INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A REVIEW ON CRYPTOGRAPHY

KU PUNAM P. HARKUT, PROF P. G. ANGAITKAR

I.B.S.S College of Engineering, Amravati.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: This paper includes detailed information about cryptography. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. That is, Cryptography is a simple technique used for converting a simple plain text message into cipher text message. Any communication in the language that you and I speak—that is the human language, takes the form of plain text or clear text. That is, a message in plain text can be understood by anybody knowing the language as long as the message is not codified in any manner[1]. So, now we have to use coding scheme to ensure that information is hidden from anyone for whom it is not intended, even those who can see the coded data. There are two basic types of cryptography: Symmetric Key and Asymmetric Key. Symmetric key algorithms are the quickest and most commonly used type of encryption. Here, a single key is used for both encryption and decryption. There are few well-known symmetric key and Asymmetric Key algorithms i.e. AES, DES, RC2, RC4, RSA etc.

Keywords: Cryptography, Plain text, Cipher text, Encryption, Decryption, Symmetric Key, Asymmetric Key

Corresponding Author: KU PUNAM P. HARKUT

Access Online On:

www.ijpret.com

How to Cite This Article:

Punam Harkut, IJPRET, 2014; Volume 2 (9): 594-600

PAPER-QR CODE

INTRODUCTION

Student records, etc. Privacy is a critical issue in many of these applications, how are we needed to make sure that unauthorized parties cannot read or modify messages.

Cryptography is the transformation of readable and understandable data into a form which cannot be understood in order to secure data. Cryptography refers exactly to the methodology of concealing the content of messages, the word cryptography comes from the Greek word "Kryptos", that means hidden, and "graphikos" which means writing **[2].**

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key—a word, number, or phrase—to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. The information that we need to hide, is called **plain text,** it's the original text, and it could be in a form of characters, numerical data, executable programs, pictures, or any other kind of information. The plaintext for example is the first draft of a message in the sender before encryption, or it is the text at the receiver after decryption. The data that will be transmitted is called **cipher text,** it's a term refers to the string of "*meaningless"* data, or unclear text that nobody must understand, except the recipients. it is the data that will be transmitted Exactly through network, Many algorithms are used to transform plaintext into cipher text **[4].** The input to an encryption process is commonly called the **plain text,** and the output the **cipher text**.

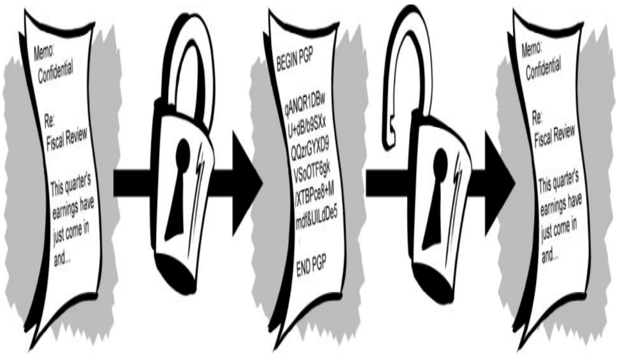

Figure 1. Encryption and decryption

Plaintext encryption ciphertext decryption plaintext

Encryption is the process of encoding a message so that its meaning is not obvious; **Decryption** is the reverse process transforming an encrypted message back into its normal original form.

That is, we can encrypt original message to hide its meaning. Then we decrypt it to revel the original message. A system for encryption and decryption is called Cryptosystem.**[5].**

Symmetric encryption refers to the process of converting plaintext into cipher text at the sender with the same key that will be used to retrieve plaintext from cipher text at the recipient. While **asymmetric encryption** refers to the process of converting plaintext into cipher text at the sender with different key that will be used to retrieve plaintext from cipher text at the recipient **[3].**

Nowadays, cryptography plays a major role in protecting the information of technology applications. Information security is an important issue, for some applications. Have the top priority such as e-commerce, e-banking, e-mail, medical databases, and so many more, all of them require the exchange of private information. For example, let us consider a person named Alice a sender who wants to send a data message which has a length of characters to a receiver called Bob. Alice uses an unsecure communication channel. This could be a telephone line, computer network, or any other channel. If the message contains secret data, they could be intercepted and read by hackers. Also they may change or modify the message during its transmission in such a way that Bob would not be able to discover the change. In this survey a various ways of encryption is viewed and have been compared, a lot of examples have been provided.

2. LITERATURE REVIEW

Cryptography comes from the Greek words for “secret writing.” Cryptography is the art and science of achieving security by encoding message to make them non-readable. And Cryptanalysis is the technique of decoding message from a non-readable format back to readable format. Whereas the combination of cryptography and cryptanalysis is refer as cryptology.

Goals of Cryptography:

By using cryptography many goals can be achieved, these goals are:

a. Confidentiality: it is the most important goal, that ensures that nobody can understand the

received message except the one who has the decipher key.

b. Authentication: it is the process of proving the identity, that assures the communicating entity is the one that it claimed to be, This means that the user or the system can prove their own identities to other parties who don’t have personal knowledge of their identities.

c. Data Integrity: its ensures that the received message has not been altered in any way from its original form, This can be achieved by using hashing at both sides the sender and the recipient in order to create a unique message digest and compare it with the one that received.

d. Non-Repudiation: it is mechanism used to prove that the sender really sent this message, and The message was received by the specified party, so the recipient cannot claim that the message was not sent.[5]

e. Access Control: it is the process of preventing an unauthorized use of resources. This goal Controls who can have access to the resources, If one can access, under which restrictions and Conditions the access can be occurred, and what is the permission level of a given access.

Types of Cryptography:

Cryptography is a process which is associated with scrambling plaintext into cipher text, then back again into plain text. There are several ways to classify the various algorithms. The most common types are **Secret Key Cryptography** which is also known as Symmetric Key Cryptography and **Public Key Cryptography** which is also known as Asymmetric Key Cryptography. These are two basic types of cryptography: Symmetric Key and Asymmetric Key Cryptography. This is shown in Figure below:

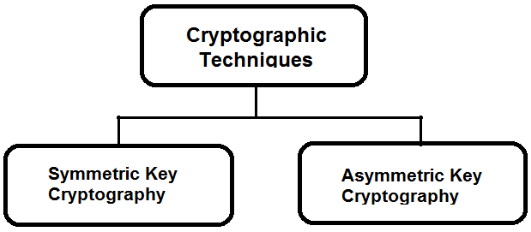

Figure 2. Cryptography techniques

Secret key cryptography

In secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 3, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key. Symmetric key algorithms are the quickest and most commonly used type of encryption.

Public key cryptography

Public or asymmetric key cryptography involves the use of key pairs: one private key and one public key. Both are required to encrypt and decrypt a message or transmission. The private key, not to be confused with the key utilized in private key cryptography, is just that, private. It is not to be shared with anyone. The owner of the key is responsible for securing it in such a manner that it will not be lost or compromised. On the other hand, the public key is just that, public. Public key cryptography intends for public keys to be accessible to all users. In fact, this is what makes the system strong. If a person can access anyone public key easily, usually via some form of directory service, then the two parties can communicate securely and with little effort, i.e. without a prior key distribution arrangement Figure 4 describes the Public Key Cryptography.

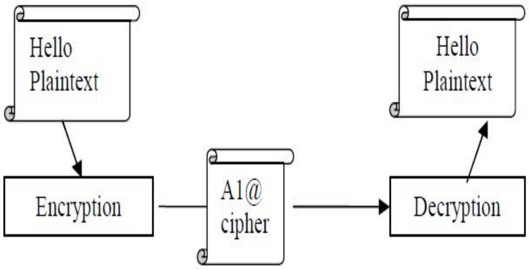

Figure 3.Secret Key Cryptography[9]

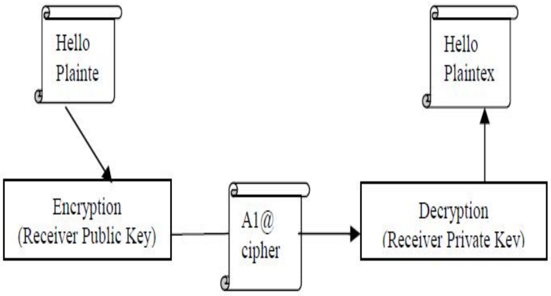

Figure 4. Public Key Cryptography[9]

Comparison Public Key & Secret Key

Table 1. Comparing Secret Key and Public Key Encryption [6]

Component	Secret Key(Symmetric)	Public Key(Asymmetric)
Number of Keys	1	2
Protection of Key	Must be kept secret	One key must be kept secret; the other can be freely exposed
Best Uses	Cryptographic workhorse; secrecy and integrity of data-single characters to blocks of data,message,files	Key exchange, authentication
Key Distribution	Must be out-of-band	Public key can be used to distribute other keys
Speed	Fast	Slow;typically,10,000 times slower than secret key

3.Application of Cryptography

Cryptography is used to protect e-mail messages, credit card information, and corporate data. One of the most popular cryptography systems used on the Internet is *Pretty Good Privacy* because it's effective and free.

Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography.

4. CONCLUSION

Cryptography is used to achieve few goals like Confidentiality, Data integrity, Authentication etc. Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. Confidentiality means nobody can understand the received message except the one that has the decipher key, and "data cannot be changed" means the original information would not be changed or modified; this is done when the sender includes a cryptographic operation called a hash function in the original message.

REFERENCES

1. ATUL KAHATE**,**"Computer and Network Security" Second Edition.

2. J.R Childs: " General Solution of the ADFGVX Cipher System ". Aegean Park Press, (2000), USA.

3. D.Salomon" Data Privacy and Security "First Edition. Springer-Verlag New York, (2003): USA.

4. D.Delfs., and K. Helmut., " Introduction to Cryptography: Principles and applications ", Second Edition. Springer Science & Business Media, (2007), Germany.

5. M. Chapple., M Solomon,: " Information Security Illuminated " First Edition. Jones and Bartlett Publishers, (2005), USA.

6. C.P. Pfleeger and S. L. P fleeger," Security in Computing", Pearson Education (LPE)

7. Introduction to Public-Key Cryptography", an article available At developer.netscape.com/docs/manuals/security/pkin/contents.htm

8. W .Stallings, "Cryptography and network security, Principles and practices ", Fourth Edition. Pearson Prentice Hall, (2006):, USA

9. Ayushi," A Symmetric Key Cryptographic Algorithm" 2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15