International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 4, Special Issue 3 (March '2018)
Proceeding of - National Conference on Recent Trends in Information Technology and Communication,
Conference held at Velammal Engineering College,Chennai,India.

AUTO DETECTION OF CIPHER TEXT AND MODIFIED AES ALGORITHM

S. Nirmal kumar,
UG Scholar
Department of Information Technology,
Velammal Engineering College,
Chennai ,Tamilnadu,India.

R. Dinesh,
UG Scholar
Department of Information Technology,
Velammal Engineering College,
Chennai ,Tamilnadu,India.

Abstract: Manual analysis and decryption of enciphered documents is a tedious and error prone work. Often—even after spending large amounts of time on a particular cipher—no decipherment can be found. Automating the decryption of various types of ciphers makes it possible to sift through the large number of encrypted messages found in libraries and archives, and to focus human effort only on a small but potentially interesting subset of them. In this work, train a classifier that is able to predict which encipherment method has been used to generate a given cipher text. We are able to distinguish 50 different cipher types (specified by the American Cryptogram Association) with an accuracy of 58.7%. This is a 11.5% absolute improvement over the best previously published classifier.Thus this algorithm detects the ciphertext and checks for any threat in the content and blocks the message from being delivered. In addition to that we have modified AES algorithm for time efficiency to encrypt and to decrypt the text at a faster rate.

General Terms

Security, Theory, Algorithm Encrypting a large amount of text using AEs algorithm makes it a time consumption process ,thus to overcome the time consumption a modification done in the AES algorithm.The modification takes place in shifting one of the steps of AES algorithm with DES algorithm.(i.e) shifting its Mixcolumn with permutation.

AES transformation;

- Bytesub transformation
- Shiftrows transformation
- Mixcolumns transformation
- Addroundkey transformation

Modifies AES transformation;

- Bytesubtransforamtion
- Shiftrows transformation
- Permutation
- Addroundkey transformation

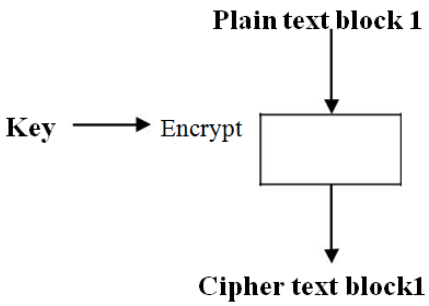
Keywords: Cryptography, Advance Encryption Standard, Cipher Text, Plain Text.

I. INTRODUCTION

Libraries and archives contain a large number of encrypted messages created throughout the centuries using various encryption methods. For the great majority of the ciphers an analysis has not yet been conducted, simply because it takes too much time to analyze each cipher individually, or because it is too hard to decipher them. Automatic methods for analyzing and classifying given ciphers makes it possible to sift interesting messages and by that focus the limited amount of human resources to a promising subset of ciphers. The American Cryptogram Association (ACA) specifies a set of 56 different methods for enciphering a given plaintext: Each encipherment method Mi can be seen as a function that transforms a given plaintext into a ciphertext using a given key, or short:

II. RELATED WORK

The user cut back provide the cipher text as input to a net page that returns the classifier's predictions. The source character of the classifier is available online. Our employment includes a reimplementation of the features secondhand in that classifier. As examples for field that deals by all of the automated decipherment of conceal texts.



These publications cook up a storm specialized algorithms for solving easily done and homophonic substitution ciphers, which are somewhat two untrue of the 56 cipher types defined separately ACA. which presents a cipher type

classifier for the finalist algorithms of the Advanced Encryption Standard (AES) contest.

cipher = Mi(plain, key)

When analyzing an unknown ciphertext, we are interested in the original plaintext that was used to generate the ciphertext, i.e. the opposite direction:

plain=Mi−1(cipher,key)

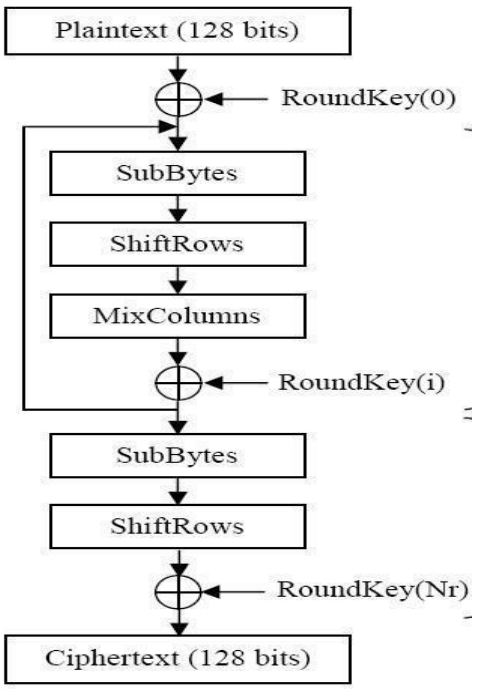
As a consequence of hardware implementation AES is very fast symmetric block algorithm. This method is known as naïve approach. Applying the naïve approach on enormous amount of data takes large computation and makes the encryption speed very slow due to

Variety of restriction. per ACA standard cipher types,thus with our implementation we are able to decrypt 52 out of 56 cipher types.

III. AES ENCRYPTION

AES encrypt idea by constantly using four kinds of message transformations: SubBytes, ShiftRows, MixColumns and AddRoundKey. interval the final completely does not have the MixColumns transformation.Each from one end to the other contain four transformations (linear and nonlinear) called Layers.Each completely has everywhere time signature derived from unusual key.Round conversion and its steps inspire intermediate statement called States.State proposed as rectangular choice of bytes with four rows and no. of columns that calculate on quantity of key length.

- Key length: 128 bit
- Key arranged in 4*4 matrix
- Each element is byte.



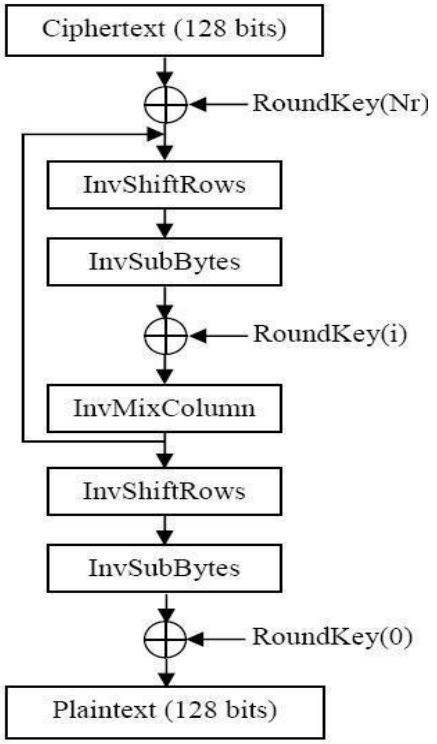


Figure 2.AES Decryption structure

IV. PROPOSED SYSTEM

DataFlow: For cipher detection

We first choose the possible plain text messages,then for each encryption method.

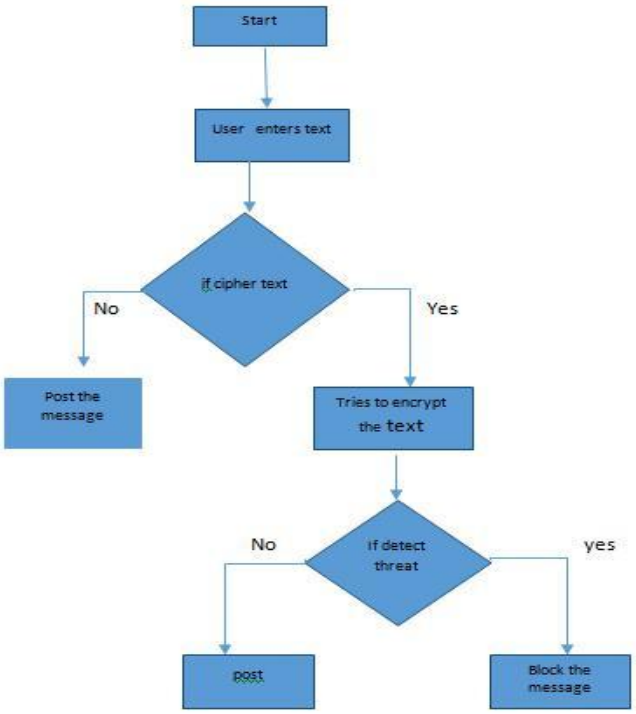


Figure .AES Encryption Structure

3.1 AES Decryption

The trsnsformation in the decryptin process Is to perform the inverse of corresponding Transformation in the encryption process. Four transformation in the AES decryption Round

- InvShiftrows
- Invsubtype
- Addroundkey
- InvMixcolumns

Algorithm

Step1:Start

Step2:User enter the text

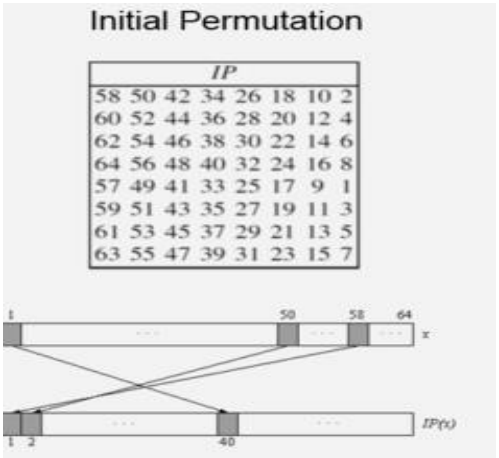
Step3:if it is not a cipher text it post the message or else Step4: it tries to encrypt the text

Step5: If it detect threats it blocks the message or else Step6:it post the message.**5. Rounds of Modified-AES Algorithm**

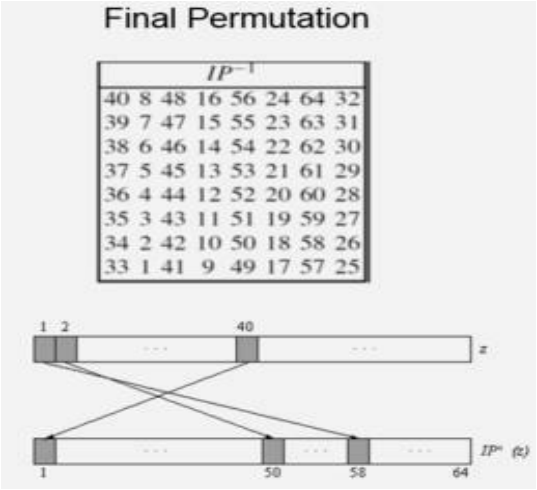
There are 10 rounds for full encryption. The four different stages that we use for Modified-AES Algorithm are:

- Substitution
- ShiftRows
- Permutation
- AddRoundKey

In modified AES algorithm except the Mixcolumns stage the remaining stage are kept Unchanged.For faster encryption in AES algorithm 128 bits block is used.Substitution and shiftrows takes 128 bit as input whereas permutation takes only 64 bit as input, thus by splitting up the shiftrows bits into two 64bit and then passing each 64 bit into permutation as a input and the bits can be shift accordingly to the intitial permutation (IP) table.



In the permutation table each entry indicates a specific position of a numbered input bit consisting of 64 bits in the output. While reading the table from left to right and then from top to bottom, we observe that the 58th bit of the 64-bit block is in first position, the 50th is in second position and so forth. After applying permutation on both sections of 128 bits we again combine both sets of 64 parts into a complete set of 128 bits and then perform next remaining functions of algorithm. If we take the inverse permutation it gives again the original bits, the output result is a 64-bit cipher text. The inverse permutation is performed according to following tables.



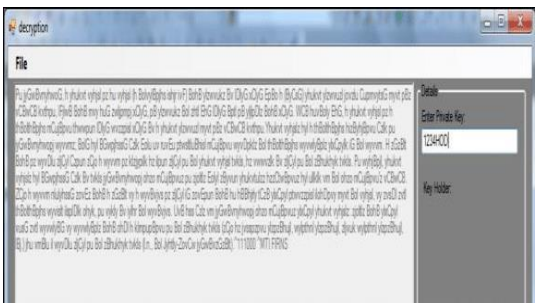
5.FEATURES

Repetation feature

This features is based on how the ciphertext contains symbols that are being repeated exactly n times in a given row. If a word contains two positions with repetitions of length n = 2, because the ciphertext contains RR, as well as DD Beyond length 2, there are no repeats. These numbers are then normalized by dividing them by the total number of repeats of length $2 \leq n \leq 6$.

Detective Feature

In this proposed system any threat causing messages or any unauthorized content are being communicate by the user can be identified and can be checked with pre defined data sets for the threat level of the content and if the threat is detected using the automated tool (i.e) the proposed system, will be able to terminate the particular content before being get posted and gives warning to the user.



VI. FOR DECRYPTION

For the full decryption of Modified-AES algorithm the transformation processes are, Inv-Bytesub, Inv-Shiftrows, Inv-Permutation, and the Addroundkey, which are performed in 10 rounds as it is in the encryption process.

Tests on Text files

To test the modified AES algorithm we take the different size of text files and compare the calculated time of the Modified-AES with Advanced Encryption Standard (AES). The comparison results performed on different sizes of text files using Modified-AES and the AES algorithm are producing entirely different results which are varying in time,thus making it time efficient.

VII. CONCLUSION

The proposed system is used to detect the cipher text and also to make sure that it is not an unauthorized or threat causing content .Thus and also to faster encryption of text between the user the AES algorithm has been modified in according to time efficient algorithm.

VIII. FUTURE WORK

Thus this proposed system is used to encrypt only the cipher text . henceforth the future project must be able to decrypt the binary digits into plain text which makes it more deciphering tool.

IX.REFERENCES

[1]. A. Thesis, ―IMAGE STEGANOGRAPHY WITH FORWARD ERROR CORRECTING CODES STRATEGY of Nahrain University in Partial Fulfillment of the Requirements for the Degree of by,‖ 2011.
[2]. ―IMPLEMENTATION OF HYBRID ENCRYPTION METHOD USING CAESAR ' CHAROMIE AlL TAT
[3]. WI A thesis submitted in partially fulfillment of the requirements for the award of degree of Bachelor of Computer Science (Computer Systems & Networking) Faculty of Computer System & Software Engineering Universiti Malaysia Pahang (UMP),‖ no. April, 2010.
[4]. B. Vijay and J. Swathi, ―Implementation of digital
[5]. Steganography using image files-a Computational approach,‖ vol. 10, no. 5, pp. 6–10, 2014.
[6]. M. A. Alia, A. A. Tamimi, and O. N. A. Al-allaf,―Cryptography Based Authentication Methods,‖ vol. I, pp. 22–24, 2014.
[7]. C. Security, ―Symmetric Key cryptosystem,‖ pp. 1–19, 2004.
[8]. C. Hall and N. Ferguson, ―Chapter 7 The Advanced Encryption Standard (AES),‖ no. November, pp. 58–73, 2001.
[9]. F.L. Bauer. 2010. Decrypted Secrets: Methods and Maxims of Cryptology. Springer.
[10]. Leo Breiman. 2001. Random forests. Machine Learning, 45(1):5–32, October.
[11]. Chih-Chung Chang and Chih-Jen Lin. 2011. LIBSVM: A library for support vector machines. ACM Transactions on Intelligent Systems and Technology, 2:27:1–27:27. Software available at http:// www.csie.ntu.edu.tw/˜cjlin/libsvm.
[12]. William AR de Souza, Allan Tomlinson, and Luiz MS de Figueiredo. 2013. Cipher identification with a neural network.
[13]. John Langford, Lihong Li, and Alex Strehl. 2007.Vowpal Wabbit. https://github.com/ JohnLangford/vowpal_wabbit/wiki.
[14]. Malte Nuhn, Julian Schamper, and Hermann Ney. 2013. Beam search for solving substitution ciphers. In ACL (1), pages 1568–1576.
[15]. Sujith Ravi and Kevin Knight. 2011. Bayesian Inference for Zodiac and Other Homophonic Ciphers. In Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics (ACL), pages 239–247, Stroudsburg, PA, USA, June. Association for Computational Linguistics.