International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 1 | ISSN : 2456-3307

Study on Cryptography and Techniques

Shivani Sharma, Yash Gupta
Tata Consultancy Services, Noida, Uttar Pradesh, India

ABSTRACT

In today's information age, communication play a very important role which help in growth of new technologies. So security is an essential parameter to be considered. A mechanism is therefore needed to secure the information that is sent. The process of transforming the original information into an unreadable format is known as encryption. The process of again converting the unreadable format in to the original information is known as decryption. The study of both encryption and decryption is known as cryptography. This paper focuses on analysing different types of cryptography, concept of encryption and decryption, a brief introduction to cryptography techniques. If we are taking about security of information then following services come in mind i.e. Confidentiality (privacy of information), Authentication, Integrity (has not been altered) .This paper provides a detailed description of all these cryptography techniques and a public key cryptography algorithm RSA.

Keywords : Information, cryptography, symmetric key, asymmetric key, Cipher text, Plain text, RSA Algorithm

I. INTRODUCTION

A plain or normal text, which is send over the network is firstly get transformed into cipher text so that only the sender and the recipient can use the information. In technical terms, the process of encoding plain text messages into cipher text messages is known as encryption. Transformation process of cipher text again into plain text is known as decryption. Decryption is just opposite to encryption. In computer to computer communications, the computer at sender's end usually transforms a plain text messages into cipher text messages by performing encryption. Then this message is sent to the receiver over the network. The receiver's computer takes the encrypted message and performs the decryption process to obtain plain text. The process of encryption and decryption is known as cryptography. In general cryptography is the art and science of achieving security by encoding message to make them non readable. It can be used to hide the meaning of information in any form. It can also be applied to software, graphics or voice.

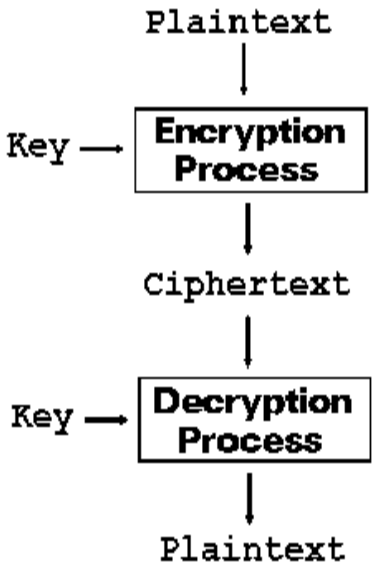

Figure1. Cryptography Process

Cryptography is the art of secret coding. The basic service provided by cryptography is the ability to send the information between participants in a way that prevents others reading it. The main purpose of the cryptography is used not only to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication, non-repudiation.

Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information. Presently continuous researches on the new cryptographic algorithms are going on. However, it is a very difficult to find out the specific algorithm, because we have already known that they must consider many factors like: security, the features of algorithm, the time complexity and space complexity.

II. TERMINOLOGIES

1) Plain text -original message
2) Cipher text- coded message
3) Encrypt -convert plain text into coded text
4) Decrypt - convert coded text into plain text
5) Cryptography-study of encryption principles and methods.

III. PURPOSE OF CRYPTOGRAPHY

In data and telecommunications, cryptography is necessary when communicating over any non-trusted medium, which includes just about any network, particularly the Internet.

Within the context of any application-to-application communication, there are some specific security requirements, including:

1) Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address based, both of which are notoriously weak.)
2) Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
3) Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
4) Non-repudiation: A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext.

IV. ENCRYPTION APPROACH

In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted Encryption has long been used by militaries and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines.

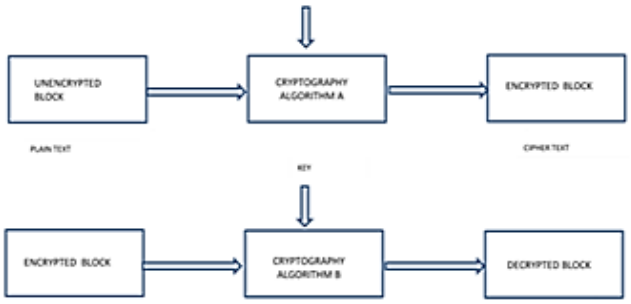

Figure 2. Encryption Method

In the proposed technique we have a common key between sander and receiver, which is known as private key. Basically private key concept is the symmetric key concepts where plain text is converting into encrypted text known as cipher text using private key where cipher text decrypted by same private key into plane text. The encryption key is trivially related to the decryption key.

V. CRYPTOGRAPHY TECHNIQUES

There are two basic techniques for encrypting information: symmetric encryption (also called secret key encryption) and asymmetric encryption (also called public key encryption).

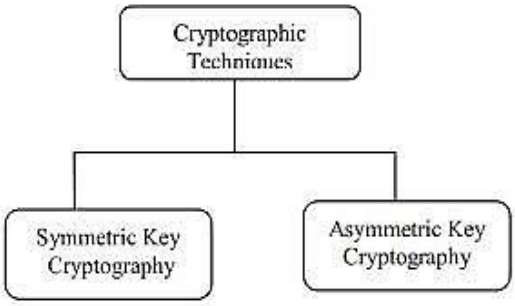

Figure 3. Techniques

Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. Asymmetric encryption, in which there are two related keys--a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it.

A. Symmetric Key Cryptography

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key .Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher. Symmetric are much faster than asymmetric cryptography.

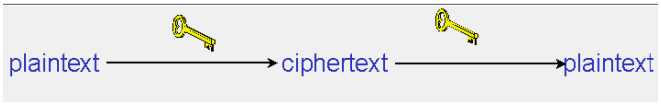

Figure4. Symmetric key Used

B. Asymmetric Key Cryptography-

Asymmetric-key cryptography refers to encryption methods in which both the sender and receiver share the different key. One key is used for encryption and another for decryption. This provides more stability than symmetric systems.

Figure 5. Asymmetric key Used

VI.ALGORITHMS:

For cryptography techniques, different types of algorithms are used for both symmetric and asymmetric key techniques. The algorithms for private (symmetric) key are DES (Data Encryption Standard), AES etc. and for public(asymmetric)key are RSA (Rivest , Shamir , Adlemen), Diffie-Hellman: etc.

A. RSA Algorithm

RSA stands for Rivest Shamir and Adleman name of three inventors. RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977.

B. Key Generation:

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

1) Choose two distinct prime numbers p and q.
2) For security purposes, the integers p and q should be chosen at random.
3) Compute n = pq.
4) n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
5) Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n - (p + q - 1)$, where φ is Euler's totient function. This value is kept private.
6) Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime.
7) e is released as the public key exponent.
8) Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., d is the modular multiplicative inverse of e (modulo $\varphi(n)$).
9) d is kept as the private key exponent.

Encryption
Ciphertext c corresponding to calculated as:

$$c \equiv m^e \pmod{n}$$

Decryption

Plain text can be calculated as:

$$m \equiv c^d \pmod{n}$$

C. Disadvantages

In RSA encryption that is a deterministic encryption algorithm (i.e., has no random component) an attacker can successfully launch a chosen plaintext attack against the cryptosystem.

RSA has the property that the product of two cipher texts is equal to the encryption of the product of the respective plaintexts. That is m1em2e ≡ (m1m2)e (mod n). Because of this multiplicative property a chosen-cipher text attack is possible.

VII. CONCLUSION AND FUTURE WORK:

Cryptography is a very interesting field in computer science area because the amount of work done is only kept secret. There are various techniques and algorithm studied and different types of research have been done. The best algorithms are those which are well documented and well known because the algorithms are well tested and well studied. This paper further studied that symmetric key cryptography are more faster than asymmetric systems. But asymmetric key cryptography are more scalable and provide more authentication and non- repudiation easily. But there us still need to develop such an algorithm that makes the encryption decryption process more easier than RSA, DES and many more algorithms.

VIII. REFERENCES

[1] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE.

[2] Symmetric key cryptography using random key generator, A.Nath, S.Ghosh, M.A.Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239-244.

[3] Data Hiding and Retrieval, A.Nath, S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.

[4] Neal Koblitz "A Course in Number Theory and Cryptography" Second Edition Published by Springer-Verlag.

[5] T Morkel, JHP Eloff " ENCRYPTION TECHNIQUES: A TIMELINE APPROACH" published in Information and Computer Security Architecture (ICSA) Research Group proceeding.

[6] Text book William Stallings, Data and Computer Communications, 6eWilliam 6e 2005.

[7] Md. Nazrul Islam, Md. Monir Hossain Mia, Muhammad F. I. Chowdhury, M.A. Matin "Effect of Security Increment to Symmetric Data Encryption through AES Methodology" Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 978-0-7695-3263-9/08 DOI 10.1109/SNPD.2008.101 IEEE 2008.

[8] Joan Daemen and Vincent Rijmen, AES submission document on Rijndael, Version 2, September 1999.