DYP DR. D. Y. PATIL INSTITUTE OF ENGINEERING, MANAGEMENT AND RESEARCH	**Dr. D. Y. Patil Pratishthan's** **Dr. D. Y. Patil Institute of Engineering, Management& Research** **Department of Computer EngineeringA.Y: 2021-22**	**Group ID: 22** **Domain of Project: Cyber Security** **Type of Project: Internal**

Title of Project: Neural Cryptography.
Students Name: Sanket Halake, Prasann Shimpi, Shivam Dharamshetti, Shashank Singh.
Project Guide: Dr. Amol Dhakne

ABSTRACT:

The goal of cryptography is to make it impossible to take a cipher and reproduce the original plain text without the proper key. With good cryptography, your messages are encrypted in such a way that brute force attacks against the algorithm or key are almost impossible. 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.

PROBLEM STATEMENT:

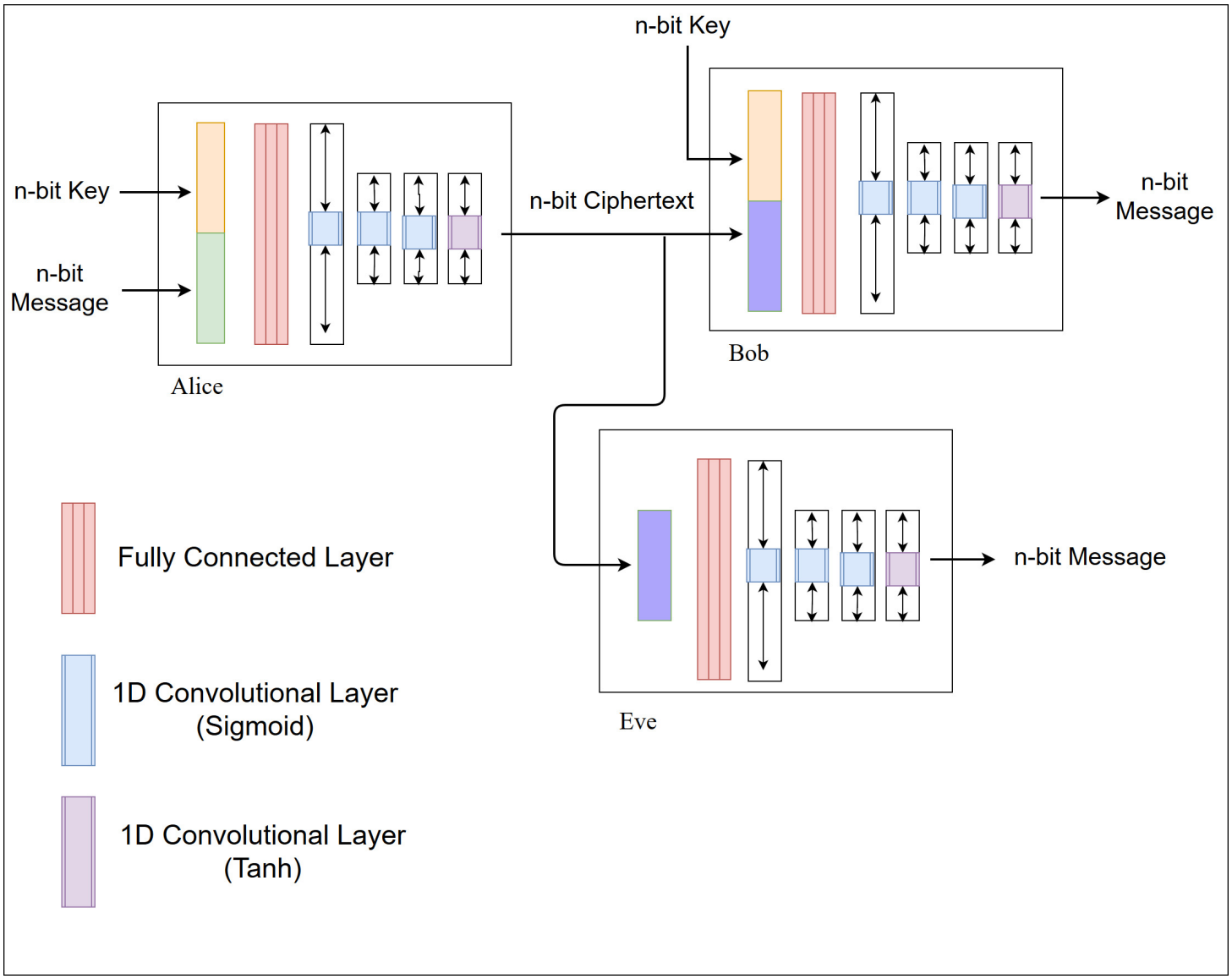
- During this modern era, the number of attacks and malicious actions online are increasing day by day, leading to identity frauds and ransoms. The domain of cyber security is based on the CIA triad, of which Confidentiality is considered of utmost importance.
- Today, we live in a data-driven world, and in most use cases, businesses collect and store sensitive personal and non-personal information, which can be exploited by cyber criminals.
- 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.

ARCHITECTURE DIAGRAM/SYSTEM MODEL:



METHODOLOGY/ PROJECT DESCRIPTION/ALGORITHM:

Alice, Bob and Eve are neural networks trained on adversaries in the form of alternating Alice / Bob and Eve training. Alice is given a plain text, P, and a key, K, and is asked to generate a ciphertext, C. Bob is asked to decrypt that C into a P if given K. He is asked to Eva to do the same without K. The specific training plan, the stall functions, can be found in the code.

In an attempt to learn more standardized symmetric key encryption operations like OneTime Pad, we created a network architecture that is localized to be by elements, or "by bits," between inputs.

SOFTWARE & HARDWARE REQUIREMENTS

Python libraries for Machine Learning

- tensorboard
- tensorflow
- matplotlib
- numpy
- flask
- scipy

CONCLUSION:

Applying the neural network is one way to advance good crypto, but we can ask questions. What are the limits of the system? The limitations of this type of system are minor, but potentially significant. This is effectively a secret key system where the key is the weights and the architecture of the network. With weights and architecture breaking down, encryption becomes trivial. However, both weights and architecture are required for encryption and decryption. Knowing just one thing or another is not enough to break it. What are the advantages of this system? The advantages of this system are that, as shown above, it seems extremely difficult without knowing the methodology behind it. It is also tolerant of noise. Most messages cannot be changed even one bit in a standard encryption scheme. The neural network-based system allows the encoded message to vary and remain accurate.