ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (418-421), Month: January - March 2015, Available at: www.researchpublish.com

Encryption

[1]Sruthi Medasani, [2]Professor Tarik El Taeib

Department Of Computer Science, University Of Bridgeport, United States Of America

Abstract: **Encryption is the most effective way to achieve data security. It is the process in which plain text converts into a cipher text and allows only authorized people to access the sender information. In this research paper I would like to explain different types of encryption techniques such as hashing function and symmetric and asymmetric methods with advantages and disadvantages including necessary practical examples.**

Keywords: **Encryption, Cryptography, Hashing, Asymmetric, Symmetric, Cipher text**

I. INTRODUCTION

To provide security for data which is confidential is one of the major difficulties especially for computer networks. Not only for the large companies but also for small companies security is a common constraint. Moreover, development has achieved by hackers as well as programmers. So, it is necessary to take certain steps to protect our data. To maintain our data only between sender party and receiver party we should apply some techniques. "Encryption" is one of the easy and secure ways to protect the data from unauthorized people. It is the process of converting electric data to another form which called as cipher text. Encryption can also provide authentication, integrity and non repudiation with confidentiality.

II. HASHING METHOD

Hashing is a encryption method in which it creates a unique code having fixed length for the input data. By using the hashing algorithm it creates hashes people can compare the sets of data with those functions. Even minor changes to that message result in a dramatically different hash.

The main difference between hashing and remaining encryption techniques is after the encryption process ,we cannot get back into first that means reverse is not possible.

The issue at hands is to accelerate looking. Consider the issue of scanning an exhibit for a given quality. On the off chance that the show is not sorted, the pursuit may oblige inspecting each and every components of the exhibit. On the off chance that the show is sorted, we can utilize the parallel inquiry, and thusly lessen the more awful case runtime multifaceted nature to O(log n). We could hunt considerably speedier in the event that we know ahead of time the list at which that esteem is found in the cluster. Assume we do have that enchantment work that would let us know the record for a given worth. With this enchantment work our pursuit is lessened to only one test, issuing us a consistent runtime O(1). Such a capacity is known as a hash capacity. A hash capacity is a capacity which when given a key, produces a location in the table.

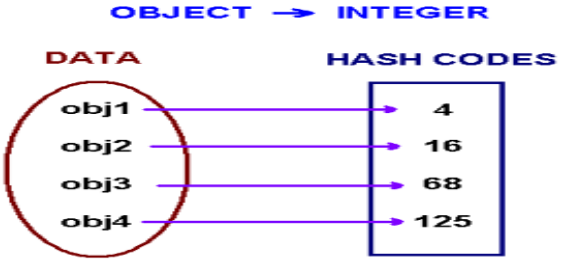

Figure 1: Hash Code Generation.

The sample of a hash capacity is a book call number. Every book in the library has an exceptional call number. A call number is similar to a location: it lets us know where the book is found in the library. Numerous scholastic libraries in the United States, utilizes Library of Congress Classification for call numbers. This framework utilizes a blend of letters and numbers to mastermind materials by subjects.

A hash work that profits an extraordinary hash number is known as a general hash capacity. By and by it is to a great degree hard to allot novel numbers to protests. The later is constantly conceivable just in the event that you know (or surmised) the quantity of items to be prepared. The methodology of putting away questions utilizing a hash capacity is the accompanying. Make an exhibit of size M. Pick a hash capacity h, that is a mapping from articles into numbers 0, 1, ..., M-1. Put these items into a cluster at lists registered through the hash capacity file = h(object). Such cluster is known as a hash table.

http://www.cs.cmu.edu/~adamchik/15-121/lectures/Hashing/hashing.html

III. ASYMMETRIC METHODS

Uneven estimations (open key figuring's) use assorted keys for encryption and unscrambling, and the disentangling key can't (basically) be gotten from the encryption key. Strayed counts are fundamental because they can be used for transmitting encryption keys or other data securely really when the social events have no opportunity to yield to a riddle enter in private.

Sorts of Asymmetric calculations:

- RSA
- Diffie-Hellman
- Computerized Signature Algorithm
- ElGamal
- ECDSA
- XTR

Deviated calculations illustrations:

***Diffie-Hellman*:** Diffie-Hellman is the first uneven encryption estimation, grew in 1976, using discrete logarithms as a piece of a restricted field. It grants two customers to exchange a riddle key more than a fragile medium with no prior insider truths. Diffie-Hellman (DH) is a comprehensively used key exchange count. In various crypto graphical traditions, two social occasions wish to begin conferring. Regardless, we should expect they don't at first have any typical puzzle and consequently can't use riddle key cryptosystems. The key exchange by Diffie-Hellman tradition cures this condition by allowing the improvement of a commonplace puzzle key over an inconsistent correspondence channel. It is considering an issue related to discrete logarithms, specifically the Diffie-Hellman issue. This issue is seen as hard, and it is in a couple of cases as hard as the discrete logarithm issue. The Diffie-Hellman tradition is generally thought to be secure when a suitable numerical social event is used. In particular, the generator part used as a piece of the exponentiations should have a generous period (i.e. demand). Generally, Diffie-Hellman is not executed on gear.

***Advanced Signature Algorithm*:** Advanced Signature Algorithm (DSA) is a United States Federal Government standard or FIPS for cutting edge marks. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Algorithm (DSA), showed in FIPS 186 [1], got in 1993. A minor remedy was issued in 1996 as FIPS 186-1 [2], and the standard was amplified further in 2000 as FIPS 186-2 [3]. Propelled Signature Algorithm (DSA) is similar to the one used by ElGamal imprint figuring. It is truly powerful however not as beneficial as RSA for imprint affirmation. The standard portrays DSS to use the SHA-1 hash work singularly to enroll message digests. The rule issue with DSA is the settled subgroup assess (the solicitation of the generator segment), which controls the security to around only 80 bits. Gear ambushes can be undermining to a couple of use of DSS. Nevertheless, it is by and large used and recognized as an OK computation.

ElGamal: The ElGamal is an open key figure - an uneven key encryption figuring for open key cryptography which is considering the Diffie-Hellman key comprehension. ElGamal is the precursor of DSA.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (418-421), Month: January - March 2015, Available at: www.researchpublish.com

ECDSA: Elliptic Curve DSA (ECDSA) is a variation of the Digital Signature Algorithm (DSA) which works on elliptic bend bunches. Likewise with Elliptic Curve Cryptography by and large, the bit size of people in general key accepted to be required for ECDSA is about double the measure of the security level, in bits.

XTR: XTR is a calculation for unbalanced encryption (open key encryption). XTR is a novel strategy that makes utilization of follows to speak to and ascertain forces of components of a subgroup of a limited field. It is taking into account the primitive fundamental the first open key cryptosystem, the Diffie-Hellman key assention convention. From a security perspective, XTR security depends on the trouble of tackling discrete logarithm related issues in the multiplicative gathering of a limited field. A few preferences of XTR are its quick key era (much speedier than RSA), little key sizes (much littler than RSA, practically identical with ECC for current security settings), and velocity (general similar with ECC for current security settings). Symmetric method is one of the basic and most secure encryption methods. It is also called as private key method. Here, the private key place a major role, anyone who has access of this secret key can able to read all the content of data and can perform both the encryption and decryption. The sender can perform encryption and converts into cipher text by using a key, and the receiver should apply the same key for decryption.

Cipher can be defined in two types depending on the amount of input data which used for both encryption and decryption as “stream cipher” and “block cipher”.

IV. SYMMETRIC ENCRYPTION

Symmetric encryption likewise alluded to as traditional encryption or single key encryption was the main kind of encryption being used before the improvement of open key encryption in 1976.

The symmetric encryption plan has five fixings:

1. Plaintext: This is the first coherent message or information that is bolstered to the calculation as info.

2. Encryption calculation: The encryption calculation performs different substitutions and changes on the plaintext

3. Secret Key: The mystery key is likewise enter to the encryption calculation. The definite substitutions and changes performed rely on upon the key utilized, and the calculation will create an alternate yield relying upon the particular key being utilized at the time.

4. Cipher content: This is the mixed message created as yield. It relies on upon the plaintext and the key. The figure content is an obviously irregular stream of information, the way things are, is incomprehensible.

5. Decryption Algorithm: This is basically the encryption calculation run in converse. It takes the cipher text and the mystery key and produces the first plaintext.

There are two necessities for a symmetric key cryptosystem

•We accept it is unreasonable to decode a message on the premise of the cipher text in addition to learning of the encryption/decoding calculation. As such, we don't have to keep the calculation mystery; we have to keep just the key mystery.

•Sender and the beneficiary must have gotten duplicates of the mystery enter in a safe manner and must keep the key secure. On the off chance that somebody can find the key and knows the calculation, all interchanges utilizing this key is decipherable. We will portray how we can utilize an open key cryptosystem for a protected key trade later in this address.

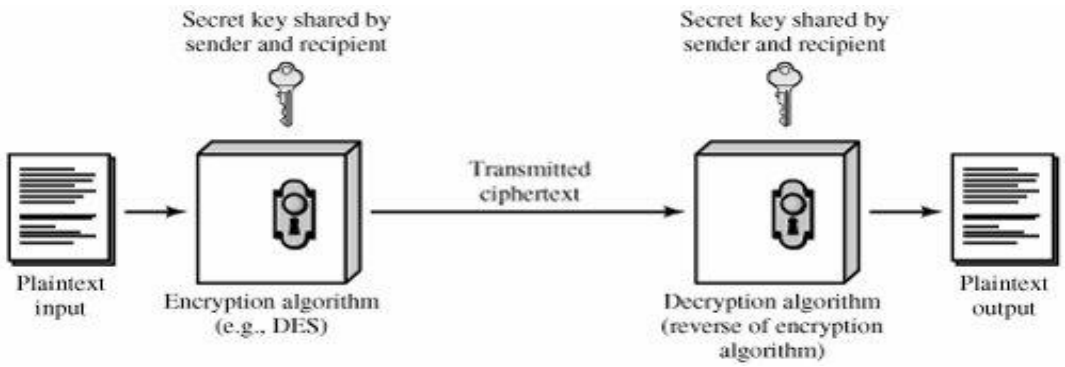

Figure 2: Symmetric Encryption process

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (418-421), Month: January - March 2015, Available at: www.researchpublish.com

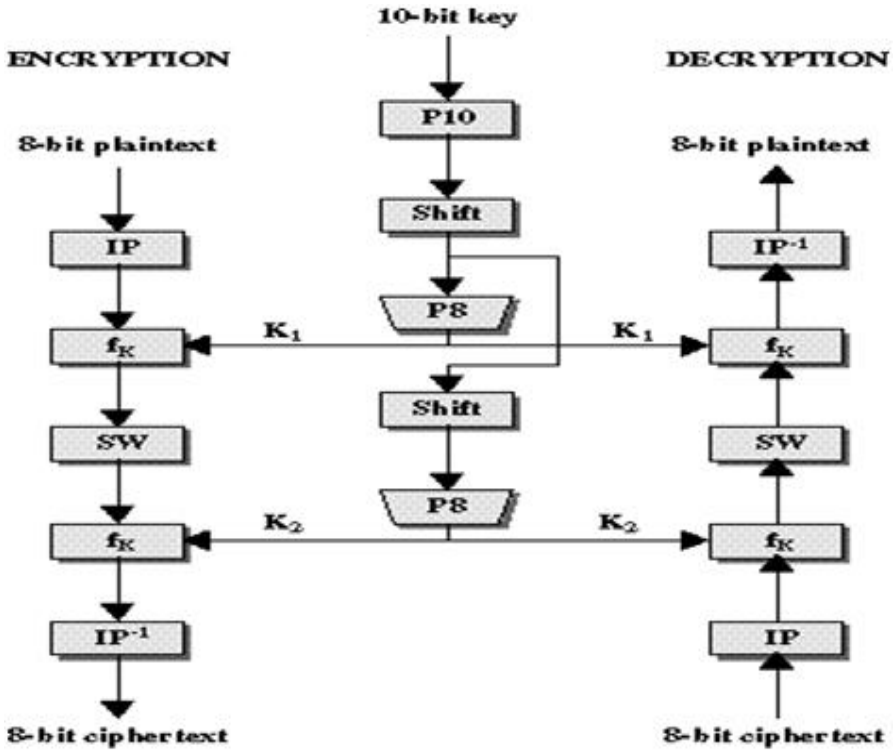

Figure 3: Simplified DES Scheme

V. CONCLUSION

In conclusion, Encryption has started with using simple codes as authentication password which uses to send by sender to the receiver. Nowadays it is providing so many methods to providing security. The popular methods are symmetric and asymmetric. In the symmetric method, public key place major role in providing security whereas in asymmetric method public and private keys helps to provide security. Each method has both advantages and disadvantages. According to the requirement of the sender and receiver party we can choose any of these encryption methods to achieve the network security.

REFERENCES

[1] Victor S.Adamchik, CMU, 2009.
http://www.cs.cmu.edu/~adamchik/15-121/lectures/Hashing/hashing.html

[2] W. Stallings, Cryptography and Network Security: Principles and Practices, 3rd edition, Prentice Hall, NJ, 2003.
http://www4.ncsu.edu/~kksivara/sfwr4c03/lectures/lecture9.pdf

[3] M.Linn, G. Wiesen, C. Wilborn, 2003-2015 Conjecture Corporation.
http://www.wisegeek.org/what-are-the-different-types-of-encryption-methods.htm