**Introduction**

Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings. Once the data is out of hand, people with bad intention could modify or forge data, either for amusement or for their own benefit. Cryptography can reformat and transform our data, making it safer on its trip between computers. The technology is based on the essentials of secret codes, by modern mathematics that protects our data in powerful ways. Encryption and Decryption, a type of cryptography, refers to the process of scrambling information so that the observer cannot be detecting the data.

**What is Encryption?**

Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as cipher text. In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of a cryptographic key: a set of mathematical values that both the sender and the recipient of an encrypted message agree on

Plain text is encrypted using an encryption algorithm and an encryption key. This generates a unreadable text which is called as cipher text (encrypted data). Decryption is the inverse of encryption; original form of data can only be viewed by decrypting encrypted data with the correct key

**Cryptographic key** is a piece of data used to encrypt or decrypt to plain text. The Crypto, from the word cryptographic mean is it has its origins in the Greek word “KRUOTOS”, which means hidden. Thus, the objective of cryptography is to hide information so that only the intended recipient can read it.

**Problem Definition**

At present there are many encryptions and decryption, especially in the communication system provided in a variety of application. Encryption and decryption are particularly impacted in the field of military communications and reliable security data to protection for transmitting.

This cipher text is used in the military is to send information such as direction, strategy, secret codes and other information that cannot be known by the national foe during the war.

Creating this system is the process by which information cannot be detect by the national foe. The information cannot be recognizing by the national foe because this system is using the process to encrypt data and decrypt data

**Objective**

Encryption is a way of keeping your data safe and confidential as it is sent over the internet. Whenever you send personal information across the internet,

Be it passwords, credit card information or personal contact details, encryption stops others from seeing what you are doing.

Data is jumbled up in a manner so that when it travels through the internet it is completely unreadable; this stops hackers, who may try tointercept the data and see what you’re doing. All they’d receive is a random bunch of letters, numbers & symbols, which can only be decrypted using a random key generated during the encryption.

**Computer Security** - generic name for the collection of tools designed to protect data from hackers.

**Network Security**- measures to protect data during their transmission.

**Internet Security** - measures to protect data during their transmission over a collection of interconnected networks Security Attacks, Services and Mechanisms to assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements. One approach is to consider three aspects of information security.

**Planning for the proposed project**

**Methodology:**

**Encyption:**

The raw data entered by the user is processed by the software and is encrypted into a mix of jumbled characters which is rendered unreadable if it is tried to be intercepted during its transmission.

**Creation of unique cryptographic key:**

When the data is being encrypted by the software, it first creates an unique key, on the basis of which the data is encrypted in a specific format. This unique key is passed on to the user as an One Time Password (OTP)

**Decryption:**

The encrypted data is taken in as an input along with the OTP generated earlier. The software then unjumbles /decrypts the data using the specific format as given by the OTP. The raw data is obtained back and can be easily and securely viewed by the person to whom the data was intended to be sent.

**Algorithm:**



**Modules/Functions Used:**

**encrypt() :** an user-defined function used to encrypt the raw data using the generated unique key.

**generatekey():** an user defined function used to generate a random unique key which will be used to encrypt and decrypt data.

**decrypt() :** an user defined function used to decrypt the encrypted data using the unique key.

**Technological Requirements**

**Minimum Hardware Requirement:**

* Processor: Intel Core i3 (4th Generation)
* RAM: 4 GB
* Disk Space: 1 GB

**Minimum Software Requirement :**

* OS: Windows 7 / MacOS/ Linux
* Python 3.6
* Python Tkinter Library

**Details of participants**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Class/sec** | **Roll No.** | **House** | **Responsibilities** |
| **Agnik Chakraborty**  **(Team Leader)** | **XII/SC-C** | **4** | **Ruby** | * **Coder** * **Documentation** |
| **Aryaman Chaudhuri** | **XII/SC-C** | **12** | **Topaz** | * **Coder** |
| **Tanisha Bala** | **XII/SC-C** | **45** | **Topaz** | * **Coder** * **Documentation** |
| **Shovik Banerjee** | **XII/SC-C** | **36** | **Sapphire** | * **Coder** |
| **Md. Sayeed Ali Mondal** | **XII/SC-C** | **21** | **Emerald** | * **Documentation** |

**Application area of the Project**

Authentication/Digital Signatures

Authentication and digital signatures are a very important application of public-key cryptography. The only requirement is that public keys are associated with their users by a trusted manner, for example a trusted directory. To address this weakness, the standards community has invented an object called a certificate. A certificate contains, the certificate issuer's name, the name of the subject for whom the certificate is being issued, the public key of the subject, and some time stamps.

Pretty Good Privacy (PGP)

It is a software package originally developed by Phil Zimmerman that provides encryption and authentication for e-mail and file storage applications. Zimmerman developed his freeware program using existing encryption techniques, and made it available on multiple platforms. It provides message encryption, digital signatures, data compression, and e-mail compatibility.

Time Stamping

Time stamping is a technique that can certify that a certain electronic document or communication existed or was delivered at a certain time. Time stamping uses an encryption model called a blind signature scheme. Blind signature schemes allow the sender to get a message receipted by another party without revealing any information about the message to the other party.

It is very similar to sending a registered letter through the U.S. mail, but provides an additional level of proof. It can prove that a recipient received a specific document. Possible applications include patent applications, copyright archives, and contracts.

Electronic Money

The definition of electronic money (also called electronic cash or digital cash) is a term that is still evolving. It includes transactions carried out electronically with a net transfer of funds from one party to another, which may be either debit or credit and can be either anonymous or identified. . There are both hardware and software implementations.

Anonymous applications do not reveal the identity of the customer and are based on blind signature schemes. Identified spending schemes reveal the identity of the customer and are based on more general forms of signature schemes.

Anonymous Remailers

A remailer is a free service that strips off the header information from an electronic message and passes along only the content. It's important to note that the remailer may retain your identity, and rather than trusting the operator, many users may relay their message through several anonymous remailers before sending it to its intended recipient. That way only the first remailer has your identity, and from the end point, it's nearly impossible to retrace.

**Limitations of the project**

Encryption requires a password to encrypt and decrypt the file .If we deal with files that have information that we need to keep secret from unauthorized people, you can encrypt them to protect them. An advantage of encrypting a file is that only the person who knows the password should be able to open it. However, there are some disadvantages of encrypting files that deserve your attention.

* Existing files cannot be encrypted. To encrypt a file that is currently not encrypted, you must copy it into a new file whose encryption policy rules dictate that the file is to be encrypted. Note that renaming a file does not change its encryption attributes. Encryption attributes are defined at the time that the file is created.
* No encryption scheme is perfect.
* Cryptography does not guard against the vulnerabilities and threats arising due to phishing, keyloggers, Trojan horses and other such malwares.
* Cryptography comes at cost. The cost is in terms of time and money
* Addition of cryptographic techniques in the information processing leads to delay.
* The use of public key cryptography requires setting up and maintenance of public key infrastructure requires a handsome financial budget.