PAPER • **OPEN ACCESS**

Triple symmetric key cryptosystem for data security

To cite this article: C Md Fuzail *et al* 2017 *IOP Conf. Ser.: Mater. Sci. Eng.* **263** 042040

IOP Conf. Series: Materials Science and Engineering **263** (2017) 042040 doi:10.1088/1757-899X/263/4/042040

Triple symmetric key cryptosystem for data security

Md Fuzail C, Jasmine Norman and Mangayarkarasi R
School of Information Technology and Engineering, VIT University, Vellore-632014, Tamil Nadu, India.

E-mail: jasmine@vit.ac.in

Abstract. As the technology is getting spreads in the macro seconds of speed and in which the trend changing era from human to robotics the security issue is also getting increased. By means of using machine attacks it is very easy to break the cryptosystems in very less amount of time. Cryptosystem is a process which provides the security in all sorts of processes, communications and transactions to be done securely with the help of electronical mechanisms. Data is one such thing with the expanded implication and possible scraps over the collection of data to secure predominance and achievement, Information Security is the process where the information is protected from invalid and unverified accessibilities and data from mishandling. So the idea of Information Security has risen. Symmetric key which is also known as private key.Whereas the private key is mostly used to attain the confidentiality of data. It is a dynamic topic which can be implemented over different applications like android, wireless censor networks, etc. In this paper, a new mathematical manipulation algorithm along with Tea cryptosystem has been implemented and it can be used for the purpose of cryptography. The algorithm which we proposed is straightforward and more powerful and it will authenticate in harder way and also it will be very difficult to break by someone without knowing in depth about its internal mechanisms.

1. Introduction

Word “Cryptography” [1] is derived from the Greek word as “Kruptos”, which means “Hidden”. It is a way to invisible the original data from the eyes of intruders and attackers from their attacks and miss using interruptions, and it’s impossible to break any information without knowing the knowledge of key (i.e., to get the plain content) without utilizing the decoding key. In some of the part, it’s very difficult to find the key in secured mechanisms. Its about the construction and analyzation of procedures that to overcome from opponent conventions. Uses of Cryptography incorporate Social networks, Transaction Cards, System Password, E - Commerce, and so forth.

2. Classification of Cryptography

There are diverse sorts of algorithms in cryptosystems as follows cryptography using symmetric key, cryptography utilizing asymmetric key and functions of hash.

2.1 Cryptography using Symmetric Key

In Symmetric [2] (it can be known as " private or mystery key ") the process of encoding and decoding takes place similar **k**ey's for both of the sides, or altered key can be used which is nearly same as the key which was used in the beginning. In this symmetric key we have two types of ciphers takes place as one is stream cipher which the data encodes in the form of each and every single characters ("Character by character") for example vinegar cipher, Caesar cipher, extended substitution cipher etc. and the other is block cipher which encodes the data in the form of blocks for the given plain content few of the famous block ciphers are "AES"[3] **A**dvanced **E**ncryption **S**tandard which is still exist in many of the organization's just because of its robust security which is very difficult to implement in current and "DES"[4] **D**ata **E**ncryption **S**tandard

2.2. Asymmetric key cryptography

In Asymmetric (it's called as "public key") Cryptography,use two keys on both of the sides as, In one side (As Sender) will have its own public and private key and in other end it will have receivers own public and private key, Those public keys will be known to all, through which the utilization with different keys the process begins There are numerous of famous asymmetric Key Cryptography available like "Rivest_Shamir_Adelmen" Algorithm [5] "RSA" is deployed on factorization and largest prime numbers products modular exponents by using which the process is difficult, and it provides moderate speed and furthermore its generation of key is moderate. (Diffie-Hellman) DH Key agreement system [6] which includes with large exponential operations and Key serializations algorithms etc.

2.3 Hash Functions

The hash function is like it can be a length of any size while receiving but after getting received of data it reduces the size of the given information, In case of "DSA"[7] (Digital Signature Algorithm) hash will be in fixed length, and like "SHA"[8] Algorithms (Secured Hash Algorithm) are some of the cryptosystem in hash function. Algorithms like MD2, MD5 are very easily broken but "SHA" algorithms is exceptionally hard to break in real time.

3. Needs of Cryptography

In a commonplace circumstance where cryptography is utilized, two gatherings (J and K) convey over the secured less channel. J and K need to guarantee that their communication stays tremendous by any individual who may tune in. Besides, in light of the fact that J and K are in remote areas, an absolute necessity make certain that the data gets from K has not been changed by anybody within transmission. What's more, it must make sure that the data truly originates from K and not somebody imitating K. Cryptography is utilized to accomplish the accompanying objectives.

3.1 Basic Terms of Cryptography

1.Encryption: The change technique of plain content into cipher content utilizing different encryption algorithms and methods.
2. Decryption: It is a reverse process of encryption where the cipher content is converted in to plain content.
3. Key: The key contains three properties One the key can be in the form of numbers, Second it can be a string (A-Z) and the third can be a combination of both integers and alphabets (alpha_numeric) used for both encoding and decoding.
4. Plain Content: It's a normal text or numeric which can be readable by normal peoples and sending to the other side.

5. Cipher Content: The content produced in the wake of utilizing the encryption algorithm on the plain content which brings about an incoherent content which can't be grasped

4. Literature Review

The referred paper gives the Knowledge about different types of encrypting and decrypting techniques. In which the security and confidentiality had been increased by applying some conversions like decimal to binary form then binary manipulation along with different theorems like (Chinese remainder theorem) CST [9] on before the encryption process takes place, some cryptanalysis attacks performed on Tea cryptosystem[10] and three layered cryptography[11] in which they convert the blank spaces with special characters such as (# and $) in odd and even counts along with that taken ascii then add squares of the given key though which the outcome of the resulted cipher text were very complicated.

5. Proposed System

In the proposed system, an old encryption algorithm Tea Cryptosystem has been included along with our implementation. This Tea having some useful advantages as it provides the two main facilities as it reduces memory consumption and time efficiency and disadvantages as some types of attacks was possible like “cipher-text-only”, “known-plain-text,” and “chosen-plaintext”. So that to overcome from this types of attacks we made changes in Tea cryptosystem by adding some scientific approach on encryption and decryption.

1. Pre Scientific encryption and

2. Post scientific decryption.

In pre scientific encryption, the encryption takes place before passing the plain text on to the actual encryption algorithm with two different keys which performs the ASCII conversions, decimal conversions and summation along with all ASCII and extended ASCII values from 0 To 255. In post scientific decryption the decryption takes place after getting the first decrypted cipher text from actual encryption algorithm with two different keys which performs the decimal conversions, ASCII conversions, and subtraction along with all ASCII and extended ASCII values from 0 To 255.

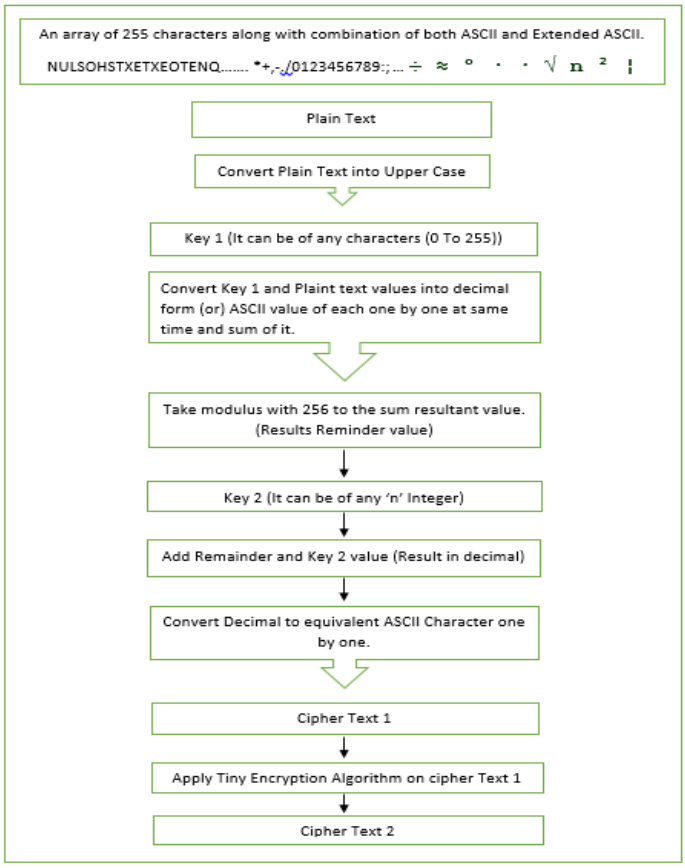

Figure.1 Pre Scientific Encryption

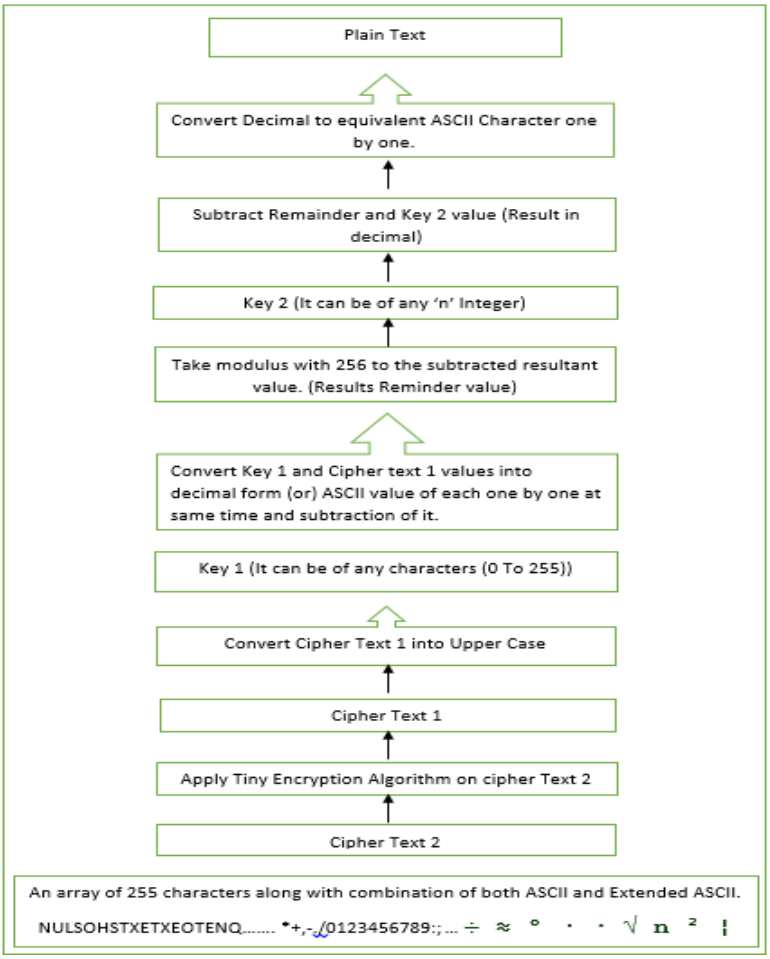

Figure.2 Post Scientific Encryption

5.1 Procedure

The steps for the encryption process is as follows.
1.Initialize all the ASCII and extended ASCII characters from 0 to 255 which is stored in an array.
2.Get the plain content.
3.Pass the key_1 which gets the n values of characters from 0 to 255.
4.Pass the key_2 which gets n values in integer.
5. Convert the plain content and key_1 into decimal which is passed into the loop one by one.
6.Plain content and key_1 ASCII values of each character by character and perform addition on it.
7.Then take the modulus from 256 for the resultant value of step 6.
8.Then add key_2 integer value along with each and every remainder value from step 7.
9.Convert ASCII values into string which will be our cipher text_1 (CT.1), It will be in the combination of both ASCII and extended ASCII.
10.Get the generated cipher text 1 (CT.1).
11.Pass the key_3 and
12.Condition takes place as of 128 bits divided in to 2 blocks 64 bits and 4 blocks of 32 bits along with delta.
13.Then the key will be taken as K0 (32) Left shift takes place four times.
14.Include delta value, it is nothing but a magical number (0X9E3779B9).
15.Then k1 (32) right shift takes place five times and perform XOR operation.
16.Repeat step 12, 13, 14 for K2 (32) and k3 (32).

17.From the computation step 13 to step 16 will get Cipher Text 2(CT.2).
Decryption:
1.Get Cipher Text 2(CT.2)
2.Pass the key_3 and
3.Condition takes place as of 128 bits divided in to 2 blocks of 64 bits and 4 blocks of 32 bits along with the delta value.
4.So the key will be taken as K.3 (32) Left shift takes place four times.
5.Include delta value (0X9E3779B9)
6.Then K.2 (32) right shift takes place five times and perform XOR operation.
7.Repeat step 4, 5, 6 for k.1 (32) and k.0 (32).
8.From the computation step 4 to step 7 will get Cipher Text1 (CT.1)
9.Declare all the ASCII and extended ASCII characters from 0 to 255.
10.Pass the key_1 which gets the n values character by character. It can be any of integers, characters and special characters.
11. Pass the key_2 which gets n values in integer.
12.Convert the cipher text 1 and key_1 values in to decimal form.
13.Pass the Cipher text 1 (CT.1) and key_1 ASCII values of each character by character and subtract it.
14.Then take the modulus from 256 for the resultant value of step 13.
15.Then subtract key_2 integer value along with each and every remainder value from step 14.
16.From resultant values of step 15, Convert ASCII values into text which will be our plain content (PT).
17.Plain Content generated successfully.

6. Conclusion and Future Scope

In this paper we have implemented a new algorithm which is applied over Tea cryptosystem which will provide very complicated cipher text also time efficiency along with a reduced amount of memory consumption and it will very difficult to halt or to perform cryptanalysis attacks on it. According to symmetric key cryptosystem the proposed algorithm not only supports Tea. It may also support other symmetric key cryptosystem of both types whether it can be a stream cipher or block cipher based on the need. On the other hand the proposed system may also be used by small scale organizations who are not capable of using expensive asymmetric key cryptosystems.

References

[1] Mini malhotral and Aman sing 20l3 Study of various cryptography algorithms *International journal of science engineering and research* **1(3)**
[2] Wikipedia Symmetric-Key Cryptography https://simple.wikipedia.org/wiki/Symmetric key_algorithm
[3] Ankit K, Dandekar l, Sagar prdhan and Sagar Ghormade 2016 Design of AES-512 Algorithm for communication network *International Research Journal of Engineering and Technology (IRJET)* **5** 438-443
[4] Coppersmith D 1994 The (Data Encryption Standards) Des and its Strength against attacks IBM *Journal of Research and Development*
[5] Nentawe Y and Goshwe 2013 Data Encryption and Decryption using RSA Algorithm in a network equivalent *International Journal of Computer Science and Network Security* **13** 9-13
[6] Maryam Ahmed, Baharan Sanjabi, Difo Aldiaz, Amirhossein Rezaei and Habeeb Omotunde 2012 Diffie Hellman and its application in security protocols *International Journal of Engineering Science and Innovative Technology* **1** 69-73.
[7] http://www.umich.edu/~x509/ssleay/fip186/fip186.htm 1994 Digital Signature Standard

(National Institute of Standards and Technology) NIST FIPS
[8] Priyanka vadhera and Bumika Lall 2012 Review Paper on secure hashing Algorithm and its variants *Int. J. of Science and Research* **3**
[9] Syed Siraj Ahmed N, Selvakumar R and Akshay Taywade 2013 public key cryptography algorithm using binary manipulation & CRT *International Journal of Research and Engineering* ISSN: 2277-3878 **2(5)**
[10] Simon J. and Shepherd 2003 A cryptanalysis of the Tiny Encryption Algorithm *Taylor & Francis Group LLC*
[11] Abhishek anand, Abhishek raj, Rashi Kholi and Vimal bhibul 2016 Proposed symmetric key cryptography algorithm for data security *1st International Conferences on innovation & challenges in cyber security on IEEE*
[12] Bhusari V and Patil S 2011 Study of Hidden Markov Model in Credit Card Fraudulent Detection *Int. J. of Computer Applications* **20**
[13] AmlanKundu, SuvasiniPanigrahi, Shamik Sural and Arun and Majumdar K 2009 Credit card fraud detection: A fusion approach using Dempster-Shafer theory and Bayesian learning *Special Issue on Information Fusion in Computer Security* **10** 354- 363
[14] RaghavendraPatidar and Lokesh Sharma 2011 Credit Card Fraud Detection Using Neural Network *International Journal of Soft Computing and Engineering*
[15] RamaKalyani K and UmaDevi D 2012 Fraud Detection of Credit Card Payment System by Genetic Algorithm *Int. J. of Scientific and Engineering Research* 3
[16] EkremDuman and HamdiOzcelik M 2011 Detecting credit card fraud by genetic algorithm and scatter search *Elsevier Expert Systems with Applications* 38
[17] Brabazon A, Cahill J, Keenan P and Walsh D 2010 Identifying Online Credit Card Fraud using Artificial Immune Systems *IEEE Congress on Evolutionary Computation (CEC)*
[18] Pejic, Bojan, AleksandarPejić and Zlatko Covic 2010 Uses of W3C's Geolocation API Computational Intelligence and *Informatics (CINTI) International Symposium on IEEE*
[19] Gardner, Matt W and Dorling S R 1998 Artificial neural networks (the multilayer perceptron) - a review of applications in the atmospheric sciences *Atmospheric environment* **32** 2627-2636