International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 02, February 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

A OVERVIEW OF CRYPTOGRAPHY TECHNIQUES AND ALGORITHMS

Nagma [1], Bhupesh Dewangan

[1]M.Tech, [2]Asst.Professor, Computer Science & Engg. Dept.CSIT, Bhilai, C.G., (India)

ABSTRACT

Data security is a vital on web. There are completely different varieties of data that include business connected, educational or user connected personal knowledge. Unknown access of the knowledge will result in massive losses, thus it's necessary that correct measures ought to be taken for securing data on web. Cryptography may be a technique of storing and sending knowledge in a very explicit type so solely those for whom it's meant will browse and method it. The term is most frequently related to scrambling plain text (ordinary text, typically mentioned as clear text) into cipher text (a method referred to as encryption), then back once more (known as decryption).Security, integrity, non-repudiation, confidentiality, and authentication services are square measure the foremost necessary factors in data security. In currently days the protection of knowledge attracts a lot of attention, particularly once this knowledge are hold on in memory or send through the communication networks. Many alternative encryption strategies are projected to stay the protection of the information, during this paper we tend to explore the implementation of AES (Advanced Encryption Standard) and its benefits and up its security mistreatment improved pattern generation technique.

Keyword: Cryptography, Public Key Cryptography, Private Key Cryptography, Advanced Encryption Standard (AES).

I. INTRODUCTION

Protecting sensitive knowledge is that the finish goal of just about all IT security measures. two robust arguments for safeguarding sensitive knowledge are to avoid fraud and to shield privacy. The improper revelation of sensitive knowledge may also cause damage and embarrassment to students, faculty, and staff, and probably damage the name of the Institute. a number of the necessary aspects of data security are:

- Data security is crucial to all or any educational medical and business operations.
- Create an idea to review your information security standing and policies and build routine processes to access, handle and store {the information} safely moreover as archive reserve data.
- Keep solely the info required for routine current business keep a copy the info to a secure place within the event of loss.

1.1 Cryptography

Cryptography is that the science of constructing communication unintelligible to everybody except the meant receiver(s). It's the study of strategies of causing messages in disguised type in order that solely meant recipients will take away the disguise and skim the message. Cryptography offers economical answer to shield sensitive

data in an exceedingly sizable amount of applications together with personal information security, net security, diplomatic and military communications security, etc through the processes of encryption/decryption. A cryptosystem may be a set of algorithmic program, indexed by some keys(s), for encryption messages into cipher text and secret writing them into plaintext.

1.2 Elements of Cryptography

- Plaintext: the initial information or text is termed plaintext.
- Cipher Text: the initial message changed to a distinct unreadable format using some formula is termed Cipher text..
- Key: secret is selection thereon formula depends, similar to the Caesar cipher text uses key no 3.
- Encryption formula: This algorithm is required at sender's facet for propelling the initial message (Plaintext) to unreadable format (Cipher text) to protect the data from completely different non valid receivers.
- Decryption algorithm: required at receiver's side for retrieving the initial message that is to change the cipher text to plaintext.
- Hashed message Authentication code: throughout this case the copy of the key is addition along with data and combination is hashed victimisation the key less hash operate like SHA one. Result of this will be HMAC that's once more assignment over with that same key and result's once more hashed victimisation that formula. At receiver side the receiver creates its own HMAC and compares it with delivered to validate and check for authentication.
- Digital signature: Like simply just in case of banks once you sign a Cheque, they check your signature for authentication to look at that the user is valid. to know the thought of Digital signature, enable United States to require AN example there are a pair of users A and B.A send message to B and B checks that the message came from A not anyone else. B can raise A to sign the message thus it will be prove that A is that the particular sender and B verifies the quality, this will be said as digital signature.

II. RELATED WORK

- It is important to cut back the correlation between the initial message and therefore the encoded version of it using enlarged knowledge structures for block cryptography rule, longer cryptography key sequences and non-linear operations [1].
- The major advantage of pattern primarily based cryptography is that it's tough to crack, however it's straightforward to implement [2]. Most hackers exploit the correlation between the cipher and plain text thus a brand new coding theme is needed specified, although the hacker gets a touch, it ought to be tough for him to crack.
- The image pattern methodology will increase the information security to nice extent. during this methodology the carrier image is generated by using a particular code referred to as four out of eight-code and addition of carrier image to original image that result into the encrypted image [3] .The four to eight digit code is additionally venerable, thus instead of encrypting a picture in its original pattern, this paper provides another approach inside that image is split into entirely completely different parts so it unified in to a pattern that is entirely known to approved parties.

- A encoding rule wouldn't be of a lot of use if it's secure enough however slow in performance [4]. The four of the popular secret key cryptography algorithms, i.e., DES, 3DES, AES (Rijndael) and Blowfish algorithm has been enforced and performance has been compared, when experiment it's shown that Blowfish is most effective rule.
- Information security plays a vital role in electronic communication. Any loss to sensitive knowledge will influence be great loss to the organization [5]. Cryptography rule plays main role once confidential knowledge is transmitted over the network. The cryptography algorithms consume a major quantity of computing resources like memory, battery power and cpu time.

III. OVERVIEW OF AES ALGORITHM

In 1997 the National Institute of Standards and Technology (NIST) of the United States place out a involve proposals for a replacement regular algorithm, which is able to be referred to as the Advanced Encryption Standard (AES). The candidates for the AES algorithm had to satisfy sure normal. First, of course the algorithm have to be compelled to be a regular algorithm and it ought to be resistant against all superb attacks. what's additional, the AES ought to be economical in performance and memory for varied platforms. The look ought to be easy, and it have to be compelled to be ready to handle fully completely different key lengths (128, 192 and 256 bits). The block length of the cipher have to be compelled to be 128 bits.

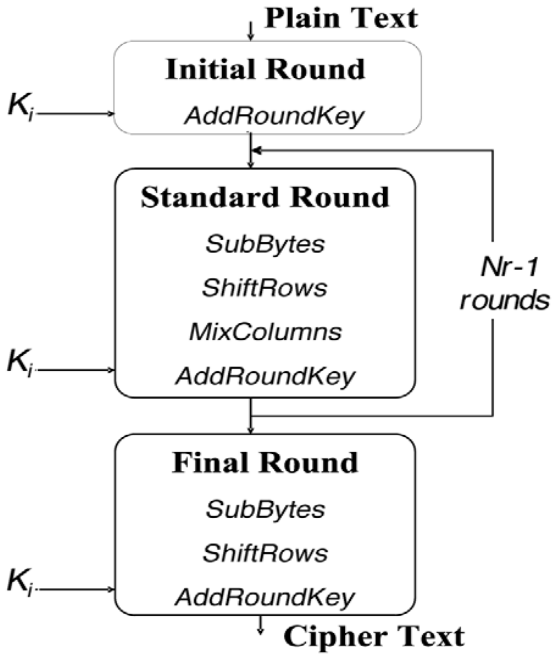

Figure: Overview of AES

The rule starts with degree of initial round followed by variety of normal rounds and it ends with the ultimate round solely four completely different operations area unit necessary to cipher these rounds and a key schedule. It is possible in Rijndael to use completely different key lengths in keeping with the protection level that's needed for the applying. Rijndael is outlined as a block cipher with key lengths of 128, 192 or 256 bits. The possible input block lengths are 128, 192 or 256 for the Rijndael rule. The AES rule is strictly similar because the Rijndael rule, however it solely defines one block length of 128 bits. The Rijndael rule is such every bit

depends on all bits from a pair of rounds past, e.g. full diffusion is provided. The quantity of rounds that has to be run depends on the key length.

IV. OVERVIEW OF DES ALGORITHM

DES is that the first block cipher—An formula that takes a fixed-length string of plaintext bits and transforms it through a series of difficult operations into another cipher text bit string of identical length. Among the case of DES, the block size is sixty four bits. DES to boot uses a key to customize the transformation therefore cryptography can supposedly solely be performed by those who acknowledge the particular key used to cipher. The key apparently consists of sixty four bits; however, solely fifty six of these are actually used by the algorithmic program. Eight digit code are used completely for checking parity, and are thenceforth discarded. Therefore the effective key length is fifty six bits. The secret's nominally keep or transmitted as eight bytes, each with odd parity. in line with ANSI X3.92-1981 .One bit in each 8-bit byte of the KEY might even be used for error detection in key generation, distribution, and storage. Bits 8, 16,... sixty four are to be employed in making certain that each byte is of wierd parity. Like totally different block ciphers, DES by itself is not a secure suggests that of secret writing but ought to instead use during a mode of operation. FIPS-81 specifies several modes to be used with DES. Cryptography uses identical structure as secret writing but with the keys utilized in reverse order.

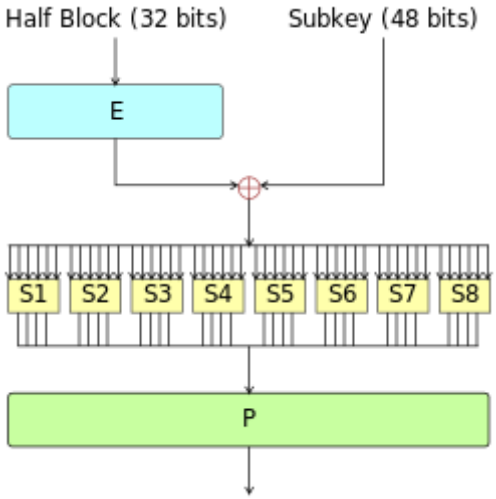

Figure: Function of DES

- Expansion: the 32-bit half-block is expanded to forty eight bits using the enlargement permutation, denoted E within the diagram, by duplicating half the bits. The output consists of eight six-bit (8 * 6 = forty eight bits) items, every containing a replica of four corresponding input bits, and a replica of the at once adjacent bit from every of the input items to either side.
- Key mixing: the result's combined with a sub key using Associate in Nursing XOR operation. Sixteen 48-bit sub keys—one for every round—are derived from the most key using the key schedule
- Substitution: when intermixture within the sub key, the block is split into eight 6-bit items before process by the S-boxes, or substitution boxes. Every of the eight S-boxes replace its six input bits with four output bits in line with a non-linear transformation, provided within the type of a operation table. The S-

boxes offer the core of the protection of DES—without them, the cipher would be linear, and trivially breakable.

o Permutation: finally, the thirty two outputs from the S-boxes are rearranged in line with a set permutation, the P-box. this is often designed in order that, when permutation, every S-box's output bits are unfold across four totally different S boxes within the next spherical.

V. CONCLUSION

In today's situation one among the main necessities is to use effective techniques so as to shield knowledge from unauthorized access if associate offender somehow manages to steal the info. The paper aims could be a review of cryptography and its varied elements. The paper additionally discusses the functioning of AES and DES algorithms.

REFERENCES

[1] "A Study Of Methods Used To Improve Encryption Algorithms Robustness", Scripcariu, L., IEEE 2015.

[2] "New Cryptographic Technique For Enhancing Security",Aamir Mohammed Suhail , Anuraag Vyas, Meghana Gudivada, Prof.T.Venkat Narayana Rao ,International Journal of Scientific & Engineering Research,2015.

[3] A potent approach to enhance security extent of an image during image encryption,Kainth, K.IEEE,2015

[4] "A Performance Comparison of Data Encryption Algorithms" Nadeem, A. ,Javed, M.Y. IEEE, 2005.

[5] "A Comparative Survey Of Symmetric Encryption Techniques For Wireless Devices",Anjali Patil, Rajeshwari Goudar ,August , 2013.

[6] "A Review and Comparative Analysis of Various Encryption Algorithms",Rajdeep Bhanot and Rahul Hans,International Journal of Security and Its Applications, 2015.

[7] "A COMPARATIVE ANALYSIS OF CRYPTOGRAPHY ALGORITHMS ",M.B.Nivetha1 , Mr.S.Sivaramakrishnan,IJIREECE,2014

[8] "A Survey on the Applications of Cryptography", Shivangi Goyal University School Of Information ,(International Journal of Engineering and Technology Volume 2 No. 3, March, 2012

[9] "Text and Image Encryption Decryption Using Advanced Encryption Standard", Kundankumar Rameshwar Saraf , Vishal Prakash Jagtap , Amit Kumar Mishra , International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)

[10] "Efficient Implementation of AES", « International Journal of Advanced Research in Computer Science and Software Engineering", Volume 3, Issue 7, July 2013.