A STUDY OF CRYPTOGRAPHY AND ENCRYPTION*

BY

SANATH KAMATH[1], DEBJYOTI MANDAL[2], NIRMAL KUMAWAT[3], VARUN KANAGO[4],

NITESH YADAV[5], OMKAR PAWAR[6], PROF. VIJAY GAIKE[7]♣

[1-6]B .Tech Scholar, Data Science, School of Information Technology, Pune, India

[7]Associate Professor, Assistant Professor, Ajeenkya DY Patil University, Pune, India

ABSTRACT

This research paper is a practical for creating software for our daily security purpose. The internet has become one of the strongest ways that merges our lives, which is growing every day for the last several decades. Data security has become a concern for anyone connected with the internet. Data security makes sure that our data is accessible by the actual user and the data cannot be interfered by others. To increase the level of security, many algorithms have been developed. Cryptography is a technique that cipher data, it defers with respect to an algorithm that make data into a foreign text which is not understandable to the human eye unless we decrypt it by an algorithm predefined by the sender.

KEYWORDS

Cryptography, algorithms, Data Security.

INTRODUCTION:

Cryptography is a technique or a study of techniques to secure information in the presence of third parties. With the help of cryptography, we can construct and analysing rules that prevent others from reading secret messages with various aspects in information security such as data confidentiality, data integrity, and authentication which are central to modern cryptography. Modern cryptography often coincides with various other fields in the scientific and mathematical world. Electronic commerce, chip- based payment cards, digital currencies, computer passwords, and military communications are some of the applications of cryptography. The art of cryptography has deep historical roots, for example, the Egyptians used hieroglyphics, or images torepresent information.

* Received 22 September 2021, Accepted 09 October 2021, Published 24 October 2021
♣ Corresponding Author

METHODS OF CRYPTOGRAPHY:

Here is a brief look at some techniques that can be used to encrypt data. Some of these methods were invented in the ancient days, while some are quite sophisticated and are even used in modern day computing to protect data:

Substitution Cipher:

In this method of encryption, we substitute every single letter with a random character of choice,

A B C D E F G H I J K L M **G U I**
Y S W P T R D O A X N O P Q R
S T U V W X Y Z **Z F B N E J Q**
M L V C H K

provided the person deciphering the message is aware of the combination. For example, we can replace the letter 'A' with random replacement the character '&'. Assuming that we replace all characters available on a regular English keyboard, we can easily encrypt any text.

If we look at the above box, we can see all 26 letters of the alphabet being replaced with another random letter below it. Let us take an example. According to the above code, the word "ENGINEER" would become: "SZPRZSSR". The same set of characters can be decrypted, assuming the recipient has accessto the above code.

Caesar Cipher:

The Caesar Cipher is one of the oldest known ciphers in history. This was known to have been invented by the Roman Emperor, Julius Caesar himself. The idea of this cipher is to increment the characters in the message by a specific number, which is pre-decided by the creator as well as the recipient. Let us take a look at an example.

Let the key (the pre-decided number) be 3. Thus, the letters of the alphabet will get incremented by 3. So therefore 'A' will become 'D', 'B' will become 'E' etc.

The message can be decrypted by decrementing the message in the opposite manner.

Symmetric Key Cryptography:

Here receiver and sender use single common key to encrypt and decrypt messages. The main advantage is that it allows the faster transfer of data. However, the main challenge here is to ensure that the key is transferred securely between the two parties. Both Caesar and Substitution ciphers are examples of this.

Hash Functions:

No key is used here. A hash value with specified length is calculated as per the plain text which makes it unfeasible for contents of plain text to be recovered.
E.g. – Operating Systems use hash functions to encrypt passwords.

Asymmetric Key Cryptography:

Here pair of keys is used to encrypt and decrypt info's. A "Public Key" is used for encryption and "Private Key" for decryption. Public and Private Key are different. Even if Public Key is known by everyone, the intended receiver can only decode it because he alone knows the Private Key. Software such as Microsoft Office use such methods to ensure that only genuine versions of such software is being used and that the company is getting its due revenue.

Data Encryption Standard (DES):

This is a block cipher that is designed to encrypt data in pieces of 64-bits using a key that is 56-bits long. Apart from just encrypting the data, the cipher also changes the order of the data, to make it more confusing to hackers. Also, the last 8 bits of the key gets discarded form the original 64-bit to the new 56- bit.

This cipher has however, ceased to become quite irrelevant as modern hacking and penetration methods have proven to compromise data protected by it. Another form of DES is 3DES (Triple-DES). The key length is 112 and 168 bits long. The 3DES applies the DES algorithm three times on the piece of data along with increasing the key length. Altogether, this adds to the increased security of the data, ascompared to regular DES.

256-bit Security:

This is the type of security that is used by the AES (Advanced Encryption Standards) and is considered as one of the most secure methods to encrypt data. The length of the key being used to encrypt the data is 256-bits long. Thus, in order to hack into the data, one would require 2^{256} different combinations to break into the message. This would take a lot of time, effort and computing power for even the most powerful and sophisticated computers to crack. This would help delay and prevent a cyber theft or phishing attack on our data.

MODERN CRYPTOGRAPHY:

Modern ways of cryptography use a number of sophisticated algorithms which involve complex mathematical formulas that manipulate the data. Modern cryptography requires the various parties dealing with the data to have secure keys. Our anti- virus software's are examples of modern security systems that protect our data.

As the scope of the internet increases, so will cybercrime increase. Thus, demand for extremely strong security for data would be growing in demand. As research in cybersecurity as well as allied technologies such as Machine Learning and Cloud Computing increases, we will be able to develop software that can predict and prevent cybercrime such as hacking and phishing.

PRPOSED SYSTEM:

Our application is a simple explanation about the working of encryption and decryption. We have created a Java Swing Application as well as a Python Application to demonstrate how encryption as well as decryption works. The software takes user input, manipulates it based on an algorithm that makes use of the ASCII code of the entered characters and gives an output. The software will also decrypt the already encrypted data using the same technique, but in the opposite manner. This can take various types of data such as credit-card numbers,

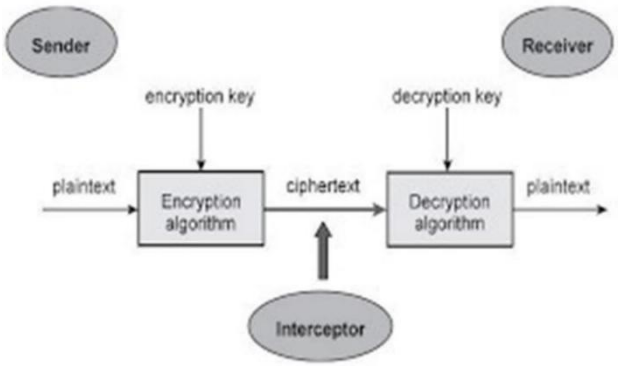
account numbers, passwords etc., and effectively encrypt, as well as decrypt it. This can be used by small businesses to protect data and prevent theft.

ARCHITECTURE OF PROPOSEDSYSTEM:

The system works directly on the data provided by the user. The user will put his data in the text field and will select the mode of ciphering the text (Encryption or Decryption). The person also has to enter an integer value to increase the positions of the letters selected to make it difficult for third party to decipher it. The entered input will go through an algorithm that will manipulate it according to the option selected by the user. The output will then be shown in a text field.

PROGRAMMING:

The examples of Java and Python encryption – decryption code are displayed in the next few pages.



JAVA CODE:

For Encrypting:

```
String a = t1.getText();
```

```
int key = Integer.parseInt(t3.getText());int n = a.length();
char[] chars = a.toCharArray();int i = 0;
char newtxt[] = new char[n+1];for(char c : chars){
   c += key; newtxt[i] = c;i++;
```

For Decrypting:

```
String a = t1.getText();

int key = Integer.parseInt(t3.getText());int n = a.length();
char[] chars = a.toCharArray();int i = 0;
char newtxt[] = new char[n+1];for(char c : chars){
   c -= key; newtxt[i] = c;i++;
```

```
# Function to encode

def encode(key, msg):enc = []
    for i in range(len(msg)): key_c = key[i % len(key)] enc_c = chr((ord(msg[i])
    +
            ord(key_c)) % 256)enc.append(enc_c) print("enc:", enc)
  return base64.urlsafe_b64encode("".join(enc).encode())
.decode()

# Function to decode
```

```
def decode(key, enc):dec = []

   enc                                          =

base64.urlsafe_b64decode(enc).decode()for i in range(len(enc)):

      key_c = key[i % len(key)] dec_c = chr((256 + ord(enc[i]) -

               ord(key_c)) % 256)

      dec.append(dec_c)print("dec:", dec)

   return "".join(dec)


   def Results():


   # print("Message= ", (Msg.get()))


   msg = Msg.get()k = key.get()

   m = mode.get()

   if (m == 'E'):

      Result.set(encode(k, msg))else:

      Result.set(decode(k, msg))

# exit function

def qExit(): root.destroy()


# Function to reset the window

def Reset():
```

```
Msg.set("")

key.set("")

mode.set("")

Result.set("")
```

CONCLUSION:

The Encryption System initiative aims to play a key role in protecting valuable data. Personal data as well as data belonging to organizations and governments around the world are always at a risk of being vulnerable to hackers who may want to use the data to achieve unethical goals for their own personal benefit. Data, as we know is increasingly becoming a very valuable resource. Thus, it is of utmost importance to keep it secure. The way in which we protect our data can make a huge difference.

Our project, apart from demonstrating the nuances of cryptography, can also be used in a real application by encrypting real, important data such as health, financial records, Aadhar and PAN card numbers etc.

REFERENCES:

[1] Abdalbasit Mohammed Qadir, Nurhayat Varol, “A Review Paper on Cryptography”, June 2019, Firat University, Elazig, Turkey

[2] https://www.researchgate.net/publication/334418542_A_Review_Paper_on_Cryptography

[3] Sarita Kumari, “A research Paper on Cryptography Encryption and Compression Techniques”, 4 April 2017 file:///C:/Downloads/3630-Article%20Text-6635-1-10-20180104.pdf

[4] Yahia Alemami, Mohamad Afendee Mohamad, Saleh Atiewi, “Research on Various Cryptography Techniques”, July 2019 https://www.ijrte.org/wp-content/uploads/papers/v8i2S3/B10690782S319.pdf