Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

ENCRYPTION AND DECRYPTION ALGORITHM BASED ON NEURAL NETWORK

KADIYARAPU PAPAYAMMA[1], B RAVI TEJA REDDY[2], T YESWANTH REDDY[3], G CHANDRA MOULI[4], B V HRUSHIKESH SAI[5]

[1] KADIYARAPU PAPAYAMMA, ASSISTANT PROFESSOR CSC & CSO DEPT, RAGHU INSTITUTE OF TECHNOLOGY , DAKAMARRI, VISAKHAPATNAM, ANDHRA PRADESH
Email:- tejaswinipadma@gmail.com
[2] B RAVI TEJA REDDY STUDENT OF B TECH, RAGHU INSTITUTE OF TECHNOLOGY , DAKAMARRI, VISAKHAPATNAM, ANDHRA PRADESH
Email:- ravitejareddy.bora@gmail.com
[3] T YESWANTH REDDY STUDENT OF B TECH , RAGHU INSTITUTE OF TECHNOLOGY , DAKAMARRI, VISAKHAPATNAM, ANDHRA PRADESH
Email:- reddyyeswanth92@gmail.com
[4] G CHANDRA MOULI STUDENT OF B TECH , RAGHU INSTITUTE OF TECHNOLOGY , DAKAMARRI, VISAKHAPATNAM, ANDHRA PRADESH
Email:- mouligaganam@gmail.com
[5] B V HRUSHIKESH SAI STUDENT OF B TECH , RAGHU INSTITUTE OF TECHNOLOGY , DAKAMARRI, VISAKHAPATNAM, ANDHRA PRADESH
Email:- hrushikesh11584@gmail.com

ABSTRACT

Cryptography is used to prevent the plain text of a cipher from being decrypted without the accompanying key. Security in network communication is of utmost importance. The two basic parts of cryptography—encryption and decryption—allow for the transmission of confidential and private data over unsecure networks. For the purpose of preventing misuse, data must be concealed from users who are not authorized. This is the main idea of cryptography.If you employ strong cryptography, it is almost impossible to use brute force to break the algorithm or the key. Very long keys and encryption algorithms that are resistant to other types of attack are essential components of good cryptography. The neural net application represents the next level in good cryptography. Neural nets have applications in cryptography and can be quite helpful. The use of neural networks for this purpose is covered in this paper. In this study, plain text and keys will be used to train a neural network for encryption and decryption. This project also consists of an experimental demonstration.

KEYWORDS:- cryptography, neural networks, encrypt, decrypt

1 INTRODUCTION

The word cryptography comes from the Greek word kryptos, which meaning secret or concealed. It is a method for secure communication when dealing with insecure third parties. It is an area of computer science and mathematics that deals with the science and practice of information concealing. Data encryption and decryption are also involved. Additionally, it makes it possible to communicate data securely over unreliable networks. Decryption is the opposite of encryption, which is the process of applying a key to plain text to transform it into encrypted text. There are essentially two sorts of cryptography models. Asymmetric and symmetric models are the two types. cryptography Encryption and decryption are two methods used in the science of data concealment via insecure networks: encryption transforms plain text into cipher text, and decryption transforms cipher text back into plain text.
Public Key Encryption: It is a cryptosystem that makes use of the asymmetric cryptography model [2]. Since everyone on the network is aware of the public key used here to encrypt plain text, it is sometimes referred to as a shared key [1]. In public key cryptography, decryption

of cipher text is accomplished with a private key only; that is, only the recipient who possesses the corresponding private key can decrypt the message. A secret key is a private key. known to the respective users and is hidden from others in the network.

A cryptography system that uses the symmetric cryptography model is called private key cryptography. This uses a private secret key for encryption of plain text and the same secret key for decryption of ciphered material [5]. A shared secret key is one that is utilized in both encryption and decryption, like in this instance. The shared key that is being used here is exclusive to this session and is only shared with the sender and the recipient.

2. LITERATURE SURVEY AND RELATED WORK

Security has various facets and uses, from safe online shopping and payment processing to password protection and private messaging. Cryptography is a crucial component of secure communications. The science and practice of writing in secret code is known as cryptography, and it was first used in writing around 1900 B.C. when an Egyptian scribe employed non-standard hieroglyphs in an inscription. Some academics argue that cryptography developed on its own at some point after the invention of writing.

with uses spanning from military plans for times of war to diplomatic messages. Thus, it should come as no surprise that new applications of cryptography emerged shortly after computer communications became widely used. Cryptography is required in data and telecommunications when exchanging information via any untrusted media, which encompasses almost all networks, most notably the Internet. Thus, cryptography can be used for user authentication in addition to safeguarding data against loss or alteration. These objectives are generally achieved by three different types of cryptographic systems, each of which is explained below: hash functions, public-key cryptography, and secret key cryptography, also known as symmetric cryptography. The original, unencrypted data is always referred to as plaintext. It is converted into cipher text by encryption, which will then (typically)

2.1 Types of Cryptographic Algorithms:

Cryptographic algorithms are classified in a variety of ways. They will be divided into groups here according to the quantity of keys used for both encryption and decryption. There are three categories of algorithms:

Secret Key Cryptography: In secret key cryptography, encryption and decryption are done using the same key. The sender encrypts the plaintext using the key (or a set of rules), as depicted in the image, and then transmits the cipher text to the recipient. The message is decrypted and the plaintext is recovered by the recipient using the same key (or set of rules). Symmetric encryption is another name for secret key cryptography since only one key is needed for both operations.

2.2 Public Key Encryption –

Some claim that the most important new discovery in cryptography in the last 300–400 years is public-key cryptography. In 1976, Whitfield, a doctoral student, and Stanford University professor Martin Hellman published the first public description of modern PKC. In order to facilitate secure communication over an insecure communications channel, the authors of the study presented a two-key cryptosystem that eliminates the need for secret key sharing. One of the keys in PKC is called the public key, and its owner is free to distribute it as widely as they choose. The other key is kept secret and is referred to as the private key. Submitting messages with this system is simple.

2.3 Hash Functions –

In a sense, hash functions—also known as message digests and one-way encryption—are keyless algorithms. Rather, the plaintext is used to construct a fixed-length hash value that prevents the plaintext's length or contents from being recovered. Hash algorithms are commonly employed to generate a digital fingerprint of a file's contents, which is frequently utilized to verify that the file has not been modified by a virus or unauthorized user. Many operating systems also frequently use hash methods to secure passwords. Thus, hash functions offer an indicator of a file's integrity.

3 Methodology

Due to the possibility of complete cryptographic key compromise, software-based attacks (such as malware) can target cryptographic software. In this paper, we investigate key-insulated symmetric key cryptography as a potential defense against recurrent assaults on cryptographic software. Our proof of concept implementation demonstrates the feasibility of key insulated symmetric key cryptography in a Kernel-based Virtual Machine (KVM) environment.

4 PROPOSED WORK AND ALGORITHM

The ultimate objective is to enable the deciphering of a coded communication without the need for a Key. Symmetric and asymmetric encryption algorithms are the two basic methods used. Both parties share the encryption and decryption keys in symmetric encryption. K represents the secret key that the sender used to build the message, and P stands for plain text. C is an acronym for ciphered or encrypted text. Neural networks are useful for deep learning, machine learning, and artificial intelligence because they can simulate how the human brain operates. Neural networks, also referred to as simulated neural networks (SNNs) or artificial neural networks (ANNs), are the foundation of deep learning techniques.

Their name and structure are also inspired by the human brain, as they mimic the communication patterns of actual neurons.The goal of this research is to create a reliable technique for properly predicting heart disease, specifically coronary artery disease or coronary heart disease.

4.1 Required steps can be summarized as follows:

1) A larger and more trustworthy dataset is created by combining five datasets.

2) Based on rank values in medical references, two selection techniques—Relief and LASSO—are used to extract the most pertinent features. This also aids in addressing machine learning's overfitting and underfitting issues.

3) In addition, a number of hybrid techniques are used to decrease execution time and increase testing frequency, such as boosting and bagging.

4) The effectiveness of the various models is assessed using the overall outcomes with the features that were chosen for All, Relief, and LASSO.

.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

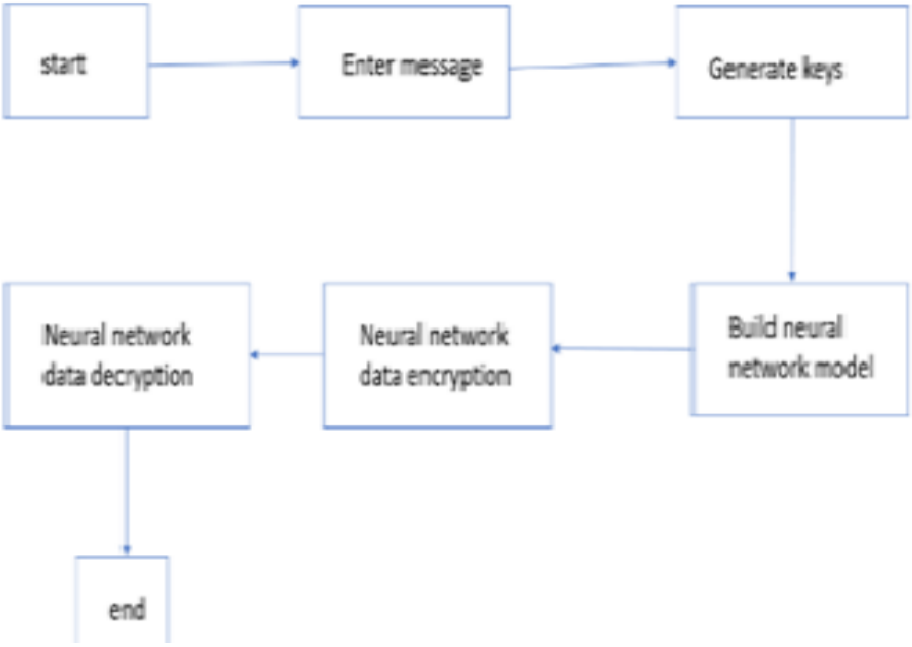

FIG 1:- PROPOSED MODEL FOR ENCRYPTION AND DECRYPTION

4.2 Algorithm:-

Three types of network architectures exist:

1. Single-layer feed forward networks: In this layer, a source node serves as the input layer and produces a neuron as the output. This kind of network called feed forward.

2. Multilayer feed forward networks: These networks only have an additional layer, referred to as a hidden layer. A greater level of statistic is obtained as a result of this concealed layer.

3. Recurrent Network: There is at least one feedback loop in this network. This loop boosts a neuron's capacity for learning by feeding its output back into its own input. Additionally, it improves performance.

2. BACKPROPAGATION

A feed forward network with only one layer has a lot of restrictions. Therefore, backpropagation is used to lower the mistakes. By back-propagating the errors of the output layer's units, the errors for the concealed layer's units are found. Backpropagation learning rule is used in this technique. It is also possible to think of it as a multilayer function delta rule generalization. The information processing paradigm known as an Artificial Neural Network (ANN) is modeled after the way biological nervous systems, like the brain, handle information. The information processing system's structure is the fundamental component of this paradigm. It is made up of several densely interconnected processing units, or neurons, that cooperate to solve particular issues. ANNs take after humans in learning. learn by example. An ANN is configured for a specific application, such as pattern recognition or data classification, through a learning process. Learning in biological systems involves adjustments to the synaptic connections that exist between the neurones. This is trueof ANNs as well.

4.3 Generalized Delta Rule –

1. δ's are calculated for each unit in the network using this formula. For feed-forward networks made up of non-linear units, this generalized delta rule applies.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

To achieve these objectives, three different kinds of cryptographic algorithms are employed:

2. Secret key cryptography: In secret key cryptography, encryption and decryption are accomplished with a single key. The sender encrypts the plaintext using the key (or a set of rules), as depicted in the image, and then transmits the cipher text to the recipient. In order to decrypt the message and retrieve the plaintext, the recipient uses the same key (or ruleset). Symmetric encryption is another name for secret key cryptography since only one key is needed for both operations.

2. Public-key cryptography: This is a two-key cryptosystem that eliminates the need for two parties to share a secret key in order to conduct secure communication across an insecure communications channel. One of the keys in PKC is called the public key, and its owner is free to distribute it as widely as they choose. The other key is kept secret and is referred to as the private key. Submitting messages with this system is simple.

3)hasing

In a sense, hash functions—also known as message digests and one-way encryption—are keyless algorithms. Rather, the plaintext is used to construct a fixed-length hash value that prevents the plaintext's length or contents from being recovered. Hash algorithms are commonly employed to generate a digital fingerprint of a file's contents, which is frequently utilized to verify that the file has not been modified by a virus or unauthorized user. Many operating systems also frequently use hash methods to secure passwords. Thus, hash functions offer an indicator of a file's integrity.

DESIGN OF THE PROPOSED ANN-BASEDENCRYPTION SYSTEM

According to Garfinger (1998), there are four basic components to every working encryption scheme (see Figure 3:

• The message (also known as the plain text) that you want to encrypt.

• The encrypted message (also known as the cipher text).

• The algorithm used for encryption.

The key, or keys, that the encryption method uses

In this paper, we conducted an experimental study with using neural network in cryptography. Thus, it means

- to design the topology of the neural network;
- to design the method of training algorithm of theneural network;
- to design the training set for training.

Neural networks are a successful encryption and decryption algorithm in the field of cryptography. Then, both neural network adaptation parameters were included into cryptography keys. We employed backpropagation to adjust multilayer neural networks. Each neural network's topology is determined by its training datasets . The message is split into 6-bit data sets during the encryption process, and additional 6-bit sets are generated at the end of the encryption process. Thus, the following was the design of both systems: six units in the input

layer and 6 output and one layer. Although we also employed six units, the concealed layer does not have a set number of units. Symbol representations in binary format were used to train both networks. Within each training set, a sequence of plain text numbers is equivalent to the binary values of that sequence's ASCII code; a sequence of plain text letters is equivalent to the binary value of that sequence, which is 96 fewer than its ASCII code; a sequence of plain text punctuation symbols is equivalent to a binary value of the space ASCII code (e.g. 32); and a sequence of other plain text characters is equivalent to zero. The encrypted text is then a six-bit random chain.

The security for all encryption and decryption systems is based on a cryptographic key. The SIMPLE systems use a single key for both

encryption and decryption. The good systems use two keys. A message encrypted with one key can be decrypted only with the other key. If we use the neural network as encryption and also decryption algorithm, their keys have adapted neural networks´ parameters; which are their topologies (architecture) and their configurations (weight values on connections in the given order). Generally, each key is written as follow:

[Input, Hidden, Output, Weights from the Units of Input, Weights from the Units of Hidden]

where the number of input units is called Input, and the number of hidden units is called Hidden. The quantity of output units is called output;

Weights derived from input units are weight values that are derived in a predetermined order from input units to hidden units;

Weights originating from hidden units are weight values that are sent in a predetermined order from hidden units to output units.

Parameter values of both ANNs in our experimental study are the following:

- each input layer consists of 6 nodes, whichrepresents the 6-bit blocks;
- each hidden layer consists of 6 nodes;
- each output layer consists of 6 nodes, used to definethe decrypted output message;
- fully connected networks;
- a sigmoid activate function;
- a learning rate equals 0,3.

5 Implementation Steps

5.1 DATA SET

This study makes use of the revolution analytics data set to identify the cardio vascular dataset from Kaggle. 51149 legitimate transactions and 3312 fraudulent transactions make up the dataset. The train, valid, and test sets of the dataset are split up as follows: 60%, 20%, and 20%, respectively.

5.2**DATA PREPROCESSING**

Before selecting features, data preprocessing is done to ensure that the classification method is implemented as efficiently as possible. To prevent the classification algorithm from being biased toward the majority class, undersampling is done to balance the dataset. A dataset that is balanced is used to apply feature selection.

5.3 **FEATURE SELECTION**

Feature selection techniques are used to eliminate redundant, pointless, and unneeded attributes from a dataset that either don't improve the accuracy of a prediction model or could make it less accurate. This study employs seven feature selection strategies: Step forward selection, Recursive feature elimination, Person's correlation, Select-K-best, Feature Importance, Extra tress classifier, and Mutual Information.

4.**FEATURE IMPORTANCE**

A set of methods known as "feature importance" is used to score input characteristics into a predictive model, indicating the relative weight of each feature at the moment a prediction is made. The quantity of input features is decreased. This work uses an additional tree classifier from the decision tree to implement feature importance. While Random Forest and Extra Trees are similar in that they both create numerous trees and divide nodes using random subsets of characteristics, Extra Trees samples without replacement and divides nodes randomly. 6 6

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

6 RESULTS AND DISCUSSION

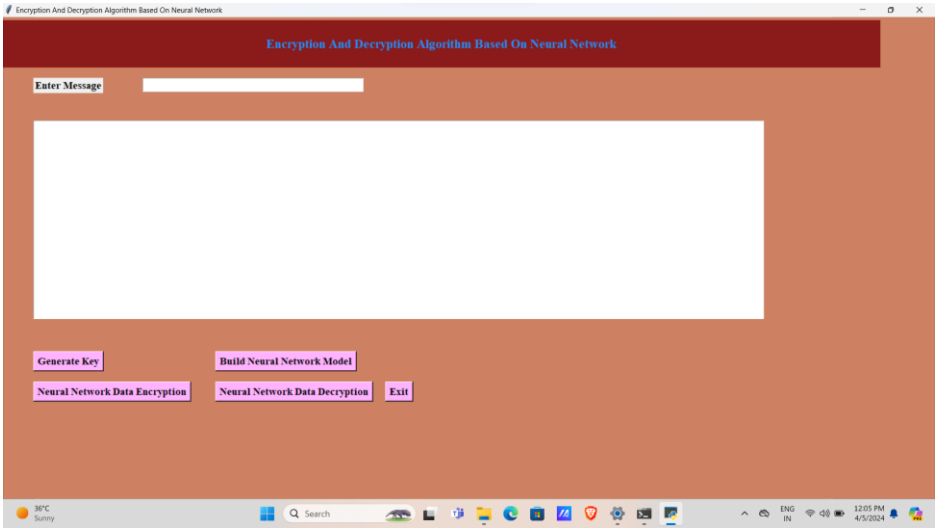

Fig 1: HOME SCREEN

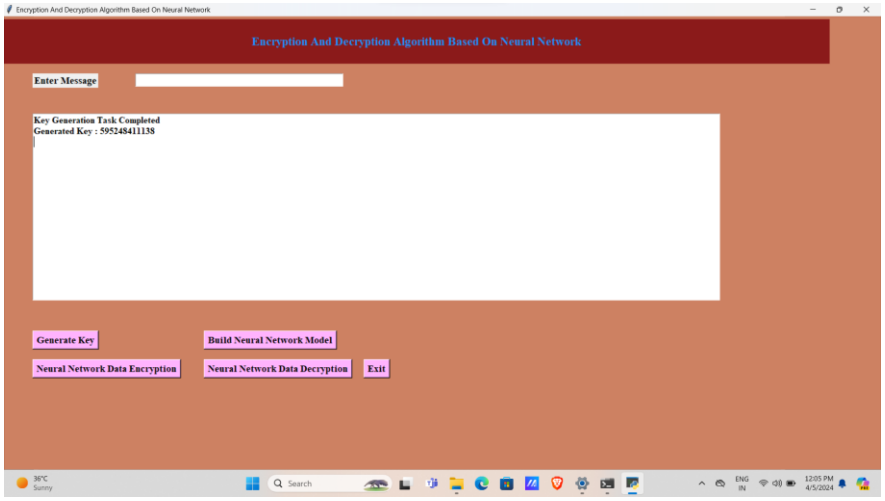

Fig 2: KEY GENERATED IN PAGE

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

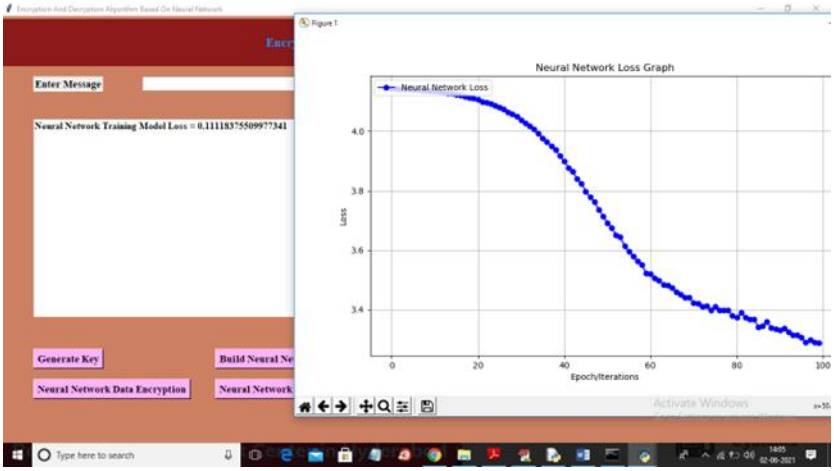

Fig 3: NEURAL NETWORK LOSS PAGE

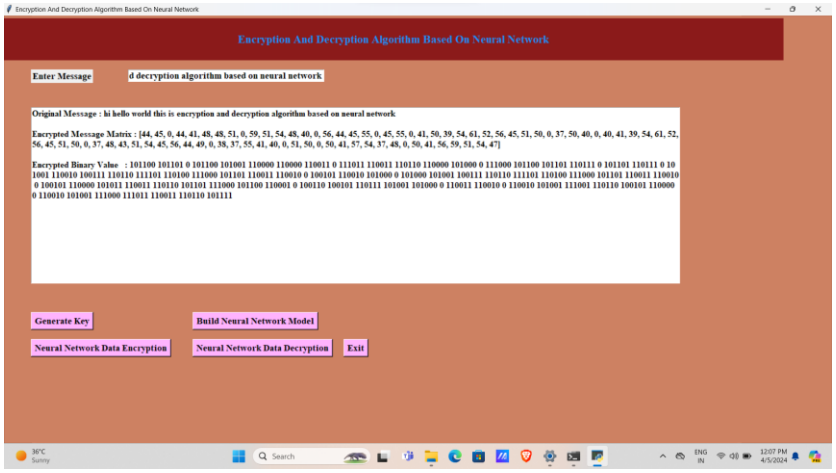

Fig 4: NEURAL ENCRYPTION OF DATA

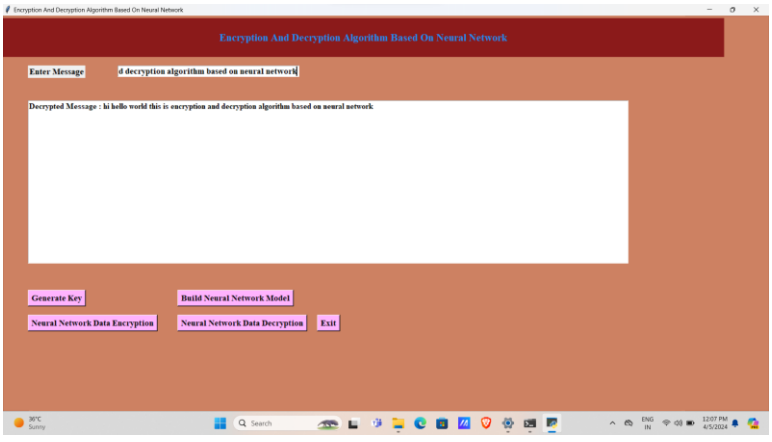

Fig 5: NEURAL DECRYPTION OF DATA

7.CONCLUSION AND FUTURE SCOPE

The idea of applying neural networks to the realm of cryptography is expanding quickly. The literature has a variety of neuro-crypto algorithms that researchers have proposed. However, the majority of them are restricted to cryptanalysis and key creation. In the study project, plain text is encrypted into a form that is completely different from the previous one using an auto associative memory network. The technique boasts faster encryption and decryption speeds and is relatively easy to implement. Because the technique uses a symmetric key scheme, key leaks are a possibility. To get around this, only reliable individuals should communicate, or a reliable third party might be utilized as an authority to stop the key leak.

.

Overall, the discussion has demonstrated that the performance of the various classifiers was adequate when compared to earlier research; nevertheless, there are a few drawbacks, such as the reliance on a particular feature selection technique, in this case, more reliance on Relief. to generate incredibly precise outcomes. Furthermore, a significant percentage of missing values in the dataset may be detrimental. Since we've shown how to solve the problem using the right techniques, if the missing value is quite large, other datasets used with this model also need to handle this problem. Additionally, even though our instruction

8 REFERENCES

[1] M. Hellman, "An overview of public key cryptography", IEEE Communications Magazine, 2002, 40(5): 42-49.

[2] Diffie W, Hellman M., "New Directions in Cryptography". IEEE Transactions on Information Theory. 1976, 22(6):644-654.

[3] L. P. Yee and L. C. D. Silva. Application of multilayer per- ceptron networks in public key cryptography. Proceedings ofIJCNN02,2 (Honolulu,HI,USA):1439–1443, May2002.

[4] Salomaa, Arto. Public-key cryptography. Springer Science & Business Media, 2013.

[5] Law, Laurie, et al. "An efficient protocol for authenticated key agreement."Designs, Codes and Cryptography 28.2 (2003): 119-134.

[6] McInnes, James L., and Benny Pinkas. "On the impossibility of private key cryptography with weakly random keys." Advances in CryptologyCRYPT0'90. Springer Berlin Heidelberg, 1991. 421-435.

[7] Dodis, Yevgeniy, et al. "Key-insulated symmetric key cryptography and mitigating attacks against cryptographic cloud software." Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. ACM, 2012.

[8] Jacob, Theju, and Wesley Snyder. "Learning rule for associative memory in recurrent neural networks." Neural Networks (IJCNN), 2015 International Joint Conference on. IEEE, 2015.