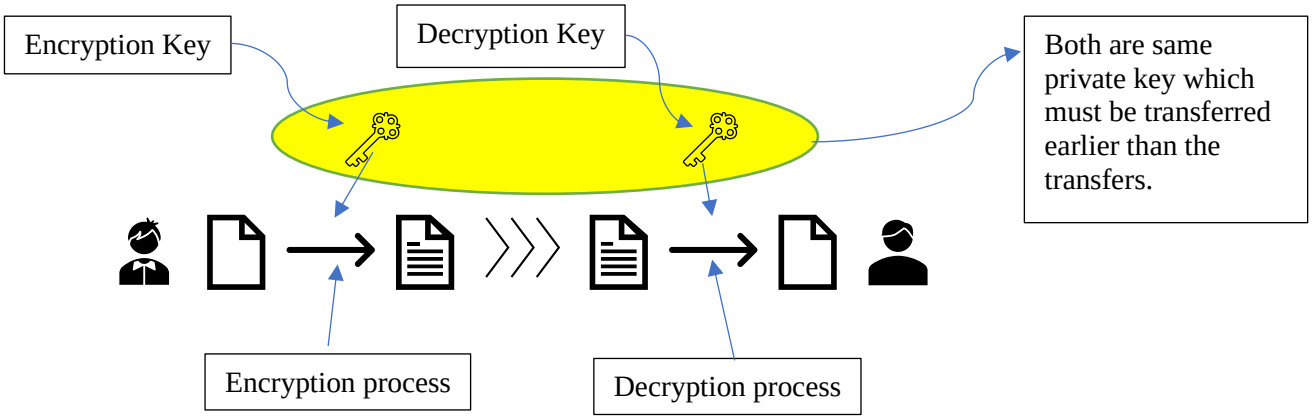


Types of cryptography

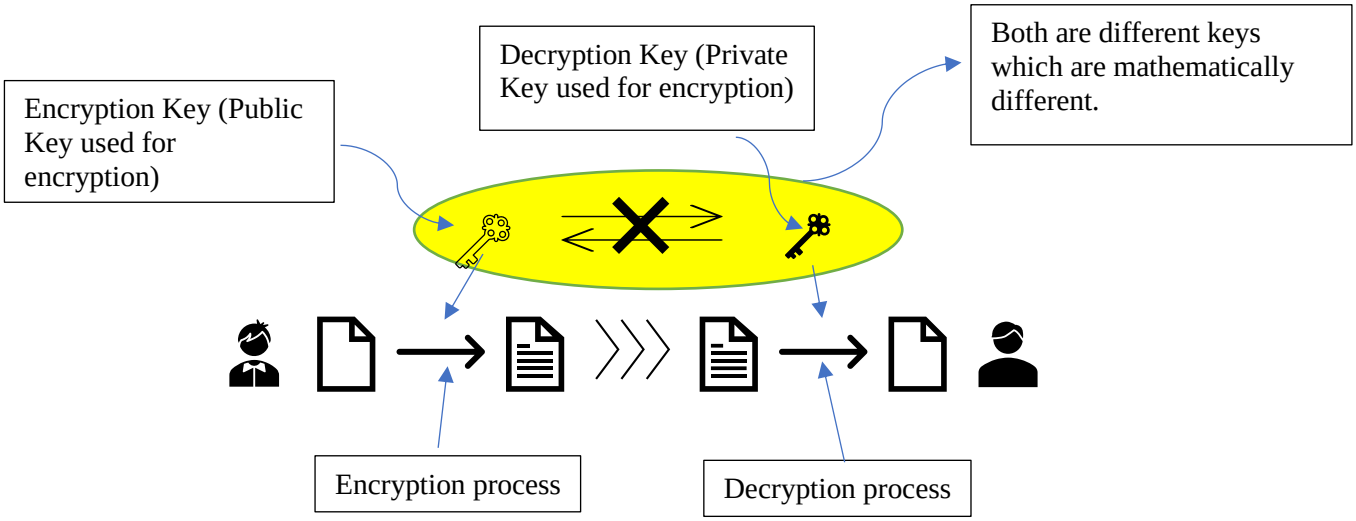
There are two types of cryptography: -

1. **Secret key (Private key cryptography): -** In this cryptography method both the party uses the same secret key which they both shared beforehand.

    a. This is generally used for faster processing.
    b. But it is considered as less secure, and many experts don't rely on this technique.

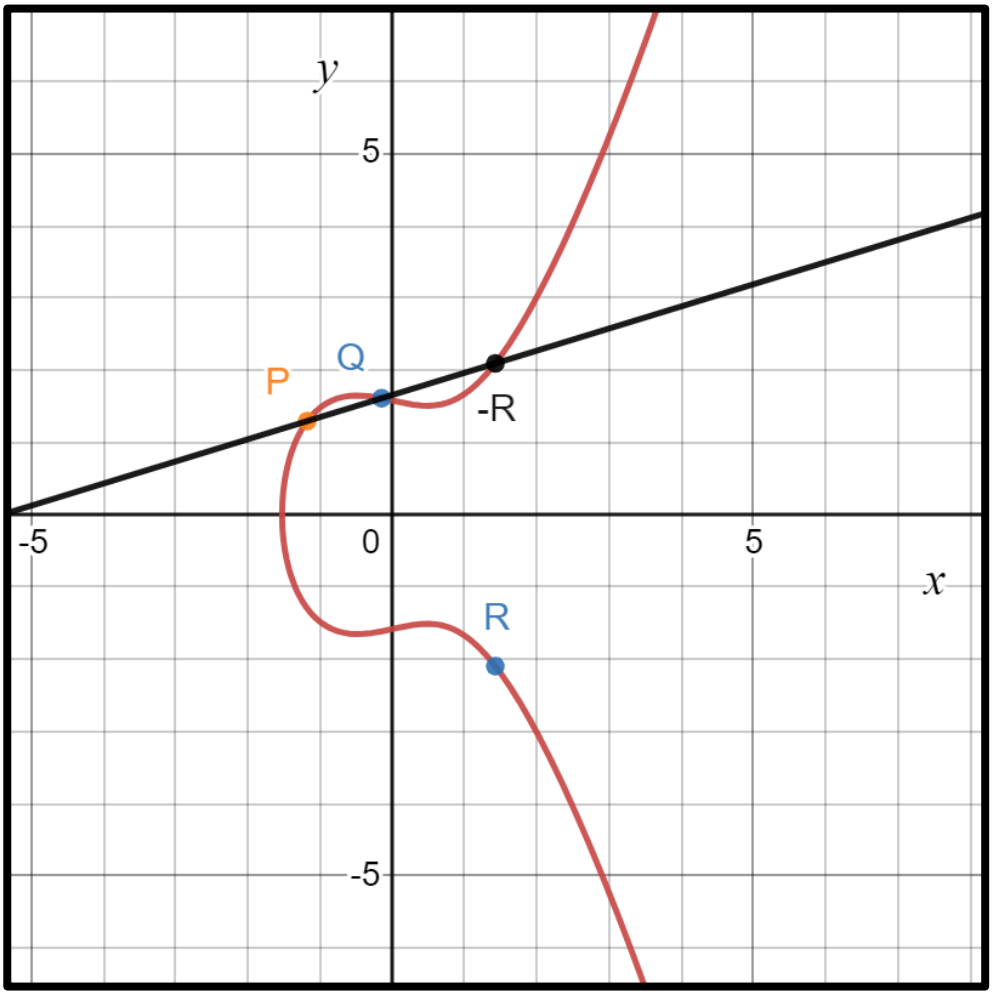


2. **Pair key cryptography (Public Key cryptography): -** This cryptography is the method where both parties have pair of keys.
    a. Public key (which are shared without compromising the system)
    b. Private key (which is within the person by which a encrypt file can be decrypt)



Elliptical Curve

To implement Elliptical Curve Cryptography, Understanding of Elliptical Curve be there. So, what is an elliptical curve?



The elliptical curve is not an ellipse, ellipse is formed with the square root and quartic roots of polynomial of x.

Elliptical curves use cubic equations to form a smooth and symmetric curve along x - axis.

Elliptical Curve has following equation:

$$y^2=x^3+ax+b$$

Properties of elliptical curve:

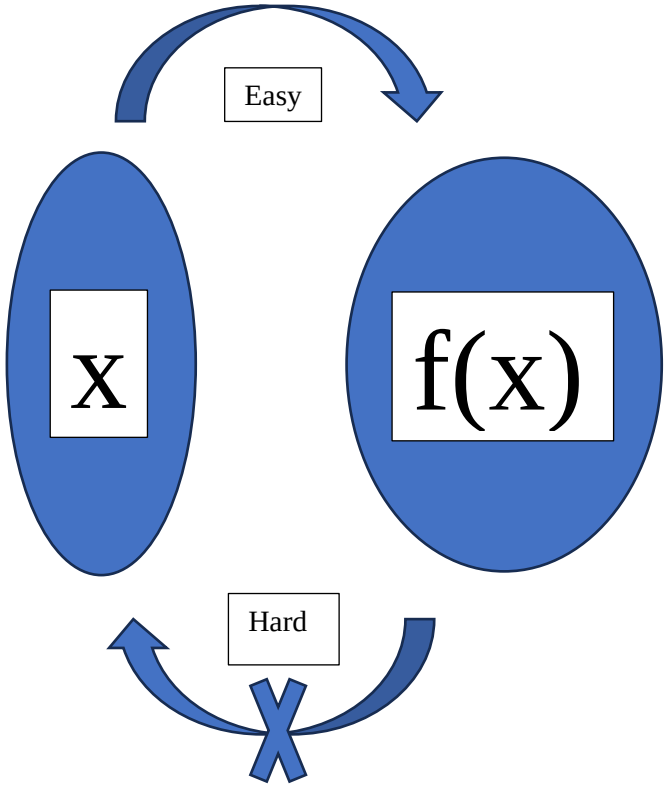
1. If we draw straight line on the curve, it will intersect the curve not more than 3 collinear points P, Q, R as labelled on the curve.
2. Curve would be symmetric on x-axis no matter whatever happen.

Elliptical Curve Encryption

Now the question is how we can use EC on cryptography. We can use the curve to formulate or to generate keys.

Since it uses the trapdoor function which is also used in **Diffie–Hellman** Key exchange algorithm.

Trapdoor function ensure that We can go to from x to f(x) easily, but we can't go f(x) back to x without the knowledge of special information (Trapdoor value) called trapdoor function.



1. Generating the key is a complex task here.
2. Using the special kind of curve some examples are given below:

    a. secp112r1
    b. secp128r1
    c. secp160r1
    d. secp224r1
    e. secp384r1
    f. secp521r1
    g. brainpoolP256r1
    h. brainpoolP384r1
    i. brainpoolP512r1

3. In ECC when we multiply fix EC point **G** (A point beyond range), with some integer **k** (Which will be our private key). We will get our **P** (Public-key)
4. In ECC we have one of the curves mentioned above over a finite field.
5. We will have **G, k, P.**
6. **P=k*G** is very fast operation to calculate via help of well known ECC multiplication algorithms (E.g., Double and add algorithm)
7. For 256-bit curve it will take couples of hundred simple EC operations.
8. But again, it is very slow operation to calculate for large value of **k** to calculate **k = P/G**.
9. Due to 7^{th} and 8^{th} point it make specialty of ECC Encryption.

Problem Statement

The problem lies within the public key encryption only, there are many techniques which uses the public key encryption Some are mention bellow:

1. Diffie Hellman key exchange
2. Digital signature standard (DSS)
3. Paillier cryptosystem
4. RSA (Rivest Shamir Adleman)

But none of them provide as much as security provide by ECC (Elliptical Curve Cryptography) system.

Just for the comparison below a table show how much difference a ECC can bring security with lower key size.

Security level	RSA key size (bits)	ECC key size (bits)	
80	1024	160	
112	2048	224	
128	3072	256	
192	4096	384	
256	15360	521	

Here we can see as for just for 80 bits of key length RSA using 1024 bits of key, compare to what ECC using is just 160 bits.

This shows us that we can utilize the more key size for more level of security which helps us to be more efficient with less resources.

File securing system

With the utilization of ECC capability I am making a system which can helps us (common man, experts) to encrypt file which can later transfer us without the fear of getting hacked with current technology of our data or information changes in file.

Providing users with a system with GUI mode to encrypt the file. Which will be complete made on python language.

Application will provide an easy way to handle files over a network for non-technical people too.

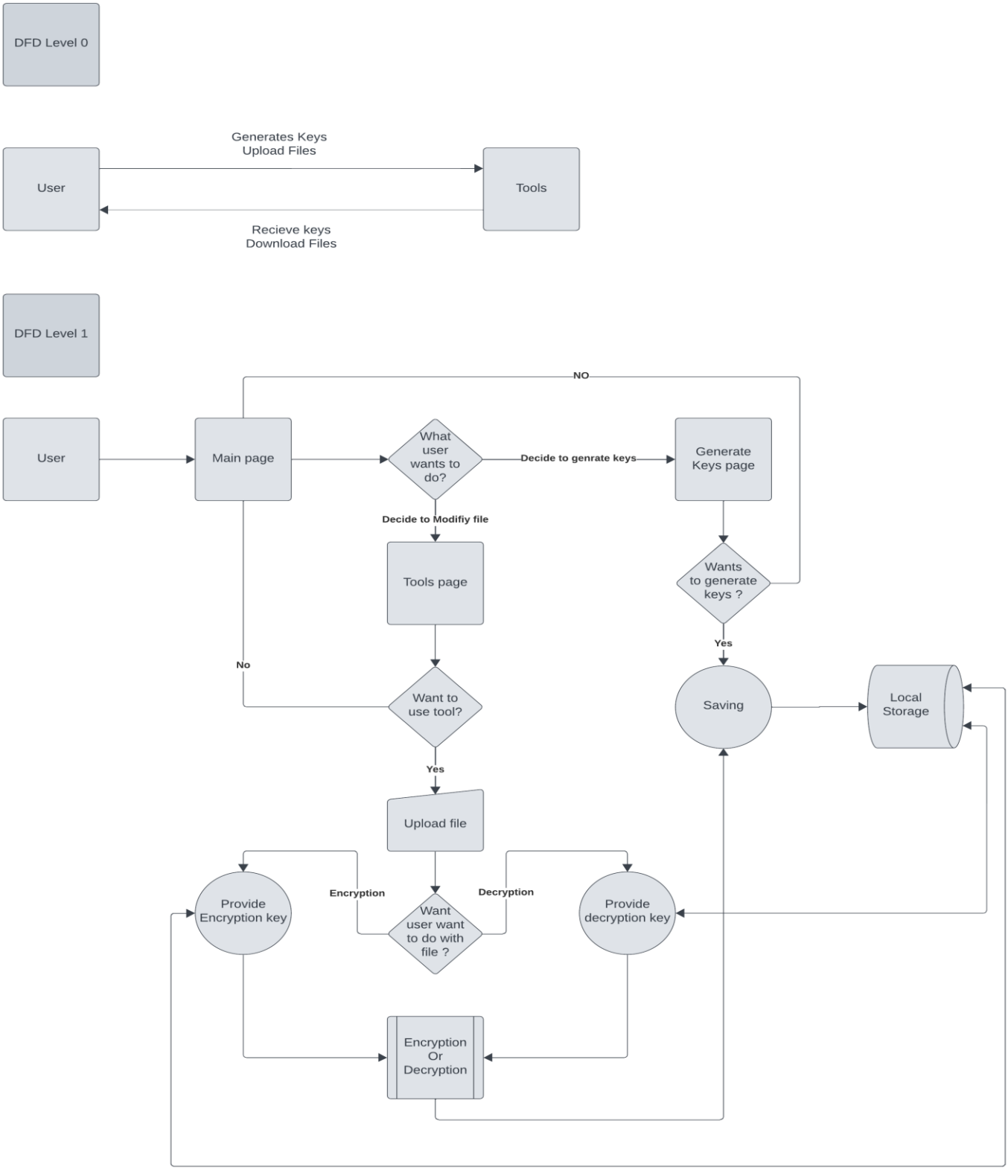
Requirement of the project (General / system)

For the application our requirement is mentioned below:

1. Laptop / PC
2. Specification of PC / Laptop
    a. Minimum requirement:
        i. i3 intel core 9th Gen or AMD Ryzen 3 5th Gen
        ii. 2 GB RAM and 120 GB ROM
    b. Recommend requirement:
        i. i5 intel core 9th Gen or AMD Ryzen 5 3rd Gen
        ii. 16 GB RAM and 256TB ROM
        iii. 4 GB Nvidia GTX 1050 Graphics Card
3. Knowledge:
    a. Basic knowledge of Cryptography
    b. Intermediate knowledge of higher mathematics
4. Programming languages (Any one of the mentioned below):
    a. Python (Recommended)
    b. C
    c. C++
    d. Java

Project design / design specification (Graphical / Visual representation)

DFD levels of the project.



Methodology / Implementation

To implement a file securing system with ECC cryptology, the following methodology can be used:

10. Generating key pairs for the user.
11. Saved in local storage.
12. With the help of key user can encrypt / decrypt file.

Outcomes / Benefits

Following are the outcomes or benefits of the project:

1. Users can achieve higher levels of encryption.
2. Developers can integrate with my project along with their projects which can reduce effort, time, and energy.
3. The market is demanding this kind of cryptography more often and over RSA which is also secure, but it takes space and resources of the users.
4. Project provides the user with a system to secure files which later can be transferred.

Conclusion

Due to the uniqueness of the ECC over RSA is very useful and extremely helpful for security.

RSA provides a well-defined security to file but due to certain scenarios where resources is the limitations, we cannot prefer it for a suitable security system.

ECC on the other hand provides us or user same level of security with lesser number of key sizes. Which means we can add more data to file and can perform strong encryption on file with lesser number of key sizes.

We can also further make addition to our security system by applying hybrid encryption like ECC with Diffie-Hellman, Or ECIES (Elliptic Curve Integrated Encryption Scheme) Hybrid Encryption Scheme.

References

1. Cryptobook website {https://cryptobook.nakov.com/asymmetric-key-ciphers/ecies-public-key-encryption (Recommended to check)}
2. Desmos of graph plotting (https://www.desmos.com)
3. Lucid Chart for DFD Diagram (https://www.lucidchart.com/pages/)
4. Internet
5. Some encryption-decryption website to get idea and reference of working of system.