MESH Encryption : A Multifarious Synchronized Haze

Akshay R[#1],Persis Urbana Ivy B[#2], Shanmugapriya S[#3], Anandha Vishnu P[#4]

[#1] Final Year Undergrad,Computer Science, Sri Krishna College of Engineering and technology,coimbatore,India

[#2] Head of The Department,Computer Science, Sri Krishna College of Engineering and technology,coimbatore,India

[#3] Assistant Professor,Computer Science, Sri Krishna College of Engineering and technology,coimbatore,India

[#4] Final Year Undergrad,Computer Science,Sri Krishna College of Engineering and technology,coimbatore,India

Abstract— *Information is not secure in this eon since any attacker can compromise a system and get access to it.. In this paper .In order to make communications secure a randomized model of encryption with key Meshing is proposed. Mesh encryption uses randomization for encrypting the plaintext into ciphers using private symmetric keys and set of preset tables.This is a stream cipher algorithm . This randomization makes the cryptanalysis exhausting on extant attacks such as ciphertext attacks brute force attacks, chosen ciphertext, digrams and trigrams attacks,. This algorithm uses different layers of encryption and the labyrinth of these layers are also non aligned. This is achieved by creating a puzzle that dynamically repositions itself. Thus making the ciphertext formed after each transmission vary and will result in distinct ciphers after each transmission. In addition to that the length of plaintext and ciphertext is analogous, the transposition occurs in bit level in irregular fashion, increasing the complexity for cryptanalysis.It also makes private one to one communications safer. It can be applied in militant applications, hospital, commerce where data security and privacy is of concern.*

Keywords — *Private Key encryption, Key Generation, Arbitrary Key(AK), Base Key(BK), Transmitted Key(TK), Meshing Key(MK), Special Character Cipher(SCC), Anagram(AG), Numeric Cipher(NCC), AlphaNumeric Cipher(ANC), Alphabet Cipher(AC), Mesh Splitter(MS), Arbitrary Slicer(AS)***.**

I. Introduction

Information Security has been a major field of Computer Science since safeguarding confidential information is necessary. It is of utmost importance the data has to be impregnable. Computer systems are vulnerable both to abuse by insiders and infiltration by outsiders[1.]Data security is critical issue in the field of communication because if the data is not secure anyone can access it. Over the last couple of decades, the Internet has been in steadfast evolution[4].The number of devices that are connected to the internet is increasing at a rapid rate.Secure communication in wireless sensor network is an important concern[5].To ensure confidentiality and integrity of data Cryptography was implemented[6].

Cryptography is the process of representing the actual information called as plaintext and misrepresent it as a ciphertext.[7].Cryptography is a method of storing and transmitting data in a peculiar form so that only those for whom it is intended to can be able to read and access it.[9].A ciphertext belies a plaintext and makes it ambiguous to the unauthenticated users.The transformation of plaintext to ciphertext is called as encryption. And the revolution of ciphertext to plaintext is called as decryption.Cryptography desires to achieve confidentiality, integrity, and availability of data.[$g]The enciphering and deciphering of data takes place using keys. The manner in which the keys are used is based on two key algorithms called as Symmetric Key and Asymmetric key.[8]] A Symmetric key encryption algorithm has a private key that is synchronised with the sender and the receiver before the transmission of data takes place. An asymmetric key uses a pair of keys inclusive of private key and public keys. public keys which may be disseminated widely, and private key which are known only to the owner of private and public keys . Ciphers that were considered virtually unbreakable in the past are continually surmounted due to the relentless growth of computational power.[2]When an encryption algorithm has to be introduced into automated systems having low power. It becomes distinct .To ensure the authenticity and confidentiality of the data we have introduced an encryption algorithm that can be implemented in areas where standard encryption algorithms cannot be employed.Devices that provide improvement to healthcare such as IoT devices has to be provided with encryption. [3]

This also makes attacks on ciphertext ,Full or partial PlainText attacks debilitating for the cryptanalysts. It could also be implemented in areas where standard encryption algorithms are used such as military applications, hospital, commerce, private ,government corporate data. This algorithm can be implemented in all these devices making it heuristic .

First in Section II ,the related works on the various cryptographic algorithms has been discussed.In Section III we illustrate the Proposed work of the ME(Mesh Encryption), Then Section IV deals with the actual algorithm , Section 5 is the result analysis of the various existing attacks on the cryptosystems,

II. Related Works

[10]Information security is playing a vital role in many sectors such as banks, private, government corporate data, hospitals and e-commerce data over the internet. To provide secure transmission of password data is hidden into an image and then is transmitted and the receiver will decrypt the hidden message from the image. Steganography is the process of hiding the data in pictures ,audios etc. This paper provides new techniques of hiding the data into images, and to smoothen the noise.

[11**]**Multilevel Network Security combines the cryptography and steganography to produce data security.

Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages.The key may be discarded after use.

This algorithm uses cryptography to change the plaintext to ciphertext then hides the data in a picture using steganography techniques. Blowfish algorithm is a strong encryption algorithm. This is employed on an ARM platform.

[12]N/2 Parallel LFSR produces a pseudo random number generator that has high randomness of generation of numbers.The construction of pseudo random number generator (PRNG) is based on linear feedback shift register (LFSR). This class of generators can be very effectively implemented hardware, is capable to generate very long pseudorandom sequences with a high quality statistical distribution.Thus enabling the distribution of randomness to be distinct.

This is used in parallel system architecture to ensure high performance.

[13]- This paper is survey of different algorithms such as Symmetric Key and Asymmetric Key algorithms. And acting on different types of cipher.Two types of cipher creation block cipher,stream cipher either blocks of bits or single bit at a time.block cipher is used to encrypt the bits in blocks of 64,128 256.Stream cipher is used to encrypt the text bit by bit.A comparison of security and difficulty of implementation is also mentioned.

[14]- The different ciphers that are extant is Caesar Cipher, PlayFair Cipher, Feistel CIpher.From the output of Caesar cipher, Feistel cipher produce the encrypted text in Alphabet ciphers and playfair ciphers it produces a combination of special character and Alphanumeric cipher.

These ciphers only use predefined set of alphabets or may include some special characters.

[15]-This paper deals with the Policies, standards and procedures will be developed to provide appropriate levels of protection for organisational data The Cryptographic Policy sets out when and how encryption should (or should not) be used. It includes protection of restricted (or sensitive)information and communications, key management, and procedures to ensure encrypted information can be recovered by the organisation if necessary.

[16]-Attribute-Based Encryption (ABE) which is a generalization of Public Key Encryption (PKE), provides flexibility of data sharing for system users in the sense that a data encryptor is allowed to specify some descriptive values x for an encryption and thus,theencryptioncanbedecryptedsuccessfullybyasecretkey associated with some descriptive values y matching x. This deals with introducing new concept of ABE which provides versatility than other major Public Key encryption algorithms

III.The Proposed Work

A. Objective

To provide an algorithm that can be implemented in all internet connected devices. And to make cryptanalysis an exhaustive work .To provide an algorithm that acts in linear time for authenticated users and exponential for unauthenticated users.To create an irregular layer of encryption and make the ciphertexts result in various ciphers other than using one pattern of symbols

B. Overview

Mesh Encryption is an arbitrary plaintext encryption algorithm which uses private symmetric keys and an arbitrary generated key to encrypt the plaintext to the ciphertext.An initial Synchronisation is done with Blowfish algorithm and the BaseKey along with a set of pre set table and a Mesh key is sent to both the sender and the receiver. Now after the sender is ready to send his message.An arbitrary Key is generated which is then slitted into five using a splitter and the mesh key is then slitted into five. Now based on the combination of the bits represented by the

arbitrary Key and the Synchronisation Key the plaintext is encrypted to a ciphertext. Then the cipher text along with the Transmission Key which is nothing but the XOR of the Base key and the arbitrary Key is set to the receiver. This ciphertext and the Transmitted key acts as the input to the receiver end. Then the BaseKey which has been already synchronised XORing it with the transmitted key the arbitrary Key is found out and now based on the newly found arbitrary key and the extant mesh Key. The Cipher is converted into the plaintext.

C. System Architecture

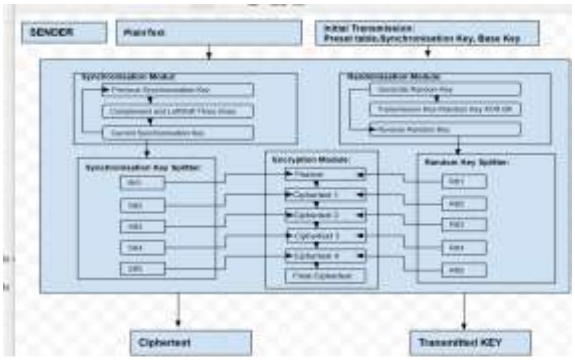


Fig 1 Encryption Module

In Fig 1 the process of Encryption used in MESH Encryption is discussed and in Fig 2 the decryption process is shown. Encryption is done in the sender side while decryption process is carried out in the receiver end.

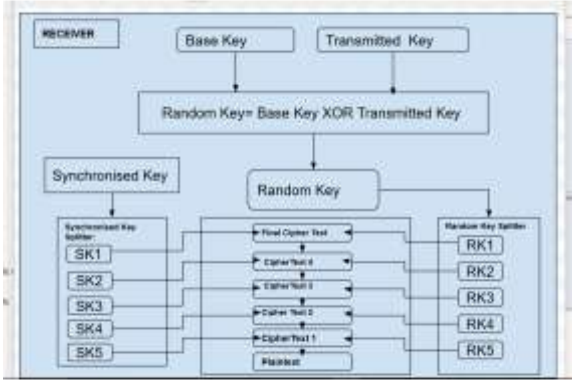


Fig 2 Decryption Module

D. Synchronisation Process:

There are two private symmetric keys that has to be paired with the users beforehand. They are BaseKey (10 bits) and Mesh Key(15 bits). Then a list of preset tables such as Special Character Cipher(SCC), Anagram(AG), Numeric Cipher(NCC), AlphaNumeric Cipher(ANC), Alphabet Cipher(AC) must be also paired. This process is done by using Secure algorithm such as Blowfish in order to synchronise the data between the users.

E. Key Generation

An arbitrary Key(10 bits) is generated for each transmission using predefined Randomisation algorithms that has high statistical distribution i,e the level of randomness is of a number being generated is high. After the encryption process is done the arbitrary Key is XORed with the Base Key to produce the Transmission Key which is then sent to the receiver.

1)*Individual cipher mechanisms:*Each individual ciphers can be brought up using 4 transpositions. Based on the arbitrary Key the selection process is done

2) *Conversion to SCC*:A preset table of Special Characters present. It includes a preset table of Special characters relative to the positions. Now based on the preset index of the key and the substitutions and transpositions that are predefined are taken into consideration and propelled to action.

3) *Conversion to anagram*: It is nothing but left shift and right shift of the given text.The number of shifting operations is different for each device which will lead to a randomisation event between different devices.

4)*Conversion to numeric cipher*: It will take a convoluted amount of substitutions and transpositions of a preset table that includes a series of number which could also be altered per device.Also the transpositions of range 0-9 is preferred because for the same character used at different position we would get the same number within the range of 0-9 which would be an hectic process to attack that cipher.

5) Conversion to Alphanumeric Cipher: This has a preset table of combination of numbers and alphabets. These will take also take extant transpositions and rules to take a expediting conversions.

Prest table pros: The most important thing to note in these conversions we define a preset table this is set for each device separately and can be identified.If the algorithm gets in hand of a particular device they cannot be used for another device because the preset table would not be the same for each device

6)Alphabet Cipher : This has a preset table of combination of alphabets. These will take also take extant transpositions and rules to take expediting conversions.

7)Randomized Layer Mechanisms:

There are 5 layers introduced introduced into this algorithm .Each will be based on the Synchronisation key .These layers will not be in a precise order of PT to SCC and TO AG then to NC and to ANC and to AC.These five layers will be interchanged and the transpositions will not be affected since it is based on Arbitrary Key(AK.)The Synchronisation key is already Meshed and so it will not be transmitted.

8)Checkpoints:

In order to provide efficient synchronization checkpoints are included after every n transmission that takes place. This is done to include failure handling techniques

This provides reliability to the system which was not produced by its predecessor hsle. Synchronization process as mentioned earlier will be encrypted by blowfish algorithm and will be sent to the receiver and thus maintaining the sanctity of the message transmission

9)Integrity checker:

Mesh encryption is a fixed length encryption algorithm it implies that if we send the count of the words that are present in the message before encrypting to the receiver. Then that number must be present with the same encrypted ,message if not before decrypting one could find that there is mishap occurring and one could resend the sata. This ensures data integrity which was not provided by hsle.

IV. Algorithm

A. Key Generation

- Create a Base Key(BK)(generally 10 bits)
- Mesh the base key with the sender and the receiver
- Create the Mesh Key((MK))(15-bits)
- Pairing of the Meshing key is done as follows:
    - ○ The (MK) will be set into the sender
    - ○ The reverse of (MK) will be set into the receiver
- After each transmissions the (MK) will be left shifted three times in the the sender and complemented once between each successive left shifts
- The (MK) will be right shifted three times in the receiver side.
- Based on (MK) the individual layer mechanisms will be arranged and thus after each transmissions the layers will differ
- Generate an arbitrary KeyAK(10-bits)
- Based on this (AK) encrypt the PlainText
- Use exclusive or of (AK) and BK to generate the Transmission KEY(TK)
- Transmit TK to the receiver before the transmission of the data

B. Randomization Of Layers

- (MK) is of 15-bit size
- Partition (MK) into Splitters which is of 3-bit size each namely Mesh Splitters((MS)
- There will be 5 Mesh Splitters((MS)
- Based on each MS arrangement of the individual layers takes place.

C. Randomized Encryption Of Plaintext

- (AK) is of 10-bit size
- Partition (AK) into Splitters which is of 2-bit size each namely Arbitrary Slicer(AS)
- There will be (n/2) AS Slicers
- Based on each AS encrypt the data into CipherText
- First Arbitrary Splitters(AS) will be used to encrypt the PlainText to any one of the five individual cipher based on the first Mesh Splitters((MS)
- Second Splitter will encrypt this cipher to any one of the individual cipher based on the second Mesh Splitters((MS)
- Third Arbitrary Splitter(AS) will encrypt the cipher to any one of the individual cipher based on the third Mesh Splitters((MS)
- The fourth Arbitrary Splitter (AS)will encrypt the cipher to the individual cipher based on the final Mesh Splitters((MS)
- The final Arbitrary Splitter (AS)will encrypt the cipher to the individual cipher based on the final Mesh Splitters((MS)
- This Cipher will be sent to the receiver with the TK
- Then the Meshing Key will be left shifted thrice. And complemented successively between the shifts.

D.Checkpoints

- After n transmissions has been over
- The base key along with preset table will be encrypted using blowfish algorithm and sent to the receiver
- The receiver finds if any change is present with its original source
- If true it uses the new set of data after discarding the previous source
- Else it will continue to operate with the same set of data.

E. Decryption Module

The Algorithm for Decryption of the Randomised text based Encryption is as follows

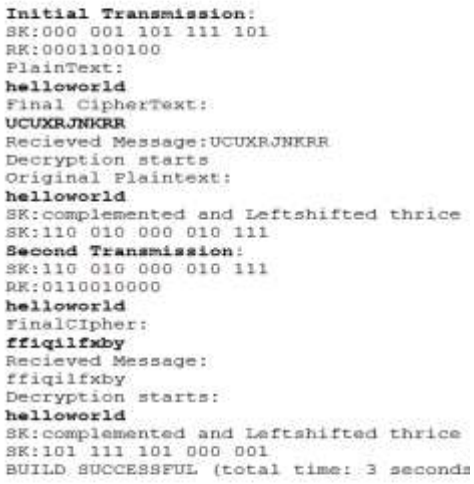
F. Key Generation

- The Transmission Key will be received
- The(Transmission key)TK will be exclusively or'ed with the (Base Key)BK will generate the (arbitrary key) (AK)
- Reverse ((AK))will be used to decrypt the ciphertext

G. Randomized Decryption

- Partition (AK) and (MK) (present in the receiver end not transmitted)into RS and SS
- The first AS will decrypt the received ciphertext to the individual layer based on the first MS
- MS will indicate which preset table to be used.
- The Second AS will decrypt the resultant of the previous decryption to the individual layer based on the second MS
- The Third AS will decrypt the resultant of the previous decryption to the individual layer based on the Third MS
- The fourth AS will decrypt the resultant of the previous decryption to the individual layer based on the fourth MS
- The final AS will decrypt the resultant of the previous decryption to the individual layer based on the final MS
- This is the Plaintext.
- Then the mesh key will be complemented and left shifted three times.

V. RESULT ANALYSIS



```
Initial Transmission:
SK:000 001 101 111 101
RK:0001100100
PlainText:
helloworld
Final CipherText:
UCUXRJNKRR
Recieved Message:UCUXRJNKRR
Decryption starts
Original Plaintext:
helloworld
SK:complemented and Leftshifted thrice
SK:110 010 000 010 111
Second Transmission:
SK:110 010 000 010 111
RK:0110010000
helloworld
FinalCIpher:
ffiqilfxby
Recieved Message:
ffiqilfxby
Decryption starts:
helloworld
SK:complemented and Leftshifted thrice
SK:101 111 101 000 001
BUILD SUCCESSFUL (total time: 3 seconds
```

A.CipherText only attacks

MESH is literally impossible to decode from knowing only one cipher of the PlainText.When the same message is being transmitted again the cipher will not be the same due to the irregularity of the layers.And this becomes a monumental task since randomisation is also included in the arbitrary Key. One cannot relate any of the ciphertext to a known plaintext. Hence Ciphertext only attacks are not possible against the algorithm.

B. Known Plaintext Attack

MESH has a strong defense against this type of attack. And is also nearly impossible to break MESH. The cryptanalyst will not only have access to ciphertexts but also several plaintext-ciphertext combinations.Even Though the cryptanalyst has these and has decoded the algorithm behind any one of these combinations.It will not be useful for decrypting other messages.Because of the randomisation that has been introduced in the key level. Decoding the 20C5 combinations of the plaintext-ciphertext algorithms which is an exhaustive task and since the cryptanalyst has a knowledge of only a few plaintext-ciphertext the 20C5 combinations cannot be deduced from these few plaintext-ciphertext combinations.

C.Chosen Plaintext

Here the plaintext will be chosen by the cryptanalyst and the ciphertext will be generated.Thus he has access to as many combinations of the plaintext-ciphertext combinations that the cryptanalyst wants. Due to the change the counter key after each transmission. Each consecutive ciphertexts will be following different sequence of layers of encryption.There are 5 different possible ciphers that could be generated from the same arbitrary Key.The cryptanalyst must find these 5 different ciphers to ensure linearity of the algorithm or else

for each transmission the arbitrary key gets changed leading to a non-linear approach.And deducing the algorithm behind these ciphers will not be useful due to randomisation.And to find these five ciphers it totally depends on the system's generation of the arbitrary Key. The same arbitrary Key. must be generated five times and for each time the counter key must vary. which is having very low possibility

D. Digram Attack

The characteristic pairs of adjacent letter, called diagram. Letters such as -en,-in,-vk.The frequency of letter groups can be used to match up plaintext letters that have been separated in a ciphertext. Since This algorithm uses randomisation the cryptanalyst be able to separate plaintext letters from a ciphertext but the transposition for these pairs will vary for each and every message thus exhausting the cryptanalyst.

E. Chosen Ciphertext

Here a purported ciphertext will be generated and for that ciphertext a plaintext is produced by the device.Based on the plaintext the cryptanalyst tries to deduce the algorithm. This attack in order to be effective the device must generate 20C5 combinations of plaintext for a single series of layers.Then the cryptanalyst must make the device generate the 20C5 combinations for each sequence of layers based on the counter key.If the counter key is not know this is amplified by 5! times.Else 5 times for 16C4 combinations the plaintext must be generated. This is really hard because the same arbitrary key to repeat itself takes a long period of time.Thus for 1024 keys to repeat itself gets amplified then for each of these keys to be repeated five times with five different counter keys is lang exhaustive process for the cryptanalyst.After getting access to all these plaintext the cryptanalyst has to deduce the algorithm behind it.Else non-linearity exists between each transmission.

VI. Conclusions

Mesh Encryption provides failure handling techniques that it's predecessor could not provide and also includes a new functionality that provides higher level of data security than its antecedent.

References

1-A Survey Of Intrusion Detection Systems,Teresa F.Lunt,Director,Secure Systems Research,Computer Science Laboratory,SRI International,Menlo Park, CA 94025 ,USA

[2]-Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey
Amitav Mukherjee, Member, IEEE, S. Ali A. Fakoorian, Student Member, IEEE, Jing Huang, Member, IEEE, and A. Lee Swindlehurst, Fellow, IEEE

[3]-Internet of Things in Industries: A Survey Li Da Xu, Senior Member, IEEE, Wu He, and Shan cang Li,IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 10, NO. 4, NOVEMBER 2014

[4]-The Internet of Things—A survey of topics and trends ,Andrew Whitmore & Anurag Agarwal & Li Da Xu,Inf Syst Front (2015) 17:261–274 DOI 10.1007/s10796-014-9489-2

[5]-A Survey on Cryptography using Optimization algorithms in WSNs ,Swapna B. Sasi 1,2* and N. Sivanandam 3,Indian Journal of Science and Technology, Vol 8(3), 216–221, February 2015

[6]-Cryptography and Steganography – A Survey by A. Joseph , Raphael Dr , V. Sundaram
Int.J. Comp.Tech.Appl.,Vol 2 (3),626-630.ISSN:2229-6093

[7]-ComparativeAnalysisofCryptographyCipherTechniquesLaukendraSingh,RahulJohari DepartmentofComputerEngineering, USICT, GGSIPUniversityNewDelhi,India
International Conference Of Advance Research and Innovation.

[8]-A comparative survey of symmetric and asymmetric key cryptography
Sourabh Chandra,.Smita Paira ,Sk Safikul Alam ,Dr.(Prof.) Goutam Sanya,2014 International Conference on Electronics, Communication and Computational Engineering(ICECCE).978-1-4799-5748-4/14/$31.00 © 2014 IEEE

[9]-Secure Password Transmission for Web Applications over Internet using Cryptography and Image Steganography:Mehdi Hussain, Ainuddin Wahid, Abdul Wahab Ishrat Batool and Muhammad Arif

[11]-Multilevel Network Security Combining Cryptography and Steganography on ARM Platform
Pallavi H. Dixit, Kamalesh B. Waskar, Uttam L Bombale.*Journal of Embedded Systems*, 2015 3 (1), pp 11-15. DOI: 10.12691/jes-3-1-2

[12]-N/2 BIT PARALLEL LFSR FOR CRYPTOGRAPHY,Shiv Dutta Mishra ,.International Journal of Advanced Engineering Research and Studies E-ISSN-2249-8974,Proceedings of BITCON 2015 Innovations For National Development National Conference on :Research and Development in Computer Science and Applications

[13]-A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms,
N Bisht, S Singh - International Journal of Innovative Research in Science, 2015

[14]-COMPARATIVE ANALYSIS OF PERFORMANCE EFFICIENCY AND SECURITY MEASURES OF SOME ENCRYPTION ALGORITHMS AL.Jeeva,Dr.V.Palanisamy, K.Kanagaram International
Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com.Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037

[15]-Cryptography Policy:Lance J. Hoffman, Ali, Faraz, A,Steven L. Heckler, and Ann Huybrechts.Communications of the ACM. *Communications of the ACM*, Sept. 1994, p. 109+. *Academic OneFile*, Accessed 2 Nov. 2017.

[16]-A secure and efficient Ciphertext-Policy Attribute-Based Proxy Re-Encryption for cloud data sharing
Kaitai Liang,Man Ho Au,Joseph K.Liu, Willy Susilo,Duncan S.Wong,Guomin Yang,YongYu,AnjiaYang.
Future Generation Computer Systems
Volume 52, November 2015, Pages 95-108