International Journal of Universal Science and Technology
ISSN: 2454-7263, Copyright@Universalprint
Volume: 01 No.: 02, Pages:85-98, Published: Dec.,2015
Web: www.universalprint.org , Publication: Universal Print
Title Key: Taxonomy of Changeover Ciphers Using Soft Computing.…

Taxonomy of Changeover Ciphers Using Soft Computing Tools

[1]Jawad Ahmad Dar
Department of Computer Science And Engineering,
Islamic University of Science And Technology Kashmir
Email: darjawad@rocketmail.com

[2]Mohd Rafiq
Department of Computer Science And Engineering,
Islamic University of Science And Technology Kashmir
Email: mrafiq7750@gmail.com

[3]Firdous ul Rashid
Department of Computer Science And Engineering,
Islamic University of Science And Technology Kashmir
Email: Firdousrashid378@yahoo.com

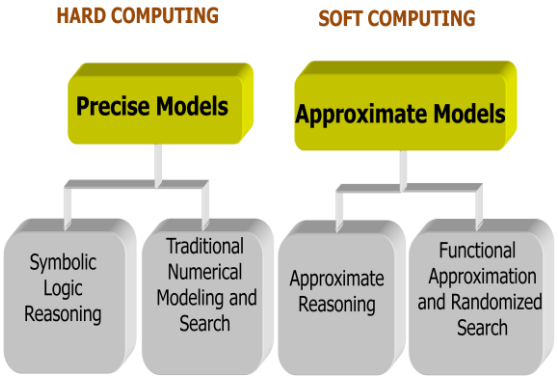
Abstract
Two Major problem-solving technologies include 1.Hard Computing 2.Soft Computing Hard computing deals with precise models where accurate solutions are achieved quickly. Soft computing is a relatively new concept; the term really entering general circulation in 1994.The term "soft computing" was introduced by professor Lotfi zadeh with the objective of exploring the tolerance for imprecision, uncertainty and partial truth to achieve tractability, robustness, low solution cost and better rapport with reality. Most of the time of a cryptanalyst is spent on finding the cipher technique used for encryption rather than the finding the key/ plaintext of the received cipher text. The Strength of the time-honored substitution cipher's success lie on the variety of characters engaged to represent a single character. More, the characters employed more the complication. Thus, in order to reduce the work of the cryptanalyst, neural network based identification is done based on the features of the cipher methods. In this paper, orthodox substitution ciphers, namely, Playfair, Vigenère and Hill ciphers are considered, More over we can take other ciphers as well like Railfence,Columnar transposition cipher, onetime pad etc and train the back propagation network accordingly. The features of the cipher methods under consideration were extracted and a back propagation neural network was trained. The network was experienced for haphazard texts with arbitrary keys of an assortment of lengths.

Subject Classification: Network Security and Cryptography

International Journal of Universal Science and Technology
ISSN: 2454-7263, Copyright@Universalprint
Volume: 01 No.: 02, Pages:85-98, Published: Dec.,2015
Web: www.universalprint.org , Publication: Universal Print
Title Key: Taxonomy of Changeover Ciphers Using Soft Computing.…

1. Introduction

Hard computing deals with precise models where accurate solutions are achieved quickly[1]. Soft computing is a relatively new concept, the term really entering general circulation in 1994.The term "soft computing" was introduced by professor Lotfi zadeh with the objective of exploring the tolerance for imprecision, uncertainty and partial truth to achieve tractability, robustness, low solution cost and better rapport with reality[1].Two major problem solving technologies include:1.Hard computing 2.Soft Computing as shown in fig 1



Encryption is a primary method of protecting valuable electronic information. Encryption is a process to transform a piece of information into an incomprehensible form. The input to the transformation is called plaintext (or clear text) and the output from it is called cipher text (or cryptogram). The reverse process of transforming cipher text into plaintext is called decryption (or decipherment). The encryption and decryption algorithms are collectively called cryptographic algorithms (cryptographic systems or cryptosystems). Both encryption and decryption processes are controlled by a cryptographic key, or keys. In a symmetric (or shared-key) cryptosystem, encryption and decryption use the same (or essentially the same) key; in an asymmetric (or public-key) cryptosystem, encryption and decryption use two different keys: an encryption key and a (matching) decryption key, and the encryption key can be made public (and hence is also called public key) without causing the matching decryption key being discovered (and thus a decryption key in a public-key cryptosystem is also called a private key).

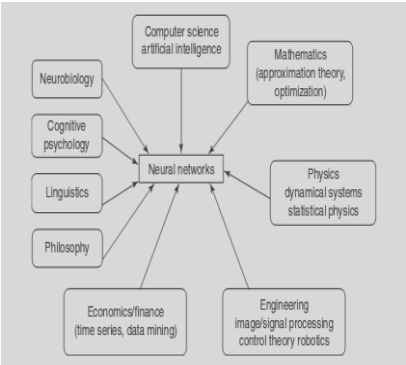
Various attacks on the cipher text are performed to identify the plaintext. The main problem of the cryptanalyst is to find the method employed and the encryption key used. Any encryption algorithm is breakable, but the real problem is that the cryptanalyst should

International Journal of Universal Science and Technology
ISSN: 2454-7263, Copyright@Universalprint
Volume: 01 No.: 02, Pages:85-98, Published: Dec.,2015
Web: www.universalprint.org , Publication: Universal Print
Title Key: Taxonomy of Changeover Ciphers Using Soft Computing.…

be able to break the cipher text within a given time frame, because after that time frame the information so obtained may be useless. Most of the useful time of cryptanalyst is shattered in finding the method or encryption algorithm. So if it is possible to recognize the encryption algorithm employed then the task of the cryptanalyst becomes easier.

2. Artificial neural networks

A neural network is a computational method inspired by studies of the brain and nervous systems in biological organisms. It is a Computing system made of a number of simple, highly interconnected processing elements, which process information by their dynamic state response to external input. Animals are able to react adaptively to changes in their external and internal environment, and they use their nervous system to perform these behaviors. An appropriate model/simulation of the nervous system should be able to produce similar responses and behaviors in artificial systems. The nervous system is build by relatively simple units, the neurons, so copying their behavior and functionality should be the solution. Neurons work by processing information. They receive and provide information in form of spikes. An artificial neural network is composed of many artificial neurons that are linked together according to specific network architecture. The objective of the neural network is to transform the inputs into meaningful outputs. An artificial neural network may contain an input layer, output layer and hidden layers (If necessary). The hidden layer may be employed if linear classification is not possible. Each layer consists of several neurons. A neuron is considered to be an adaptive element. Its weights are modifiable depending on the input signal it receives, its output value and the associated teacher response (if available). Thus the neuron will modify its weights based only on the input and/or output. One of the distinct strengths of neural networks is their ability to generalize. The network is said to generalize well when it sensibly interpolates input patterns that are new to the network. Fig 2 shows Multidisciplinary view of neural networks.



International Journal of Universal Science and Technology
ISSN: 2454-7263, Copyright@Universalprint
Volume: 01 No.: 02, Pages:85-98, Published: Dec.,2015
Web: www.universalprint.org , Publication: Universal Print
Title Key: Taxonomy of Changeover Ciphers Using Soft Computing.…

fig 2 Multidisciplinary view of neural networks.

3.Back –Propagation Network

The back-propagation learning algorithm is one of the most important developments in neural networks.This network has re-awakened the scientific and engineering community to the modeling and processing of nemerous quantitative phenomena using neural networks.This learning algorithm is applied to multilayer feed-forward networks consisting of processing elements with continuous differentiable activation functions.the networks associated with back propagation learning algorithm are also called back-propagation networks(BPN'S).The back-Propagation Algorithm is different from other networks in respect to the process by which the weights are calculated during the learning period of the network.The training of the BPN is done in three stages-The feed-forward of the input training pattern,the calculation and back-propagation of the error,and updation of weights.The testing of the BPN involves the computation of feed-forward phase only. The terminologies used in the flowchart and in the training algorithm are as follows:

x=input training vector($x_1,\ldots,x_i,\ldots,x_n$)

t=Target output vector($t_1\ldots,t_k,\ldots t_m$)

α =Learning rate Parameter

x_i=input unit i.

v_{0j}=bias on jth hidden unit

w_{0k}=bias on kth output unit

z_j=hidden unit j. the net input to Z_j is :-

$z_{inj} v_{0j} + \sum_{i=1}^{n} x_i v_{ij}$ and output is $z_j=f(z_{inj})$ y_k =output unit k,the net input to y_k is and the output is $y_k=f(y_{ink})$commonly used Activation functions are binary sigmoidal and bi polar sigmoidal activation functions.These functions are used in the BPN because of the following characteristics (1) Continuity (2) differentiability (3) nondecreasing monotony.range of the binary sigmoid is from 0 to 1,and for bipolar sigmoid it is from -1 to +1. The enhanced standard Back propagation algorithm [5] can train any network as long as its weights, net input and transfer functions have derivative functions. Here the weights are adjusted according to gradient descent.

$$\Delta w = -k \frac{\partial E}{\partial W} \qquad (1)$$

$$= n \frac{\partial E}{\partial W} \qquad (2)$$

International Journal of Universal Science and Technology
ISSN: 2454-7263, Copyright@Universalprint
Volume: 01 No.: 02, Pages:85-98, Published: Dec.,2015
Web: www.universalprint.org , Publication: Universal Print
Title Key: Taxonomy of Changeover Ciphers Using Soft Computing.…

where η is the learning rate , Δw is the weight change and E is the sum of squares of error
The problem with the standard gradient descent method is that it at times gets trapped into local minima, and hence variations were suggested. In Gradient descent algorithm with momentum, the weights are adjusted according to gradient descent. However some weightage is given to the previous weight change also.

$$\Delta W = \alpha \Delta W_{n-1} + n\left(1-\alpha\right)\frac{\partial E}{\partial W}$$

where α is the smoothing factor for applying the momentum and η is the learning rate.

4. Training Algorithm

The error back-propagation learning algorithm can be outlined in the following Algorithm.
Step 0:Initialize weights and learning rate.
Step 1:Perform Steps 2-9 when Stopping condition is false.
Step2:Perform Steps 3-8for each training pair.

Feed-forward phase(phase 1)

Step 3:Each input unit receives input signal x_i and sends it to the hidden unit(i=1 to n).
Step 4:Each Hidden unit Z_j(j=1 to p) sums its weighted input signals to calculate net input:

$$z_{inj} = v_{0j} + \sum_{i=1}^{n} x_i v_{ij}$$

Calculate output of the hidden unit by applying its activation functions over z_{inj}(binary or bipolar sigmoidal activation function)
$Z_j=f(z_{inj})$
and Sends the output signal from the hidden unit to the input of the output layer units.
Step 5:for each output unit y_k(k=1 to m),calculate the net input:

$$yink = wok + \sum_{j=1}^{p} z_j w_{jk}$$

and apply the activation function to compute output signal
$y_k=f(y_{ink})$.

Back-Propagation of error(Phase II)

Step 6: Each output unit y_k(k=1 to m) receives a target pattern corresponding to the input training pattern and computes the error correction term:

$$\delta_k = \left(t_k - y_k\right) f^{1}\left(y_{ink}\right)$$

On the basis of calculated error correction term, update and change in weights and bias:

International Journal of Universal Science and Technology
ISSN: 2454-7263, Copyright@Universalprint
Volume: 01 No.: 02, Pages:85-98, Published: Dec.,2015
Web: www.universalprint.org , Publication: Universal Print
Title Key: Taxonomy of Changeover Ciphers Using Soft Computing.…

$$\Delta w_{jk} = \alpha \delta_k Z_j; \quad \Delta w_{0k} = \alpha \delta_k$$

Sends δ_k to the hidden layer backwards.

Step 7: Each hidden unit(z_j,j=1 to p)sums its delta inputs from the output units:

$$\delta_{inj} = \sum_{k=1}^{m} \delta_k w_{jk}$$

The term δ_{inj} gets multiplied with derivative of f(z_{inj}) to calculate the error term:

$$\delta_j = \delta_{inj} f'\left(z_{inj}\right)$$

On the basis of the calculated δ_j ,update the change in weights and bias:

$$\Delta vij = \alpha \delta xi; \quad \Delta v_{0j} = \alpha \delta_j;$$

Weight and bias updation (Phase III):

Step 8: Each output unit(y_k,k=1 to m) updates the bias and weights:

$$w_{jk}(new) = w_{jk}(old) + \Delta w_{jk}$$

$$w_{0k}(new) = w_{0k}(old) + \Delta w_{0k}$$

Each hidden unit(z_j,j=1 to p) updates its bias and weights:

$$v_{ij}(new) = v_{ij}(old) + \Delta v_{ij}$$

$$v_{0j}(new) = v_{0j}(old) + \Delta v_{0j}$$

Step 9:Check for the stopping condition. The stopping condition may be certain number of epochs reached or when the actual output equals the target output.

5. Taxonomy of Changeover Ciphers using Back Propagation Network

1. Above algorithm is based on incremental approach for updation of weights i'e the weights are being changed immediately after a training pattern is presented.
2. When BPN is used as a classifier, it is equivalent to the optimal Bayesian discriminant function for asymptotically large sets of statistically independent training patterns.so we can use this network for analysis of different Substitution and Transposition Ciphers like Hill , Ceasar, Playfair ,Rail Fence,Columnar transposition for different plaintext parameters, cipher text parameters, key length and also for analysis of Cryptanalysis.
3. If BPN algorithm converges at all,then it may get struk with local minima and may be unable to find satisfactory solutions.

International Journal of Universal Science and Technology
ISSN: 2454-7263, Copyright@Universalprint
Volume: 01 No.: 02, Pages:85-98, Published: Dec.,2015
Web: www.universalprint.org , Publication: Universal Print
Title Key: Taxonomy of Changeover Ciphers Using Soft Computing.…

6. Back Propagation network for XOR function using Bipolar and Binary Targets (7 Epochs) [1].

Intial weights and bias are assumed to be of small random values
Floatv[2][4],w[4][1],vc[2][4],wc[4][1],de,del[4],bl,bia,bc[4],e=0;floatx[4][2],t[4],zin[4],delin[4], yin=0,y,dy,dz[4],b[4],z[4],es,alp=0.02; int i,j,k=0,itr=0; v[0][0]=0.1970; v[0][1]=0.3191; v[0][2]=0.1448;v[0][3]=0.3594;v[1][0]=0.3099;v[1][1]=0.1904; v[1][2]=-0.0347; v[1][3]=-0.4861;w[0][0]=0.4919; w[1][0]=-0.2913; w[2][0]=-0.3979; w[3][0]=0.3581; b[0]=-0.3378; b[1]=0.2771; b[2]=0.2859; b[3]=-0.3329; bl=-0.141; x[0][0]=-1; x[0][1]=-1; x[1][0]=-1; x[1][1]=1; x[2][0]=1; x[2][1]=-1; x[3][0]=1; x[3][1]=1; t[0]=0; t[1]=1; t[2]=1; t[3]=0;Implementation is shown in fig 3 in Turbo c/c++

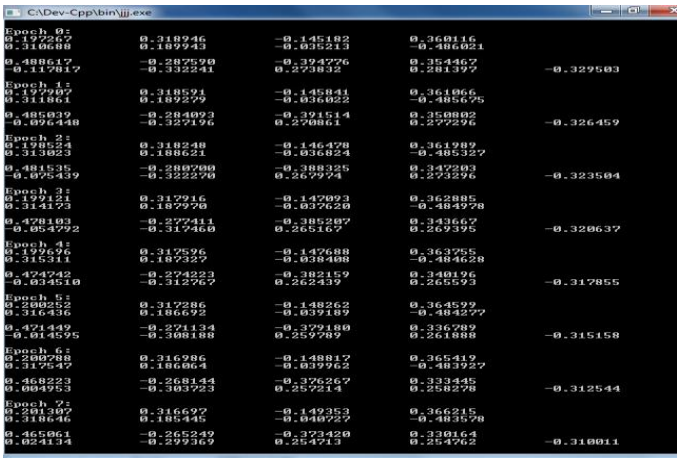


fig 3

7. Classical Ciphers

Most of the classical ciphers are substitution type. Each character may be represented by one (Caesar cipher) or many characters (Vigenère). Some of the ciphers are block ciphers, which converts one plaintext character block into one cipher character block[6]. The description of the ciphers used for identification in this paper are given below.

8. Playfair Ciphers

The Playfair cipher is a polygraphic cipher; it enciphers more than one letter at a time. The Playfair cipher enciphers digraphs – two-letter blocks. An attack by frequency analysis would involve analyzing the frequencies of the digraphs of plaintext. Complications also occur when digraph frequencies are considered because sometimes common plaintext digraphs are split between blocks. The playfair cipher has a password length of 25 characters. All the characters are involved in the key matrix which is 5 X 5 Matrix. Both I and J share the same space or it may be any other lower frequency character which is left out in

International Journal of Universal Science and Technology
ISSN: 2454-7263, Copyright@Universalprint
Volume: 01 No.: 02, Pages:85-98, Published: Dec.,2015
Web: www.universalprint.org , Publication: Universal Print
Title Key: Taxonomy of Changeover Ciphers Using Soft Computing.…

the matrix. The plaintext characters are encrypted into cipher text taking two characters at a time. The cipher text characters will be the intersection of row of the first plaintext character and the column of the second plaintext character and the second cipher text character will be the first plaintext character column and the second characters row. If the both plaintext characters are same then they are separated by a filler character, say "X". So, no two adjacent cipher text characters will be the same. If the plaintext characters are in the same row, the next characters in the same row after the plaintext characters are taken as cipher characters. The same applies for plaintext characters in the same column. The Playfair cipher is a simple example of a block cipher, since it takes two-letter blocks and encrypts them to two-letter blocks. A change of one letter of a plaintext pair will always change at least one letter, and usually both letters of the cipher text pair. However, blocks of two letters are too small to be secure, and frequency analysis, is usually successful.

The features of Playfair ciphers are

1. No two adjacent characters are identical
2. Only 25 alphabets will be used in the encryption process for the conversion of plaintext to cipher text.
3. The number of characters in the Plaintext is always even.
4. If "AB" is encrypted as "UH" then "BA" will be encrypted as "HU".
5. The plaintext character will not be represented by itself in the cipher text.

9. Hill Ciphers

Hill ciphers are asymmetric ciphers where one key is used for encryption and a second key (the key inverse) is used for decryption. The Hill cipher is a cryptosystem that enciphers blocks. Any block size may be selected, but it might be difficult to find good keys for enciphering large blocks. The advantage of having large blocks is that change of one character in a plaintext block may change potentially all the characters in the corresponding cipher text block. Hill cipher uses invertible matrices for encryption. An invertible matrix of sufficient order is used as key. The number of characters to be converted in each block depends on the order of the matrix. As the order of the matrix increases the diffusion property of the cryptosystem increases, but it is very difficult to find invertible matrices of higher order. Characters of the size of the order are selected and multiplied with the key matrix. The resulting matrix is operated on modulo 26 and the elements of this matrix now contain the cipher text. Hill cipher has more diffusion property which means that frequency statistics of letters, in a plaintext are diffused over several characters in the cipher text, and

International Journal of Universal Science and Technology
ISSN: 2454-7263, Copyright@Universalprint
Volume: 01 No.: 02, Pages:85-98, Published: Dec.,2015
Web: www.universalprint.org , Publication: Universal Print
Title Key: Taxonomy of Changeover Ciphers Using Soft Computing.…

hence much more cipher text is needed to do a meaningful statistical attack. The features of Hill Cipher are

1. Strong against Frequency analysis
2. All characters (A to Z) are employed for encryption and hence all the characters may be present in the cipher text.
3. Higher order keywords are very rare as it is difficult to find invertible matrices both of which contain integers only.
4. Higher diffusion property and increases with matrix order.

10. Vigenère ciphers

The Vigenère Cipher, proposed by Blaise de Vigenere from the court of Henry III of France in the sixteenth century, is a progressive poly alphabetic substitution method. The set of related mono alphabetic substitution rules makes use of 26 Caesar ciphers with shifts of 0 to 25.[6]The table used for encryption can be created for a simple alphabet from A to E, which can be extended to all letters from A to Z .Each row in a table can be created by a simple shift of the previous row. Thus a vigenere cipher of password one can be considered as a Caesar cipher as this involves only one shift of the alphabets and thus forming a Caesar cipher

Table 1 – vigenere table for alphabet A to E

Plaintext / key	**A**	**B**	**C**	**D**	**E**
A	**A**	**B**	**C**	**D**	**E**
B	**B**	**C**	**D**	**E**	**A**
C	**C**	**D**	**E**	**A**	**B**
D	**D**	**E**	**A**	**B**	**C**
E	**E**	**A**	**B**	**C**	**D**

To derive the cipher text using the table, for each letter in the plaintext, one finds the intersection of the row given by the corresponding keyword letter and the column given by the plaintext letter itself. It can be modeled mathematically as, **C = (P+K)** % **26** Where C is the cipher text letter and P, K are plain text and key letters. Decipherment of an encrypted message is equally straightforward This time one uses the keyword letter to pick a row of the table and then traces down the row to the column containing the cipher text letter. The

International Journal of Universal Science and Technology
ISSN: 2454-7263, Copyright@Universalprint
Volume: 01 No.: 02, Pages:85-98, Published: Dec.,2015
Web: www.universalprint.org , Publication: Universal Print
Title Key: Taxonomy of Changeover Ciphers Using Soft Computing.…

index of that column is the plaintext letter. It can be modeled mathematically as, **P = (C-K) % 26**

The Features of Vigenère Ciphers are

1. Since this method employs 26 Caesar ciphers, each character may be represented in 26 different ways and each character may be used to represent 26 characters.
2. Kasiski's technique for finding the length of the keyword was based on measuring the distance between repeated bi grams in the cipher text and can be used to find the length of keyword.
3. If the keylength is "n" then every character at (n+m)th character (m < n)will follow the same column and hence each can be treated as individual Caesar ciphers. Thus we will have "n" Caesar ciphers.

11. Research and Results

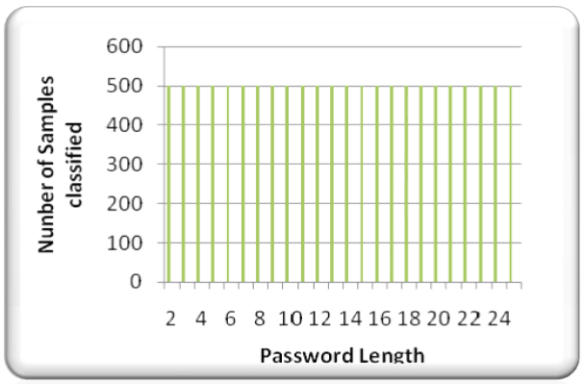
11.1 Training of network

The facial appearances of the ciphers under contemplation were extracted and a back propagation neural network was trained. For 500, 750,900 samples of500 bits,750 ,1 Kb were taken for training Back propagation network so designed had 3 layers including a hiddenlayer. Tan sigmoidal and log sigmoidal learning rules were adopted.

11.2 Testing the network

The network was experienced for different type of input ciphers and the a mixture of conditions that were considered are

1. dissimilar Password length and same Plaintext
2. similar Password and diverse Cipher texts
3. dissimilar Password length and Different Plaintext



International Journal of Universal Science and Technology
ISSN: 2454-7263, Copyright@Universalprint
Volume: 01 No.: 02, Pages:85-98, Published: Dec.,2015
Web: www.universalprint.org , Publication: Universal Print
Title Key: Taxonomy of Changeover Ciphers Using Soft Computing.…

Figure 4 Results of Playfair for different Plaintext encrypted with different password lengths

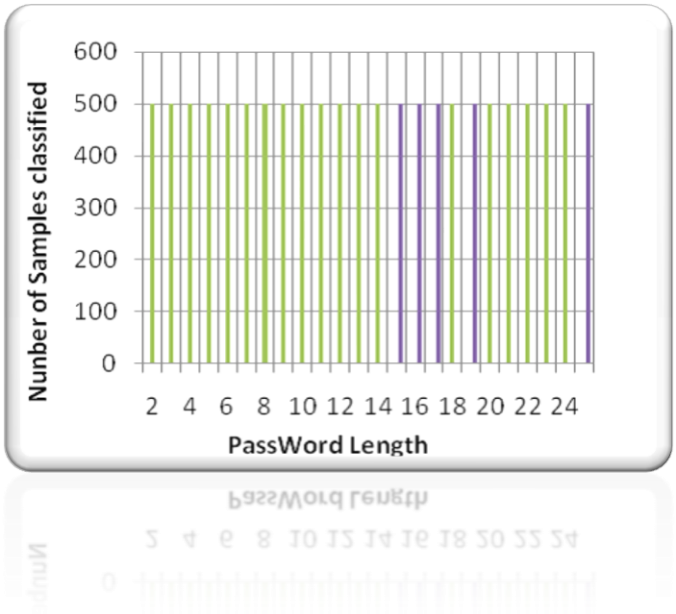


Figure 5 Results of Vigenère for different Plaintext encrypted with different password lengths

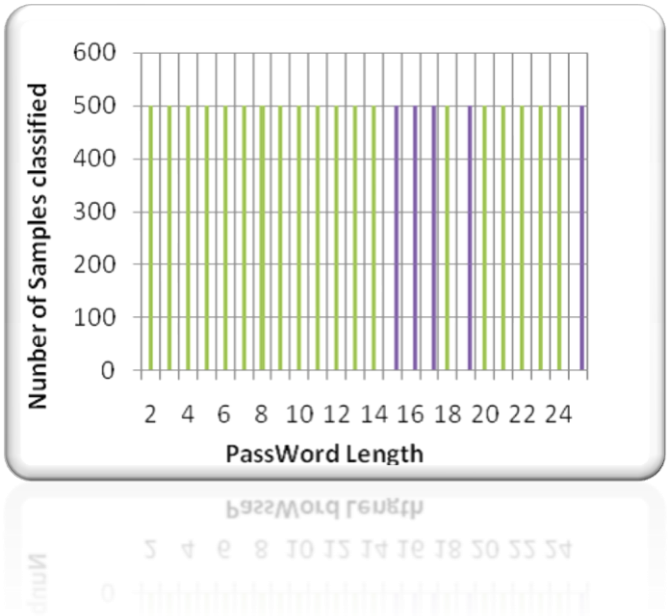
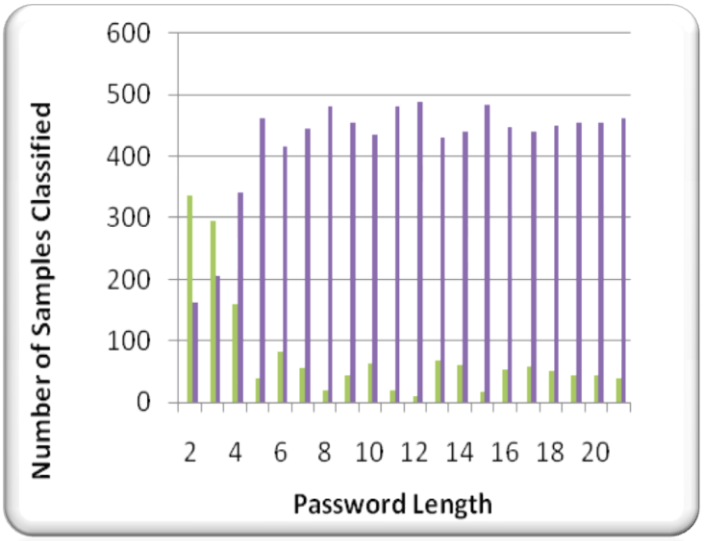


Figure 6 Results of Hill Cipher for different Plaintext encrypted with different password lengths

International Journal of Universal Science and Technology
ISSN: 2454-7263, Copyright@Universalprint
Volume: 01 No.: 02, Pages:85-98, Published: Dec.,2015
Web: www.universalprint.org , Publication: Universal Print
Title Key: Taxonomy of Changeover Ciphers Using Soft Computing.…



11. Conclusion

Discovery of orthodox changeover ciphers like one time pad, Playfair cipher, Vigenère cipher and Hill cipher, also transposition ciphers were identifiedlike columnar transposition,Railfence was attempted using neural networks. Some of the facial appearance like adjacent duplicates and their occurrence of duplication were used to identify the encryption process.Hence the sensation rate of different ciphers was identified.

References

[1] Principles of Soft Computing S.N Sivanandam,S.N Deepa Wiley 2nd Edition.

[2] Pooja Maheswari "Classification of ciphers", Indian Institute of Technology, Kanpur , 2001

[3] Sreenivasulu Nagireddy "A Pattern recognition approach to block cipher identification" Indian Institute of Technology, Chennai , 2008

[4] B.Chandra and P.Paul Varghese, "Application of cascade correlation Neural Network for cipher system Identification", World Academy of Science, engineering and technology 262007

[5] D. E. Rumelhart; G. E. Hinton and R. J. Williams; "Learning internal representations by error propagation", Parallel Data Processing, Vol.1, Chapter 8, the M.I.T. Press, Cambridge, MA, 1986, pp. 318-362.

International Journal of Universal Science and Technology
ISSN: 2454-7263, Copyright@Universalprint
Volume: 01 No.: 02, Pages:85-98, Published: Dec.,2015
Web: www.universalprint.org , Publication: Universal Print
Title Key: Taxonomy of Changeover Ciphers Using Soft Computing.…

[6] William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall. 2006.
[7] Reinhard Wobst, "Cryptology Unlocked", John Wiley and sons ,2007
[8] Jawadahmaddar,"Humanizing the Security of Rail Fence Cipher Using Double Transposition and Substitution Techniques, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064,Volume 3 Issue 9, September 2014.
[9] William Stallings, Cryptography and Network Securit Principles and Practice. Second edition, Pearson Education.
[10] AtulKahate (2009), Cryptography and Network Security, second edition, McGraw-Hill
[11] William Stalling "Network Security Essentials(Applications and Standards)",Pearson Education,2004
[12] practicalcryptography.com/ciphers/rail-fence-cipher/
[13] Johannes A.Buchmann, Introduction to Cryptography .Second Edition, Springer – Verlag NY, LLC,2001.
[14] Shiv Shakti Srivastava, Nitin Gupta."A Novel Approach to Security using Extended Playfair Cipher" International Journal of Computer Applications (0975 – 8887) Volume 20– No.6, April 2011
[15] Charles P.Pfleeger "Security in Computing", 4th edition, Pearson Education
[16] Neal R. Wagner "The Laws of Cryptography: Perfect Cryptography: The One-Time Pad "
[17] jawad ahmaddar,sandeepSharma" Implementation of One Time Pad cipher with Rail Fence and Simple Columnar Transposition Cipher, for Achieving Data security,,International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064,Volume 3 Issue 11, November 2014
[18] jawadahmaddar,Enhancing the data security of simple columnar transposition cipher by Caesar cipher and Rail fence cipher technique. International Journal of Computer Science & Engineering Technology (IJCSET), ISSN : 2229-3345 Vol. 5 No. 11 Nov 2014
[19] Behrouz A. Forouzan, Cryptography and Network Security. Special Indian Edition, The McGraw- Hill companies, New Delhi,2007.
[20] Dhiren R.Patel, Information Security Theory and Practice. First Edition, Prentice-Hall of India Private Limited, 2007
[21] Mohit Kumar, Reena Mishra, Rakesh Kumar Pandey and Poonam Singh "Comparing Classical Encryption With Modern Techniques"in proceedings of S-JPSET, Vol. 1, Issue 1,2010.

International Journal of Universal Science and Technology
ISSN: 2454-7263, Copyright@Universalprint
Volume: 01 No.: 02, Pages:85-98, Published: Dec.,2015
Web: www.universalprint.org , Publication: Universal Print
Title Key: Taxonomy of Changeover Ciphers Using Soft Computing.…

[22] Packirisamy Murali and Gandhidoss Senthilkumar, Modified version of Playfair cipher using Linear Feedback Shift Cipher, International Conference on Information Management and Engineering ICIME,pp.488-490,2009.

[23] Shiv Shakti Srivastava, Nitin Gupta and Rajaram jaiswal "Modified Version of Playfair Cipher by using 8x8 Matrix and Random Number Generation" in Proceedings of IEEE 3rd International Conference on Computer Modeling and Simulation (ICCMS 2011), Mumbai, pages 615-617, January, 2011.

[24] Andrew S. Tanenbaum, Networks Computer, 5th edition, Pearson Education, ISBN-10: 0132553171.

[25] Aftab Alam, Sehat Ullah, Ishtiaq Wahid, & Shah Khalid, "Universal Playfair Cipher Using MXN Matrix". International Jourrnal of Advanced Computer Science, Vol.1, No.3, Pp.113-117, Sep.2011.

[26] Ravindra Babu K, S.Uday Kumar, A. Vinay Babu, I.V.N.S. Aditya, P.Komuraiah, "An Extension to Traditional Playfair Cryptographic Method". International Journal of Computer Applications (0975 – 8887), Volume 17- No.5, March 2011.

[27] Muhammad Salam, Nasir Rashid, Shah Khalid, Muhammad Raees Khan, "A NXM Version of 5X5 Playfair Cipher for any Natural Language (Urdu as Special Case)". World Academy of Science, Engineering and Technology 73 2011.

[28] S.S.Dhenakaran,, M. IlayarajaExtension of Playfair Cipher using 16X16 Matrix, International Journal of Computer Applications (0975 – 888) Volume 48– No.7, June 2012

[29] Dhiren R.Patel, Information Security Theory and Practice. First Edition, Prentice-Hall of India Private Limited, 2008.

[30] Keith Harrison, Bill Munro and Tim Spiller, Security through uncertainty. P Laboratories, February, 2007.

[31] W. Diffie and M. E. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, pp: 644 654, http://citeseer.ist.psu.edu/340126.html.