

# Neural Network based Message Concealment Scheme

Neural Cryptography: Future of Communication  
Security

Prasann Shimpi  
Sanket Halake  
Shivam Dharmshetti  
Shashank Singh

Guide: Dr. Amol Dhakne

# Overview

Nowadays, we live in a data-driven world, and in most use cases, businesses collect and store sensitive personal and non-personal information, which can be exploited by cyber criminals.

Good cryptography keeps you safe by using incredibly long keys and using encryption algorithms resistant to other attacks.

The neural network application is a form of the next development in good cryptography. This project is about the use of neural networks in cryptography, for example, the design of a neural network that is practically used in the field of cryptography.

To demonstrate an application of ANNs in the field of cyber security, we create three neural networks: Alice, Bob and Eve. Two of these participate in a message exchange using symmetric encryption and the third acts as an adversary and observe the rate of success.

# Literature Review

Sr No.	Paper Title	Authors and Published on	Overview
1	Deep Neural Networks based key concealment schemes	Taehyuk Kim, Tae Young Youn 04 Nov 2020	In this paper, we propose a new DNNs-based key concealment scheme for concealing cryptographic keys within DNNs.
2	A Neural Network based Approach for Cryptographic Function Detection	Li Jia, Anmin Zhou, Peng Jia, Luping Liu, Yan Wang, Liang Liu 2020	This paper proposed a novel approach for cryptographic function detection in malware.
3	Neural Cryptography based on Complex Valued Neural Networks	Tao Dong,Tingwen Huang 2019	This paper took a complex value based parity machine (CVTPM) approach to neural cryptography.
4	Neural Cryptography Based on Topology Evolving Neural Networks	Yuetong Zhu, Danilo Vasconcellos Vargas, Kouichi Sakurai 2018	This paper suggested a neural network architecture to learn neural cryptography.
5	Neural Cryptography: From symmetric encryption to Adverarial Steganography	Dylan Modesitt, Tim Henry, Jon Coden, and Rachel Lathe 2018	This paper discussed various research in the field of neural cryptography from symmetric encryption to steganography.

# Literature Review

Sr No.	Paper Title	Authors and Published on	Overview
6	Use of Neural Networks in Cryptography: A Review	Pranita P. Hadke, Swati G. Kale 2016	This paper gave a review of the current usage and possibilities of the utilisation of neural networks in cryptography.
7	Neural Network based Cryptography	Apdullah Yayik,, Yapik Kutlu 2014	This paper discussed the iteration of ANNs in cryptography and their advantages over other methods (symmetric encryption).
8	Cryptography based on Neural Networks	Eva Volna, Michael Janosek, Martin Kotyrba 2014	This paper brought into light the method of practical implementation of neural cryptography in real world applications.
9	Cryptography using Artificial Neural Networks	Vikas Gujral, Satish Pradhan 2009	This paper represented a comparative study between different neural network architectures for a adder and discussed their possible applications in cryptography.
10	Neural Cryptography	Wolfgang Kiesel, Ido Kanter. 2002	This paper discussed the first iteration of ANNs in cryptography and their advantages over other methods (symmetric encryption).

# Traditional Cryptography

The most basic form of cryptography is symmetric cryptography, also known as private key cryptography, where a secret key is known by both the sender and receiver.

This makes a conversation using symmetric encryption prone to man-in-the-middle and eavesdropping attacks. While this was tackled with the introduction of public key encryption, public key encryption itself is computationally demanding.

With the advent of machine learning, it's implementation in cryptography is still a point to ponder upon. A successful implementation of AI in cryptography will surely help save privacy to a greater extent while saving computational resources.



# Problem Statement

**PROBLEM:** The problem in focus is to determine whether 2 neural networks are able to perform cryptographic operations in presence of an adversary

**BACKGROUND:** In this revolutionary age of big data and artificial intelligence, there is imminent focus on data privacy and confidentiality. As observed with recent events, data leaks and ransomware attacks are undesirable and more efficient measures are an uprising necessity.

**STATEMENT:** To demonstrate the current progress of implementing Artificial Intelligence in Cryptography and see how it performs against traditional methods. The project is based in the demonstration using three artificial neural networks that will generate and exchange keys for symmetric encryption while the third acts as an adversary. This will not only help test the strength of the encryption and key exchange algorithm but also supersede the need of a human adversary. When executed via the right strategies, cryptography helps you safeguard this sensitive information, preventing it from falling prey to cyber threats and threat actors.

# Objectives

To ensure data integrity through hashing algorithms and message digests. By providing digital codes and keys to ensure that what is received is genuine and originates from the intended sender, the recipient can ensure that the data received has not been tampered with in transit

To test key exchange between two neural networks in presence of an adversary.

# Introduction

Neural Cryptography is a recently emerging subsection in cryptography.

It utilises artificial neural networks for encryption and cryptanalysis of data. Key and message concealment is achieved through the usage of CNNs and RNNs.

It is a novel method of exchanging secret keys between 2 neural networks through mutual learning.

In this project, we shall explore the performance of two neural networks in key/message exchange in presence of an adversary.



# Software Requirements and Technology Stack

Front End:

HTML, CSS, JavaScript

Backend:

Anaconda

Python 3 and Packages:

Tensorflow

Keras

Flask

Database: Randomly generated key and messages of fixed lengths, MySQL.

# Structure Overview

The project includes 3 neural networks with further discussed topology.

The sender is given a  $n$ -bit input message and a  $n$ -bit key.

The job of this sender is to generate an  $n$ -bit output - the ciphertext.

This neural network has a fully connected layer followed by four convolutional layers .

The receiver also has a similar architecture.

The eavesdropper is also a neural network, but its input consists of ciphertext only and not the key.

# Dataset

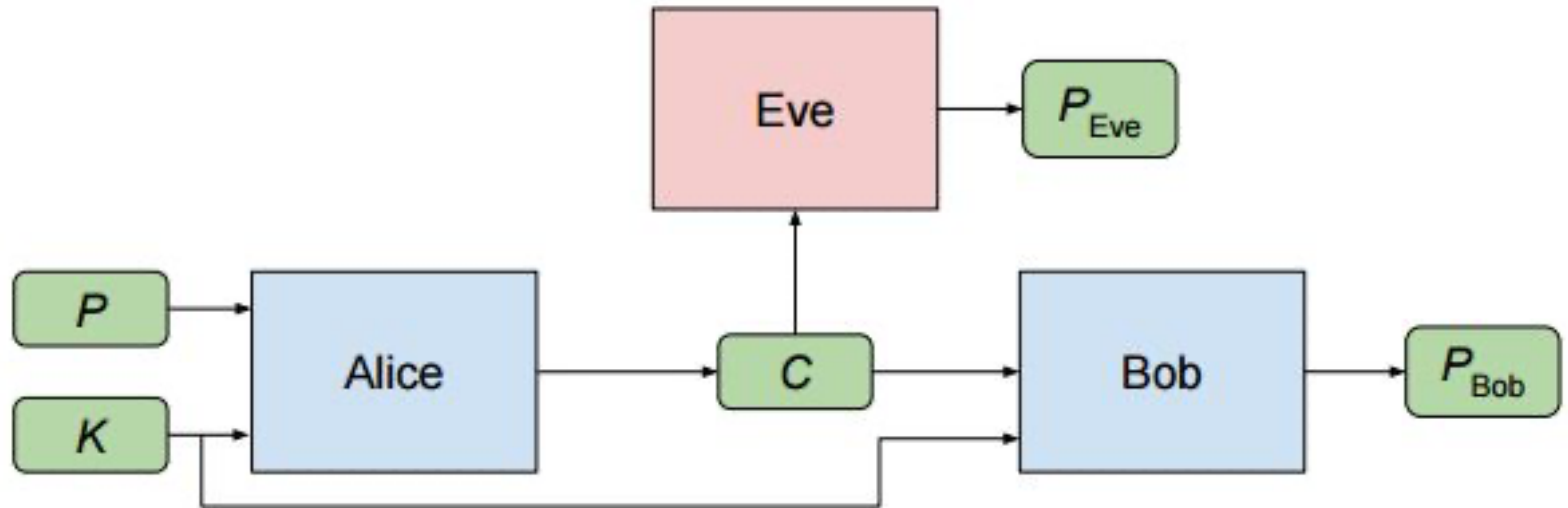
The dataset includes two randomly generated strings: plaintext data and associated keys.

This is done using uniform random distribution

The size of message is any one of the three : 16, 32 and 64.

The size of key is always the same as the message.

# Framework



# Neural Network Architecture

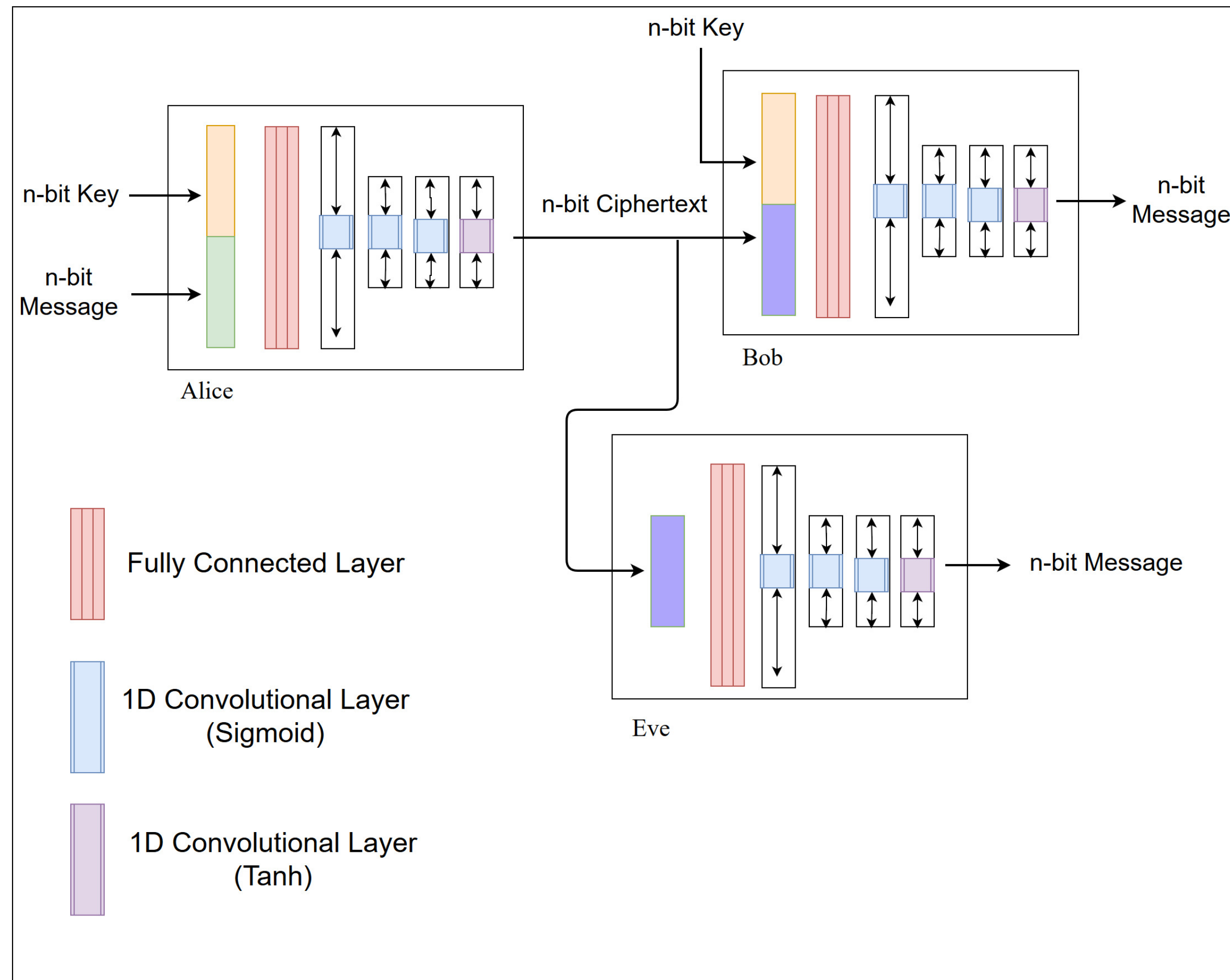
The project has a “mix and transform” type of architecture.

The first layer is a fully connected layer followed by 4 convolutional layers

These layers are responsible for learning to perform cryptographic operations.

Three of these are sigmoid and the last is a tanh layer.

# Network Architecture

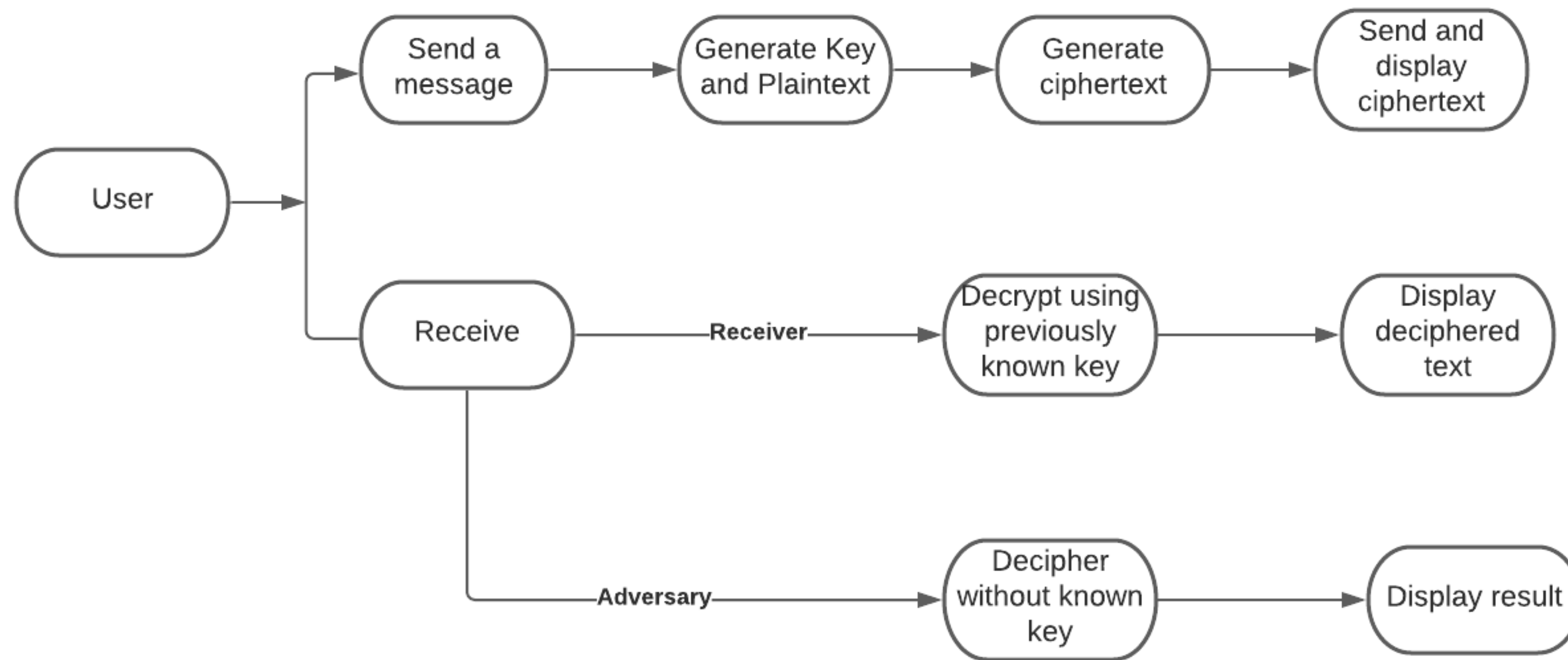


The proposed system has three neural networks that have similar architecture from a neural standpoint.

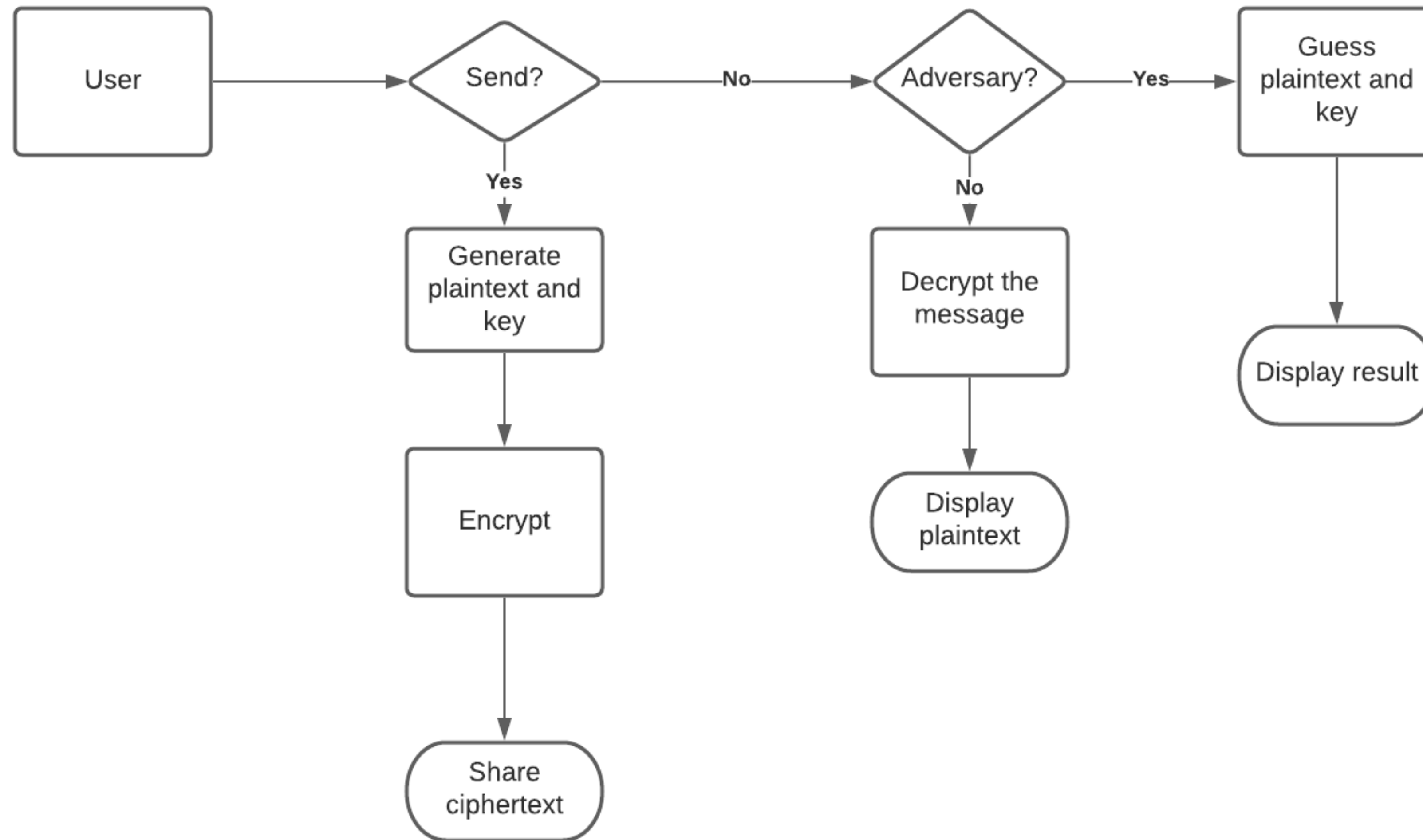
They consist of a fully connected layer followed by 3 convolutional layer (sigmoid) and a non linear tanh layer.



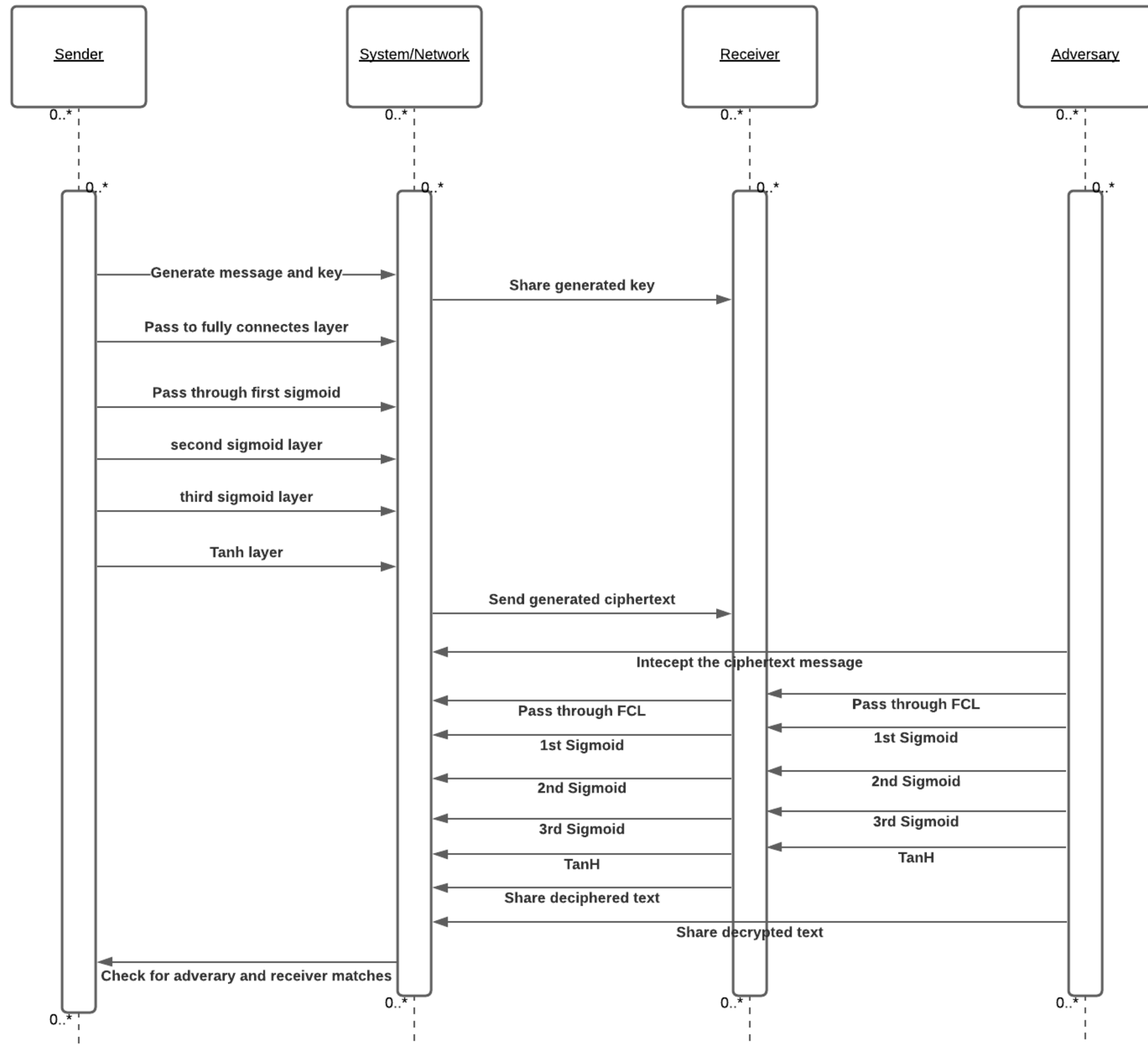
# Network Structure



# Data flow Diagram



# Sequence Diagram



# Training

- The proposed model has three loss functions -
  - Bob
  - Eve
  - The network
- The loss functions of Eve and Bob will be setup to maximise their encryption and decryption capabilities by minimising their reconstruction errors.
- The network denotes the loss function that will regulate the values of the loss functions of Bob and Eve. The aim of this is to minimise the reconstruction error of Bob while maximising the same for the adversary Eve.
- The network loss function will take into account two things :
  - The communication between Alice and Bob
  - Eve's reconstruction score
- The more accurate Eve's reconstruction becomes, the more the value of loss between Alice and Bob increases.

# Advantages

Successfully mitigates cyber attacks like:

- Man-in-the-middle

- Probabilistic attacks

Exceedingly difficult to crack without prior knowledge of implementation.

A system based on ANN allows bits to fluctuate and yet produce the desired output.

Due to its implementation being through machine learning, it is tolerant towards noise. Most messages cannot be modified by even a single bit with standard encryption schemes. A neural network-based system allows the encoded message to be varied and still accurate.

# Future Scope

Practical implementations for everyday applications are possible with a few tweaks and advancements of the near future.

While this project focuses on symmetric encryption, use of ANN in the already powerful and tough asymmetric algorithms will increase their security exponentially.



# References

Taehyuk Kim, Tae Young Yuon, Doocho Choi - Deep Neural Networks based Key Concealment Scheme, Nov. 4 2020.

Dylan Modesitt, Tim Henry, Jon Coden and Rachel Lathe - Neural Cryptography : From Symmetric Encryption to Steganography, 2018

Abadi, M Anderson, Learning to Protect Connections with Adversarial Neural Cryptography, Oct. 24, 2016.