**Cryptography using Neural Networks**

**Shyamala Mathi1, Varun Santhana Gopalan2, Archana Subramaniam3, Yadav Sachin Krishnan4,** *1Shyamala Mathi Department & S.I.E.S.G.S.T, Nerul.*

*2Varun Santhana EXTC Department & S.I.E.S.G.S.T, Nerul*

*3Archana Subramaniam EXTC Department & S.I.E.S.G.S.T, Nerul*

*4Sachin Yadav EXTC Department & S.I.E.S.G.S.T, Nerul*

*5Shyam Ravi EXTC Department & S.I.E.S.G.S.T, Nerul*

---------------------------------------------------------------------\*\*\*---------------------------------------------------------------------

**Abstract -**Security is a vital component of any communication system. People send sensitive information over the channel and it needs to be secure without getting infiltrated by any third party. So, it is crucial to protect human resources, data, information with the absence of threat to make progress in society. AS humankind evolved, so did the technology used in security. The up-gradation of algorithms made the network more compact & harder to break. From different techniques like Caesar cipher, enigma machine, and block-chain the succession is significant. The study and implementation of various secure communication is called cryptography. It is a protocol that prevents the public from invading personal data.

Cryptography comprises two parts; encryption and decryption. The sender only shares the decoding method with the receiver to avoid potential hackers. It mainly works on number theory but, for real-time communication, cryptography falls short of its goal. So, cryptography got merged with real-time protocol and can give real-time output. One such technique currently under research is the artificial neural network. The artificial neural network is a system that functions like a human brain. Once the information gets filled into the ANN system, it analyses and connects the pieces as per the output requirement. It is a process with multiple nodes, neurons working simultaneously to figure out the output. In the project, we combine both concepts to implement a new security method known as Neural Cryptography. Neural cryptography is a dedicated cryptography method that deals with the use of an ANN algorithm for the encryption and decryption process. The network uses the mutual learning concept to train, learn the input task for generating the result.

# 1.INTRODUCTION

Cryptography is a method of concealing messages for the transmission of sensitive information and communication. It's used to send sensitive information from one person to another in a safe manner that can't be intercepted or forged by a third party. It has a variety of other uses in the banking industry, as well as protection and maintenance. The following are the key components of cryptography:

1. The Plain Text- The plain text is the initial message that will be sent to the recipient/secondperson.
2. The Cipher Text- The Cipher Text is a hidden or encoded version of plain text that is used to send information.
3. Key- This is a code that is used to send encrypted data or to receive encrypted data and decrypt it. encoding
4. Encryption-Encryption is the transformation of plain text into Cipher text
5. Decryption-Decryption is the process of translating cypher text into plain text.

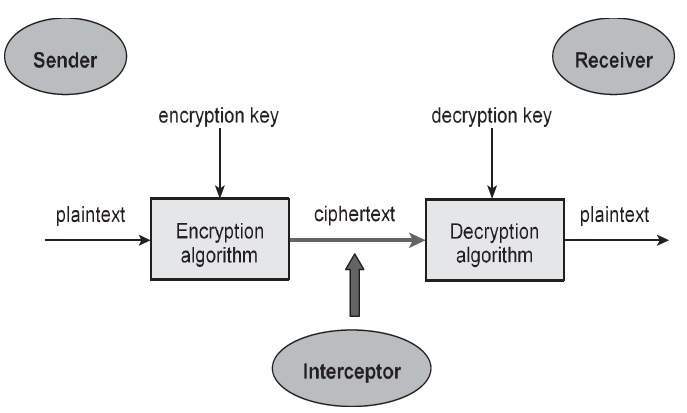


Fig-1:Basic Cryptography Block Diagram

# 2. Need of Project

The advancement of technology has always raised concerns about security in the communication field, resulting in a greater demand for safe communication networks. Cryptography is one of the most effective methods for safe communication, with various implementations in mobile devices, smartphones, the internet, and other electronic devices. As a result, we've created a project that will enable cryptography to be used in conjunction with ANN and other methods to provide a safe form of communication for confidentiality purposes. This software will teach you how to write plain text, encrypt it, and decrypt it. This approach, which combines ANN and cryptography, will boost the system's speed. It is primarily useful in the defence, manufacturing, and other sectors. As we all know, a Deep Social business leaked data from Instagram, Tiktok, and YouTube, which was confirmed by the cybercrime unit as a breach in data of the users. Cryptography may play a critical role in preventing hackers or intruders from hacking into or obtaining information from companies in this situation. According to Sources, a violation occurred in companies such as Just Dial and SBI in India. The data might have been encrypted at this time if the protocol used was cryptography, a programme that uses cryptography to secure communication with

# 3. Literature Survey

# Artificial neural networks have recently been explored in relation to different network approaches and their learning properties, according to recent research.

# The neural implant network was explored by Zurada [2] in relation to contrast learning methods and network architectures. The best way to explain supervised and unsupervised learning is to use specifics and the aid of network design. The layout indicates how to use training parameters. The reduction of error functions in multilayer supply networks is described by the back-built algorithm.

# Koshy [3] focused on problem-solving strategies and implementation of it. We use Fermat’s Little Theorem, to find the small residue variables. Different algorithms and cryptography systems depict the methods of encryption and decryption. Depending on the use of key, the cryptography system is fragmented and defined in detail.

# Kanter and Kinzel [4] introduced neural network and cryptography theory based on a novel method of synchronising secure neural network private message transfer. Encryption is focused on neural synchronisation shared learning networks, which use dual neural formation networks to synchronise synaptic instruments through exchanging and reading data. The results of the shared feedback have been given. With the release of another network, one network can be trained. When the findings are inconclusive, the weights are balanced and renewed according to Hebrew reading regulation. Synchronization of the two real-time networks, which tends to degrade as the size of the input grows. The author focuses on reducing the number of time steps in the synchronisation process to a bare minimum while preserving network security.

# Laskaris [5] investigated the role of artificial neural networks in encryption problems involving various types of computer-generated cryptosystems. It has shown how to use neural artificial networks to solve problems and found better solutions. The output of a cryptosystem on a computer can be used to assess its effectiveness. The analysis of three problems is discussed in this paper: the logarithmic problem, the factorization problem, and the Diffie-Hellman key exchange protocol problem.

# The back-propagated method is used to train the feed network of page text and plain text using neural implant networks. This aims to give the network the right amount of weight in order to reduce the gap between real and desired performance. The network's output is reviewed after general information is entered. A percentage of qualified data is measured, as well as its estimated value..\\

# Meletiou [6] discusses RSA cryptography and how it has been used in a variety of attacks. To capture the defining key, the author used a neural input network to calculate the Euler Totient function. As a result, RSA cryptography is simple to use. To train data setup for backward errors, a multilayer feedforward network is used. Although the network literacy standard is not optimal, it is definitely reachable. The estimated and full error rates are used to assess network efficiency. And the outcome is assured by a collection of main numbers that range from high to low.

# Asymmetric key encryption (RSA) is a technique that uses asymmetric keys to encrypt data. It is the most commonly used and flexible public key algorithm. Only the modular exponentiation of long integers is used in RSA. The entire system's public keys or private keys are regenerated, ensuring more reliable data protection. Since high throughput is needed in data communication, quick modular multiplication becomes the key to real-time encryption and decryption.

# The RSA cryptosystem is the most commonly used public-key cryptosystem for both encryption and digital signatures. It's often used to secure e-commerce and e-mail, as well as to set up virtual private networks. It is present in most commercially available security products and is implemented in most web servers and other browsers. Indeed, RSA's widespread use has positioned it at the forefront of modern information security. It is not an exaggeration to conclude that the RSA cryptosystem's security properties are crucial to Internet security

# 4. Proposed System

The current encryption scheme is AES (Advanced Encryption Standard), which is a method for data encryption developed by the National Institute of Standards and Technology in the United States. This norm primarily focuses on block cypher encryption using matrix and symmetric key algorithms, which is also known as shift cypher.

This approach is currently in use, in which the sender and receiver both obtain the same key for data encryption and decryption. We'll use an asymmetric key algorithm to generate unique keys for different senders and receivers, ensuring that the key is also safe.

**Methodology**

{Language used to code: Python (Version - 3.7.4)} Guido van Rossum developed Python in 1991 as a high-level, scripted, general-purpose programming language. Of all the scripting and programming languages, it is one of the best.MachineLearning libraries and frameworks come in a wide variety. It has a large number of libraries and frameworks that help developers save time. NumPy, for example, is a versatile library that aids in scientific computation. The most critical element is simplicity. It has a basic syntax and is very convenient to use. The codes are clear and easy to understand. Machine learning and deep learning benefit from this. After every conditional and loop expression, no brackets or semicolons are needed, and everything works with the indentation. As a result, the coding time is significantly reduced, allowing one to consider algorithms during that time.Python has a wide community of people working on it, as well as a wealth of documentation. As a result, there are several tools available to assist developers who get lost at any point during their project.

**One Hot Encoding:**One Hot Encoding is a technique that transforms unique data into binary vectors, thus indicating the winning node and removing any uncertainty in the model. The first solution was to use neural networks to solve the problem because the decision-making process should be similar to that of humans and the margin of error should be small.

**NumPy:**NumPy is a free and open-source Python library for numerical computations. It is a Python programme that can be used for scientific computing and a variety of operations. It's a general-purpose array processing kit that includes high-performance multidirectional array objects and software for manipulating them. It can be used to perform a variety of operations on arrays, including trigonometric, statistical, and algebraic routines. NumPy is a Numeric and Num array extension..

**TensorFlow**: To comprehend tensor flow, we must first comprehend what a tensor is. In tensor flow, tensors are a standard way of representing data. They are multi-dimensional arrays, which are two-dimensional tables (matrices) with additional dimensions. So, tensors are represented as n-dimensional arrays of base datatypes in TensorFlow. The key object you control and move around when writing a tensor flow programme is tf.Tensor.TensorFlow is a free software library for dataflow and differentiable programming that can be used for a variety of tasks. TensorFlow APIs are organised in a hierarchical structure, with high-level APIs based on lower-level APIs. Low-level APIs are used by machine learning researchers to develop and test new algorithms.

**Keras on TensorFlow:**TensorFlow's implementation of the Keras API specification is called keras. This is a high-level API for building and training models, with the strongest support for TensorFlow-specific features like eager execution, tf.data pipelines, and Estimators. wtfTensorFlow is made easier to use with keras, without compromising flexibility or output. For quick deep neural network experimentation, the Keras on TensorFlow module was used. Keras includes various implementations of popular neural-network building blocks including layers, goals, activation function, optimizers, and a slew of other tools to make interacting with image and text data simpler and to reduce the amount of coding required for writing.The main goal of keras was to identify user feedback so that intents could be recognised. We've added Sequential and Dense to Keras because they're different and serve different purposes. Sequential usually refers to an entire model, not just one layer, whereas Dense usually refers to a single layer. The sequential Api (from keras.models import Sequential) allows you to create neural networks one layer at a time, in the following order: input layer, hidden layer 1, hidden layer 2, etc... output layer. This is simple and intuitive, but it restricts the types of networks you can create..In contrast, the functional Api (from keras.models import Model) allows you to create acyclic graphs, shared layers, and other stuff, but you must define several of the parameters yourself (e.g., how layers should be connected, which one is the input and which one is the output, etc...) Dense refers to the types of neurons and connections used in that layer, specifically a regular completely connected layer, as opposed to an LSTM layer, a CNN layer (different types of neurons), or a Dropout layer (same neurons, but different connectivity compared to Dense).

**Shallow Neural Network:**A neural network has intermediate layers, also known as hidden layers, in addition to input and output layers. They're also known as encoders.

There are less hidden layers in a shallow network. While studies show that a shallow network can accommodate any feature, it will need to be extremely large. As a result, the number of parameters increases dramatically. Just one or two hidden layers are present in shallow neural networks. Understanding the deep neural network allows one to gain insight into what is actually going on inside it. A deep network can suit functions better with fewer parameters than a shallow network, according to definitive findings.

**Backpropagation in neural networks :**Back propagation, also known as "back wave propagation," is a technique for studying artificial neural network surveillance using gradient reduction. The method calculates the gradient function of the error in relation to the weights of the neural network given the artificial neural network function and error function. It's a hybrid of perceptron delta law and multilayer feedforward neural networks.The neural implant network is a linked community of nodes that are in charge of simplifying the network's neurons. Each circular node represents an artificial neuron, and an arrow represents a link formed when one artificial neuron is released into the environment.. Artificial neurons are a group of connected units or nodes in an ANN that freely balance neurons in the network. Each link, like the network's synapses, can send signals to other neurons. A signal is received by an artificial neuron, which processes it and displays neurons connected to it.

**Encryptions Methods** :Symmetric and asymmetric encryption are the two key methods of encryption. Public key encryption is another name for asymmetric encryption. There is only one key in symmetric encryption, and all contact groups use the same (secret) key for encryption and decryption. There are two keys in asymmetric, or public key, encryption: one is used for encryption, and the other is used for decryption. The encryption key is kept secret (hence the name "secret key"), but the encryption key is exchanged freely and can be used by anyone (hence the term "public key").

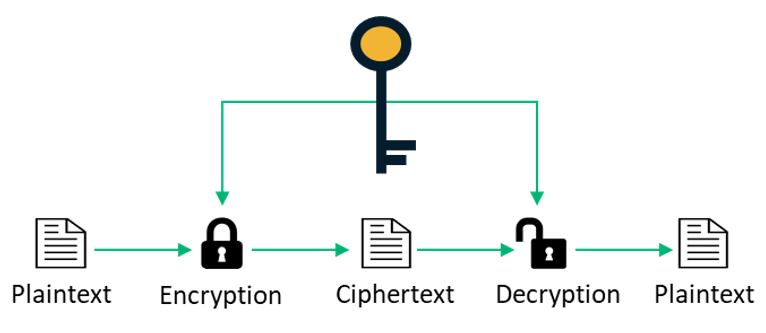


Fig-2:Encrytion Methods

**Caesar Cipher:**Caesar Cipher is a cryptographic algorithm. Caesar cypher, also known as Caesar's cypher, shift cypher, Caesar code, or Caesar's shift, is one of the simplest methods of encryption. It is a form of substitution in which Each letter is inserted into the alphabet's alphabetical number of positions.

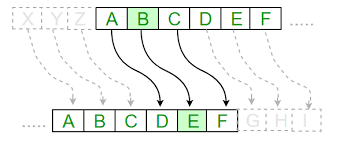


Fig-3:Caeser Cipher Basic Working

**Steps followed in the process**

1. All libraries are being imported
2. Using a formula to define the Caeser cypher for encryption and decryption
3. Generation of a randomly generated dataset
4. Converting the dataset to a single alphabet with corresponding cypher text
5. Shallow neural network training
6. Analyzing and decoding

**5. Dataset And Flowchart**

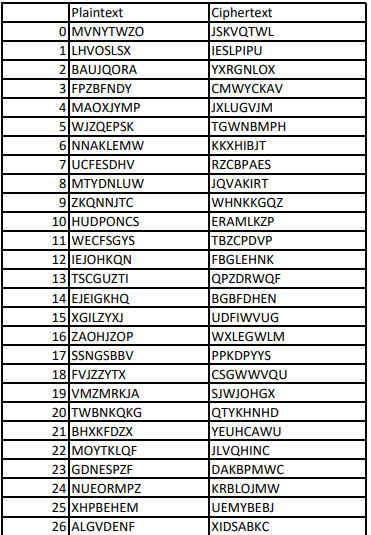


Fig-4 A: Sample Dataset

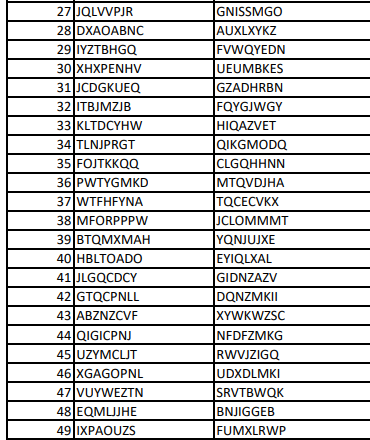


Fig-4 B: Sample Dataset

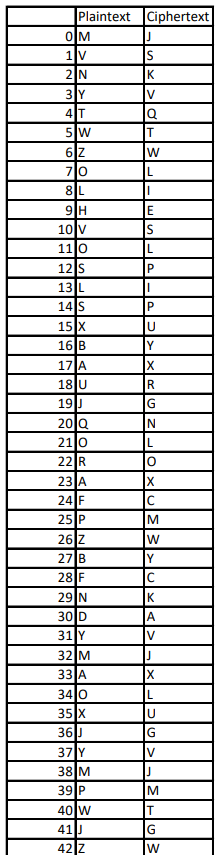


Fig-4 C:Caeser Cipher Dataset

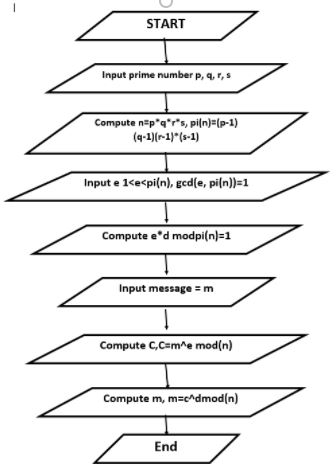


Fig-5 A: Encryption Flowchart

Flowchart 1

1. Step 1: Take input for keys
2. Step 2: Using formula compute cipher text key
3. Step 3: Take input of plain text
4. Step 4: Use the key value in formula to get an encrypted value
5. Step 5: The formula gives new cipher text

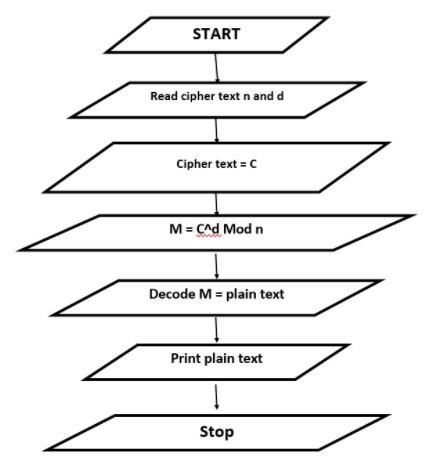


Fig-5 B: Decryption Flowchart

Flowchart 2

1. Step1: Read the cipher text and key
2. Step2: By using formula compute the real (plain) text
3. step 3: print the Plain Text

# 7. Conclusion And Future Scope

Using the method of Caeser cipher we were able to encrypt and decrypt the given data successfully with an accuracy of 100 percent during the testing and training phase of the system.

The output of our proposed system is shown below:

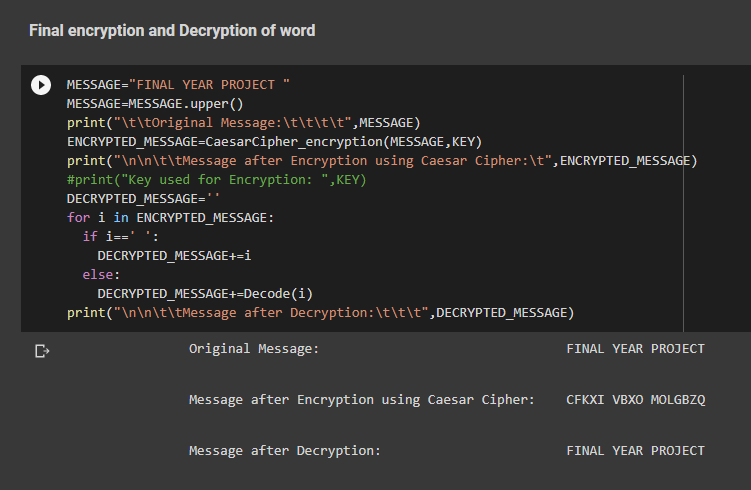


Fig-6: Result Using Sample Dataset

The future scope of this system is that it can be used in a fast way of encrypted communication between two systems and it can also be used in many confidential communications.

# REFERENCES

1. Analysis of Neural Cryptography by Alexander Klimov, Anton Mityagin and Shamir, The Weizmann Institute.
2. Cryptography based on Artificial neural networks by ShitalDaulatJagtap and Mr.P.BalaRamudu, IJAIEM.
3. Jacek M. Zurada, Introduction to Artificial Neural Systems, West Publishing Company, St. Paul, 1992.
4. Thomas Koshy, Elementary Number Theory with Applications, Elsevier, a division of Reed Elsevier India Private Limited, Noida, 2009.
5. Kanter and W.Kinzel, “The Theory of Neural Networks and Cryptography,” Quantum Computers and Computing, vol. 5, pp. 130-139, 2005.
6. E.C.Laskari, G.C.Meletiou, D.K.Tasoulis, M.N.Vrahatis, “Studying the performance of artificial neural network networks on problems related to cryptography,” Nonlinear Analysis: Real World Applications, vol.7, pp. 937-942, 2006.
7. G.C.Meletiou, D.K.Tasoulis, M.N.Vrahatis, “A first study of the neural network approach in the RSA cryptography,” in Sixth IASTED International Conference on Artificial Intelligence and Soft Computing (ASC 2002), Banff, Alberta, Canada, July 17-19, 2002.
8. URL: http://www.wikipedia.org/. “Mathworks,” The Mathworks, Inc., URL:\ http://in.mathworks.com/help/nnet/ref/trainlm.html;jsessionid=a15fe82129a83dc8a92470543e5c.

|  |  |
| --- | --- |
|  |  |
|  |  |