International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 12, December-2014

A Survey on Common Symmetric Encryption Algorithms

Arvind Kumar Sharma[1] and Hitesh Sharma[2]
Department of Computer Science and Engineering
Lovely Professional University
Phagwara, India

***Abstract*— Encryption algorithms play very important role in performing security related tasks. There are three major issues about which every algorithms have to deal with, which are Confidentiality, Integrity, and Availability. There are number of encryption algorithms that are used to provide security at different levels and with different points on which they focus on. Some algorithms for managing Confidentiality and Security and other for managing the Integrity of the shared and transmitting data. Different level of security provided by different algorithms depending on how difficult is to break them. This study provides evaluation of four symmetric algorithms namely: Hill Cipher, DES, 3DES, and AES. From our study we come to conclusion that the best algorithm is one that provides security and speed. We come on new design of encryption algorithms with Data Encryption Standard and Hill cipher about which little discussion provided on this paper.**

Keywords-Algorithm; Encryption; Integrity;Confidentiality; Cipher

I. INTRODUCTION

Cryptography is known as the study of secrets. This is basically connected to the definition of providing security with encryption/decryption process. Encryption is the process through which the actual plaintext information or message converted to new un-understandable message with the help of encryption algorithms in order to hide the actual meaning of message which is to be stored or transmitted over the channels. And decryption is the reverse of encryption process. For both processes same secret key to be used that is to feed to algorithm for performing such tasks.

Security mechanism require specific algorithm for encryption/decryption purpose, and for managing the sub-keys that are to be used to make cipher text from standard plaintext. As the security of the algorithms directly related to key length of secret key, longer the key stronger the technique will be but with longer key computation power of CPU must be affected.

An algorithm will be stronger if it is difficult to recover the plaintext if we have substantial amount of ciphertext available.

A. Way how to convert plaintext:

In Stream Cipher character by character conversion takes place with particular key and in block cipher a defined set of elements converted at a time to ciphertext with key.

B. Type of Operation used for conversion of plaintext to ciphertext:

There are two basic principles that are to be used for plaintext to ciphertext conversion which are:
Transposition: Elements are reorder or rearranged.
Substitution: Every element mapped to another elements.

C. Number of Key Used:

In system where same key to be used by sender and receiver than it is referred to as symmetric key encryption and when both sender and receiver use different key then it is referred to as asymmetric key encryption.

The rest of the paper is organized as follow. Section II describe some commonly used symmetric cryptographic algorithms, Section III will explain general study about Research paper and finding from these papers, Section IV give a comparison of such previously existing algorithms and there modified forms also and, Section V provide conclusion and my future work.

II. STUDY OF SOME COMMONLY USED ALGORITHMS

Implementation or modification into/for encryption algorithms is just for providing security to the plaintext messages or other data.

A. Hill Cipher

Hill cipher is one of the well-known symmetric key algorithms that work on mathematical matrix computation basis, use to encrypt set of characters of plain-text at a time with square matrix and decrypt ciphertext with inverse of that matrix that has to use for encryption.

With advancement in this algorithm now in order to reduce the computation power of calculating inverse of defined matrix now involutory matrix and self-invertible matrix used.

B. DES

Data Encryption Standard was one of the popular and strong algorithms used previously and now also for providing highly secure cipher text of plaintext. This technique use 64 bit computation with 56 bit key with its sub-keys in binary format. Algorithm depends on Feistel structure for providing confusion-diffusion.

Implementation of DES based on hardware of low cost, flexible and, providing efficient encryption solutions.

C. 3DES

Triple DES is the modification of Standard DES algorithms for providing highly secure data as compared to DES with three different keys of total 168 bit key. That means sixteen rounds on particular 64 bits performed three times with three different keys and their sub-keys so as to make algorithms beyond the reach of brute-force attack performed by EFF DES cracker.

Although triple DES much secure than standard DES it consume three times CPU power than DES. In forms of triple DES algorithm is considered to be more secure, in spite of having theoretical attacks.

D. AES

Advanced encryption standard is mostly used symmetric key algorithm that operates on 128 bits at a time and having 4 of the basic operation in each round of total of 10 round. Sub-byte(), Shift-row(), Mix-column() and Add-roundkey(). First three operation just make the management of bits and add-round () key use the key to encrypt the information received after these three operations.

The management of key takes place separately which secure and not so power consuming

Technique, that's why this algorithm still widely used in many of the area for providing security, And it is hard to find out the match of one sub key with other key.

III. General Study

By research paper [1] provide the information about various symmetric and asymmetric encryption algorithms with their advantages on particular situation captured. And it also discusses a broad comparison of all these techniques in case of their efficiency to perform tasks and level of security they are providing to data.

By research paper [2], [4], and [5] provide information how to make uses of Hill cipher with self-invertible matrixes and generation of involutory, permuted matrixes that are to be used in advanced hill cipher technique in order to maintain efficiency of algorithm for performing computation that consume less power as compare to finding inverse of pre generated matrix. The main reason of using such matrix is to make computation faster as compare to previously discussed basic terminology of Hill Cipher which focus on using one matrix for encryption process and then finds out inverse of the that key matrix which be used for making decryption of the computed cipher-text. But there are huge amount of matrixes for which no inverse exist so this form of checking to find the inverse matrix is quite time consumable tasks, in order to provide relief from this task the uses of self-invertible matrixes preferred that is same key matrix will be used for both the process for encryption and decryption, in case of involutory matrix the process of finding one matrix that is inverse of itself also, will be used for encryption and decryption process. To find these types of matrixes is quite easier task as compare to finding inverse of matrix. And permuted and reiterative nature of these matrices enhances the security power of Hill cipher.

By research paper [1] and [7] at first we got complete description about all the well-known symmetric and asymmetric security providing algorithms such as DES, 3DES, AES, Blowfish, RSA and RC2, RC4. This paper and book briefly describe how some of techniques useful in particular type of situation and what are pros and cons of each of them according to operating power in situation with security risks. And then we deeply understand the plus point of each it during comparison phase with other.

By research paper [3] we got new or you can say advance method for implementing data encryption standards that uses new type of s-boxes as most of cryptanalysis attack heavily depends on s-boxes. Here we collectively use 'AND' and 'XOR' operation with s-boxes. This replacement introduces new level of security and more robustness against breaking methods. From this paper deep information how to make uses of double key management takes place one for the encryption-decryption process and other for the identification of what new s-box we have to use. Here at first the 32-bit binary value converted to new 16 decimal numbers and from this 16 decimal number we found the corresponding value form 4 truth tables depends on the value. This technique basically enhances the security providing power to data and, generates robust system at the end for providing secure data that is to be flaws on to the medium and similar reverse process will be used for making decryption process in order to generate the actual message.

By paper [6] which is a lecture note we get complete information about AES technique and various steps involved in this technique with their purposes to enhance security. And from this deep working about each step how sub-byte (), substitute-byte () and most importantly mix-column () which is a mathematical operation on hexadecimal value has to made. Also the complete information about how key will be generating from words (32-bit) of data and using it with Add-round key () function to make possible all these information with full description I learnt from this note.

By book [7] we get deep study and knowledge about structure and step by step knowledge of each of algorithms that we have discussed above with their advantages and disadvantage according to situations they are used in order to provide security.

IV. Comparison of Selected Algorithms

From the above study we are now giving some brief introduction about the advantages and disadvantages of above explained algorithms as under below:

- Advanced Data encryption standard is more secure and robust encryption technique as compare to previous implementation.
- Triple DES is more secure than prior implementation of DES but consume lots of CPU time.
- It is concluded that AES is superior to DES and 3DES in case of performance.
- Hill cipher is strong against ciphertext only attack but not performs against know-plaint text attack, but modified form with invertible matrix is strong enough to provide security.
- Modified DES which based upon new four truth tables is more securable than ordinary DES.

From the above description we identifies that Advanced encryption standard is good enough to provide security and to manage computation power, although triple DES is more secure by using three keys for same operation but computation power quite high and modified Hill cipher developed recently more securable and more resistant to very type of attack whether plain-text only or cipher-text only and computation power still low as we are using single matrix for both purposes encryption-decryption.

S no.	Algorithms	Evaluation
1	DES	Less Secure
2	Modified DES with new 4 truth tables	Secure and robust system
3	3DES	Slower than other
4	AES	Time consumption, throughput better than other
5	Hill Cipher	Not resistant to plaintext only attack
6	Advanced Hill Cipher Hill++	Faster and Much resistant to known plaintext attack

Table I: Compared Result of Algorithms

V. Conclusion

From the above description of four algorithms DES, 3DES, AES, Modified Hill cipher we conclude that AES and modified Hill are stronger than other according to type of attack and performance of operation they performed. And modified DES is much better to provide security. And we will shortly come with new encryption algorithms design with DES and Hill cipher for enhancing the security of such cryptosystem. And with such new proposed system security must be increased and computation power must decrease for making such encryption-decryption operation.

References

[1] Evaluation of Common Encryption Algorithm and Scope of Advanced Algorithm for Simulated Wireless Network
Dr. Atul M. Gonsai1, Lakshadeep M. Raval2 (2014)

[2] A New Approach of Classical Hill Cipher (Hill++)
M. Nordin A. Rahman, A. F. A. Abidin, MohdKamirYusof, N. S. M. Usop. (Year 2013)

[3] New Approach of Data Encryption Standard Algorithm Shah Kruti R, BhavikaGambhava (Year 2012)

[4] Involutory, Permuted and Reiterative Key Matrix Generation Methods for Hill Cipher BibhudendraAcharya, Sarat Kumar Patra2, and Ganapati Panda (Year 2009)

[5] Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm BibhudendraAcharya, GirijaSankarRath, Sarat Kumar Patra, Saroj Kumar Panigrahy (Year 2007)

[6] The Advanced Encryption Standard AvinashKak, Purdue University (Year 2014)

[7] Hill Cipher and modular arithmetic Data Encryption Standards
Feistel Cipher and its working Cryptography and Network Security Principles and Practice, William Stallings

[8] Matrix Operations, Manipulation Spectrum Mathematics
Prof. D.R. Sharma