A Review Paper on Symmetric Key, Asymmetric key Encryption and Hash Function

[1] Dr. Jitendra Singh Chauhan, [2] Nimisha Khetan

[1]Associate Professor and Head, [2] Research Scholar
[1, 2] Department of Computer Science and Engineering, Aravali Institute of Technical Studies, Udaipur, Rajasthan, India
Email – [1] chauhan.jitendra@live.com, [2]nimishakhetan94@gmail.com

Abstract: *Cryptography provides the various techniques for secure communication of data over networks. It generally, construct and analyze various protocols that deals with the various aspects of information security like confidentiality, integrity, etc. Modern cryptography combines various disciplines of engineering and sciences. There are various applications of cryptography in day to day like ATM cards, computer passwords, and electronic commerce, etc.*
Cryptography is the technique which we called as a synonymous of encryption, which convert the readable and under stable form of information into some other unknown form, which is decoded at the other end to get the desired information using decoding technique provided by the originator of the message, thereby secure data from unwanted persons. In this review paper we are focusing on study of Symmetric Key, Asymmetric key Encryption and Hash Function.

Key Words: *Symmetric Key, Asymmetric key, Encryption, Hash Function, Cryptography.*

1. INTRODUCTION:

With respect to classification cryptography is utilized to scramble information dwelling on capacity gadgets or venturing out however correspondence channels to guarantee that any illicit access isn't fruitful. Likewise, cryptography is utilized to verify the way toward confirming various gatherings endeavoring any capacity on the framework. Since a gathering wishing be conceded a specific usefulness on the framework must present something that demonstrates that they surely who they state they are. That something is once in a while known as certifications and extra estimates must be taken to guarantee that these qualifications are just utilized by their legitimate proprietor. The most great and evident certification are passwords. Passwords are encoded to ensure against unlawful utilization. Approval is a layer based over confirmation as in the gathering is validated by exhibiting the qualifications required (passwords, keen cards and so forth). After the qualifications are acknowledged the approval procedure is begun to guarantee that the mentioning party has the consents to play out the capacities required. Information respectability and Non-Repudiation are accomplished by methods for computerized signature, a strategy that incorporates performing cryptography in addition to other things. In this Paper we are dealing with the review of various cryptographic encryption methods.

2. SYMMETRIC ENCRYPTION SCHEMES:

With symmetric-key encryption, the encryption key can be determined from the decryption key and the other way around. With most symmetric algorithms, a similar key is utilized for both encryption and decryption, as appeared in figure 1. Usage of symmetric key encryption can be exceptionally proficient, with the goal that clients don't encounter any huge time delay because of the encryption and decryption. Symmetric-key encryption additionally gives a level of verification, since data encrypted with one symmetric key can't be decrypted with some other symmetric key. Accordingly, as long as the symmetric key is stayed quiet by the two gatherings utilizing it to encrypt communications, each gathering can make certain that it is speaking with the different as long as the decrypted messages keep on appearing well and good.

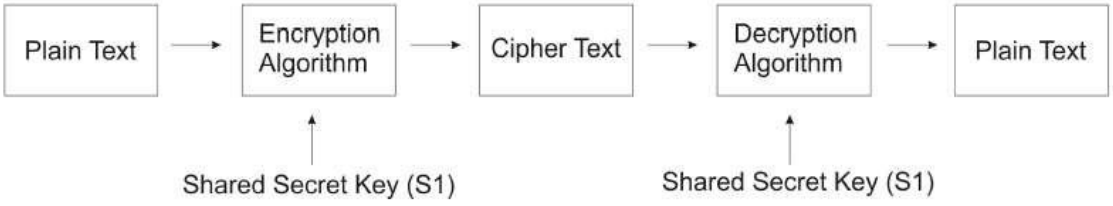

Figure 1 General Symmetric Key Encryption Method

Encryption works regularly take a fixed-measure input to a fixed-size output, so encryption of longer units of information must be done in one of two different ways: either a block is encrypted at once and the blocks are by one

way or another consolidated to make the figure content, or longer key is created structure a shorter one and XORed against the plaintext to make the figure content. Schemes of the previous sort are called block ciphers, and schemes of the last kind are called stream ciphers.

3. ASYMMETRIC-KEY ENCRYPTION:

The most commonly used implementations of asymmetric-key [7, 8] encryption are based on algorithms patented by RSA data security. Hence, the RSA approach to public-key encryption is described in this section. Asymmetric key encryption (also called public key encryption) involves a pair of keys a public key and a private key, used for security & authentication of data. Data encrypted with one key can be decrypted only with other key as each public key is published, and the corresponding private key is kept secret. The scheme shown in figure 2 says public key is distributed and encryption being done using this key. In general, to general, to send encrypted data, one encrypt the data with the receiver's public key, and the person receiving the encrypted data decrypts it with his private key. Compared with symmetric-key encryption, public-key encryption more computation and is therefore not always appropriate for large amounts of data. However, real time environment uses a combination of symmetric & asymmetric schemes. The SSL protocol uses this approach. As it happens, the reverse of the scheme shown in figure 3.4 also works as, Data encrypted with one's private key can be decrypted only with his public key. This may not be an interesting way to encrypt important data, however, because it means that anyone with receiver's public key, which is by definition published, could decipher the data. And also the important requirement with data transfer is authentication of data which is supported with asymmetric encryption schemes, which is an important requirement for electronic commerce and other commercial applications of cryptography.

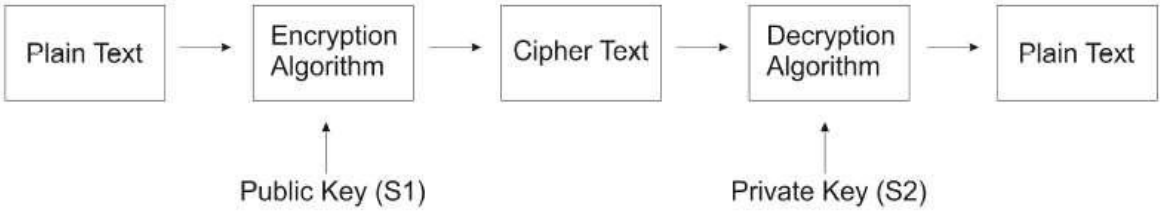

Figure 2 General Structure of Asymmetric Key Encryption

4. HASH FUNCTION:

Hash functions uses, no key and also called as message digests. Instead, a fixed length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are mainly used to achieve principle of confidentiality and integrity. Hashing methods are useful when we don't have trust on the other person with which we are sharing information. If say you have a suppression list of email addresses and you want someone else to remove them from their database, but you don't want to actually share the list of email addresses with them send the other party the list of digests. They can to through their database and generate the digest for each of their email addresses.

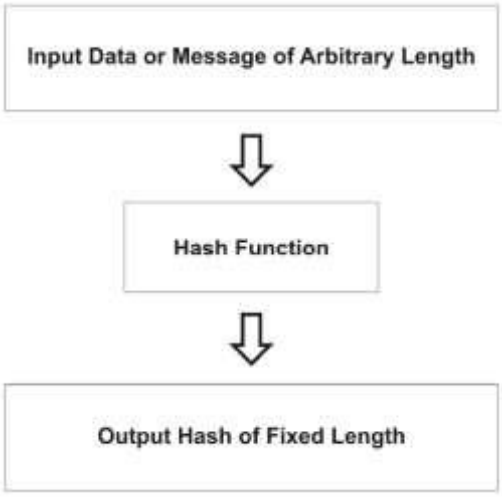

Figure 3 Flow of Hash Function

5. THE PRINCIPLES OF CRYPTOGRAPHY:

Security often requires that data be kept safe from unauthorized access. The main emphasis of defense is based on physical security. Physical security is always not an appropriate option. Computers are mostly interconnected via appropriate communication channels for transferring data.
The five major principles of security are:
1. Confidentiality: assuring that private data remains private.
2. Authentication: Assuring the identity of all parties attempting access.
3. Authorization: assuring that a certain party attempting to perform a function has the permissions to do so.
4. Data integrity: assuring that an object is not altered illegally.
5. Non-Repudiation: assuring against a party denying a data of a communication that was initiated by them.

6. CONCLUSION:

In this paper, we have studied the basic of Symmetric key encryption, Asymmetric key encryption and Hash function. The principles of cryptography are also illustrated in this review paper.

REFERENCES:

1. B. Schneier The two-fish encryption algorithm a 128 bit block cipher. J. Wiley, 1999.
2. "Data encryption standard." Federal Information Processing Standards Publication 46, 1977.
3. "Advanced encryption standard." Federal Information Processing Standards Publication 197, 2001.
4. G. Chen, Y. Mao, and C. K. Chui "A symmetric image encryption scheme based on 3d chaotic cat maps." Chaos Solitons and Fractals, vol. 21, no. 3, pp. 749-761, 2004, DOI: 10.1016/j. chaos. 2003.12.022.
5. Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3rd chotic baker maps", International Journal of Bifurcation and Chaos. 2003.
6. A Torrubia and F. Mora "Perceptual cryptography of jpeg compressed images on the bit- stream domain" in Consumer Electronics, 2003. ICCE. 2003 IEEE International Conference on, june 2003, pp.58-59.
7. F. Ahmed, M. Siyal and V. Abbas, "A perceptually scalable and jpeg compression tolerant image encryption scheme," in Image and Video Technology (PSIVT), 2010 Fourth Pacific-Rim Symposium on nov. 2010, pp. 232-238.
8. M. Khan, V. Jeoti, and M. Khan, "Perceptual encryption of jpeg compressed images using dct coefficients and splitting of dc coefficients into bitplanes," in Intelligent and Advanced Systems (ICIAS), 2010 International Conference on june 2010, pp. 1-6.
9. O. Matoba, T. Nomura, E. Perez-Cabre, M. Millan, and B. Javidi "Optical techniques for information security" Proceedings of the IEEE, vol. 97 no 6, pp. 1123-1148, june 2009.