

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 2 ISSUE : 2 Print / Issue Publication Date: 27-Jan-2017

ISSN : 2455-2143

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 2, Issue 2, ISSN No. 2455-2143, Pages 109-112
Published Online December-January 2016 in IJEAST (http://www.ijeast.com)

A REVIEW ON CRYPTOGRAPHY ALGORITHMS, ATTACKS AND SECURITY

Rajendra Kumar

Namrata Dhanda
Department of CSE
G I T M Lucknow

Abstract— **Data Security has become crucial aspect in every sectors .Therefore order to protect it various methods and Algorithm has been implemented. Cryptography combines Mathematics, Computer Science (both Software and Hardware), Engineering and Networking. In this paper we have reviewed different type cryptography algorithms. What are the different types of attacks to slow down network are defined. Basic tools of encryption for secure messaging transformation and connectivity are listed out.**

Keywords— **algorithm, cryptography, data, encryption, decryption, type of cryptography, technique of cryptography, security**

I. HISTORY AND INTRODUCTION

To protecting data has become a very difficult task. Every company and organization today must have strategies regarding data security .In order to provide security some algorithms, tools must be implemented. Cryptograph often called "code breaking" exists way back from many years ago. Most of there were used during wars to send messages and data in hidden format. Cryptography is mainly concern with algorithm. The initial recognized application of cryptography is originated from the Old Kingdom of Egypt circa 1900 B.C. Cryptography was design in such a way to send message in coded format and would easily receiver to read the message who was knows to decode it. The sixth century BC, consisted of covering a roll of paper around a cylinder and then writing the message on the paper. The unrolled papers were send to the recipient, who could easily decode the message if they were knew the diameter of the unique cylinder. 2000 years ago Julius Caesar was used a simple switch over cipher, representing as the Caesar cipher, Roger bacon described a number of methods in 1200s. In simply Cryptography is the technique to convert the message (Plain text) into coded message (encrypt) from Sender and transmit it to Receiver who converts(decrypt) the message into readable format(Plain text) after receiving it to avoid the message from getting damaged or lost and in order to protect it. Cryptography has been very important for data transmission. Different types of algorithms of cryptography have been studied.

Security Services: In security of information then following components need to be considered. *Data Integrity:* it is 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.

Non-Repudiation: This plan is used to prove that the sender really sent this message, and the message was received by the specified party, so the recipient cannot be claimed that the message was not sent.

Authentication: Authentication is the process of proving the identity, that guaranteed the communicating entity is that who one to be claimed, this means that the user can prove their own identities to other parties who do not have any personal knowledge of their identities.

Confidentiality: The most important issue, that ensures that none of any one can understand the received message except the one who has the encrypted by a key.

II. ENCRYPTION

Encryption is basically a process or algorithm to make information hidden or secret. It is considered as the subset of cryptography. It is the actual process of applying cryptography. It is the process to transform or converting the data into some another form that appears to be random, meaningless and unintelligible. It can also be said that encryption is the process of transforming plaintext into the ciphertext where plaintext is the input to the encryption process and ciphertext is the output of the encryption process.

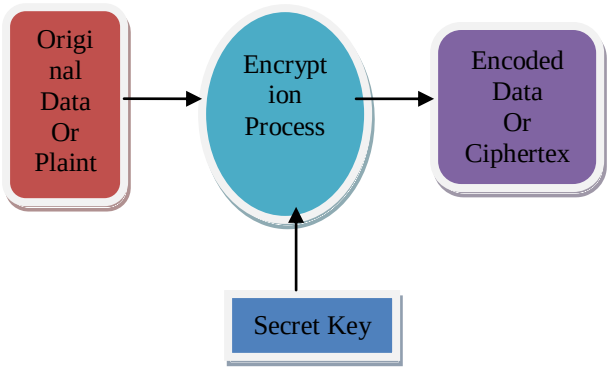


Fig.1. Encryption process

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 2, Issue 2, ISSN No. 2455-2143, Pages 109-112
Published Online December-January 2016 in IJEAST (http://www.ijeast.com)

III. DECRYPTION

It is the process to transform or converting the encoded data into some meaningful form. It can also be said that decryption is the process of transforming cipher text into the plaintext where ciphertext is the input to the decryption process and plaintext is the output of the decryption process.

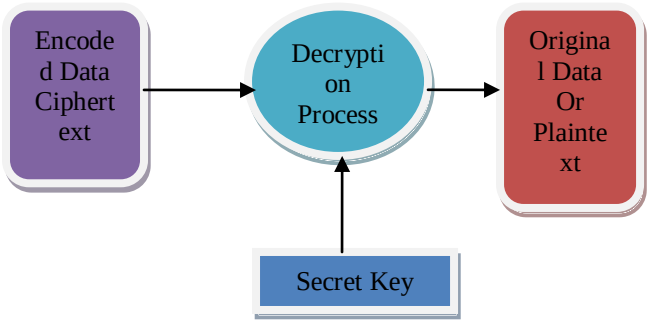


Fig.2. Decryption Process

IV. TYPES OF CRYPTOGRAPHY

The modern cryptography is classified into two types-

1. Symmetric Key Cryptography
2. Asymmetric Key Cryptography.

A. Symmetric Key Cryptography: In Symmetric Key algorithms, only one key is used for both encryption and decryption process. Both the parties must agree on the secret key before the actual exchange of data takes place. The sender uses this key for encryption algorithm to encrypt data; the receiver uses the same key for corresponding decryption algorithm to decrypt the data. Symmetric Key Ciphers are basically classified into two categories –Stream Ciphers and Block Ciphers. A stream cipher breaks the plaintext T into successive characters or bits t1,t2,.. and enciphers each ti with the ith element ki of a key stream K = k1,k2. . . whereas , a block cipher breaks T into successive blocks (each block is typically several characters long.) T1,T2 . . . . . and enciphers each Ti with the same key K; that is , EK(T) = EK(T1)EK(T2) . . .

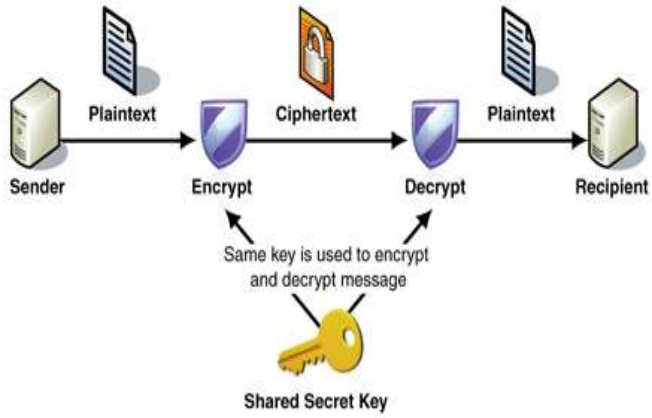


Fig.3. **Symmetric Key Cryptography**

B. Asymmetric or Public-key cryptography: Asymmetric Cryptography refers to a cryptographic system requiring two different keys, one is to be encrypt the plaintext, and other is to be decrypt the cipher text. One of these keys is published or public and the other is kept private. Public key algorithms, unlike symmetric key algorithms, do not require a secure initial exchange of secret keys between the parties. Public-key cryptography is used as a method of assure the confidentiality, authenticity and non-reputability of electronic communications and data storage.

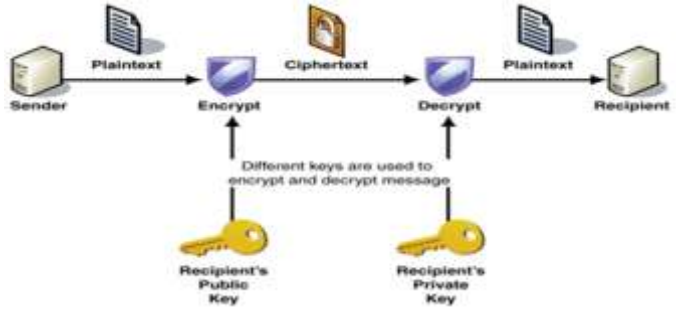


Fig.4. Asymmetric Key Cryptography

V. REVIEW OF VARIOUS CRYPTOGRAPHIC TECHNIQUES

Data Encryption Standard*:* The Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of electronic data. DES was highly influential in the advancement of modern cryptography in academic world. DES is a block cipher that enciphers 64-bit blocks of data with a 56-bit key the remaining eight bits are used for checking parity. Decryption uses the same structure as in encryption but with the keys used in just reverse order. These are advantages that the same hardware or software can be used in both parties.

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 2, Issue 2, ISSN No. 2455-2143, Pages 109-112
Published Online December-January 2016 in IJEAST (http://www.ijeast.com)



Due to a relatively short key length, DES was done to many attacks. DES can be broken under a known-plaintext attack by exhaustive search. It was also observed that a special purpose machine consisting of a million LSI chips could try all 256 ≈ 7 X 10 16 keys in 1 day. DES is not an ideal encryption technique in modern cryptography; instead it is used in mode of operation.

Asymmetric Encryption Standard*:* AES is a symmetric key block cipher and is fast in both software and hardware. AES has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. The AES algorithm holds a 4*4 array of bytes called the state, that is initialized to the input of 128 bits (i.e., 16 bytes) to the cipher. The substitution and permutation operations are all applied to state array. There 4 different stages in every round of AES .It can be implemented on various platforms especially on small devices.

Rivest, Shamir Adleman*:* RSA is a public-key cryptosystem and is widely used for secure data transmission. In RSA, the encryption key is public and different from the decryption key which is to be kept secret. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The public key consists of the modulus n and the public (or encryption) exponent e. The modulus n is the product of two large prime numbers p and q. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret because they can be used to calculated.

Diffie–Hellman Key Exchange: DHKE is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange to the other is implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that they have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. The scheme was first published by Whitfield Diffie and Martin Hellman in 1976. Although Diffie–Hellman key agreement itself is an anonymous (non-authenticated) key-agreement protocol, it provides the basis for a variety of authenticated protocols, and is used to provide perfect forward secrecy in Transport Layer Security's ephemeral modes.

Elliptic Curves: *Elliptic* curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography. Elliptic Curve Cryptography (ECC) is a newer approach, and considered as a marvelous technique with low key size for the user, and have a hard exponential time challenge for an intruder to break into the system. In ECC a 160-bit key provides the same security as compared to the traditional crypto system RSA with a 1024-bit key, thus lowers the computer power. Therefore, ECC offers considerably greater security for a given key size. Consequently, a key with smaller size makes it possible a much more compact implementations for a given level of security.

ElGamal Encryption: The ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography is based on the Diffie–Hellman key exchange. It can be viewed as an extension of the DHKE protocol. Not surprisingly, its security is also based on the intractability of the discrete logarithm problem and the Diffie–Hellman problem. We consider the Elgamal encryption scheme over the group $Z*p$, where p is a prime. The protocol consists of two phases, the classical DHKE which is followed by the message encryption and decryption.

TYPES OF ATTACK

Security Threats

There are an amount of security threats that can be the beginning of a network security attack. Most important security threats are denial of service, distributed denial of service, viruses, Trojan horses, spywares, malwares, illegal way in to the network property and data, accidental erasure of the records and the uncontrolled internet access.

Data stealing and cryptography attacks

One more threat to a network is loss of the major information and this loss can be prohibited, if you use good encryption methods such as 128 bit security or 256 bit security encryption techniques. In this manner your data when transferred during FTP programs, can be encrypted and cannot be read or use.

Virus assault

A computer virus is a program or an executable code that when executed and computer-generated, act upon different unwanted and damaging functions for a computer and a network. Viruses know how to destroy down your hard disks and processors, utilize memory at a very large scale and wipe out the overall performance of a computer or network. A Trojan is a malicious code that performs critical actions but it cannot be replicated. Trojan is capable of erasing systems important records. A computer worm is a program that replicates to all network and wipe out useful information. The viruses, malware, adware and Trojan horses can be controlled if you have a modernized antivirus program with the most up to date pattern files.

Unauthorized application installations

An additional virus and security assault prevention method is to install only the certified software applications to our set of connections i.e. server and all client computers. No one should be permitted to install any kind of program which can be source of security threats such as songs or video programs, gaming software or additional internet based applications.

Application-Level Attacks

The invader exploits the limitation in the application layer – for example, security limitation in the web server, or in faulty controls in the filtering of an input on the server side.

Unauthorized Access

Admission to the network resources and records should be allowed only to the approved persons. Every common folder



and resources in your network must have been accessed only by the sanctioned persons and supposed to be scanned and monitored repeatedly.

CYBER SECURITY TECHNOLOGIES:

Access Control and Identity Management:
The username/password combination has been a fundamental of computer access control since the early 1960s.
Authentication: Documents need to be authenticated as having originated from a trusted source and that they have not been subsequently altered.
Firewalls:
A firewall program will monitor traffic both into and out of a computer and alert the user to apparent unauthorized usage.
Malware scanners:
Software that is regularly scans files and messages for malicious code.
Cryptography:
It is used in two main ways in information security. The better known is to provide confidentiality by encrypting stored data and data in transit.

SUMMARY

Cryptography makes sure that the data when transferred over network is not modified. So in order to maintain data privacy cryptography algorithms are used to prevent the data being altered while in transit state. One can maintain security by having setup like anti-virus, anti-malware, regular updates, monitoring, spreading awareness and education.

V. REFERENCE

[1]Pawlan, M. (1998, February). Cryptography: the ancient art of secret messages. Retrieved May 4, 2009, from http://www.pawlan.com/Monica/crypto/.

[1] [2] Pranab Garg1, Jaswinder Singh Dilawari2, A Review Paper on Cryptography and Significance of Key Length, IJCSCE Special issue on“Emerging Trends in Engineering” ICETIE 2012.

[2] [3] Gary C. Kessler, An Overview of Cryptography, 1998-2015 — A much shorter, edited version of this paper appears in the 1999 Edition of Handbook on Local Area Networks, published by Auerbach in September 1998., http://www.garykessler.net/library/crypto.html.

[3] [4] Vishwa gupta,2. Gajendra Singh ,3.Ravindra Gupta, Advance cryptography algorithm for improving data security, www.ijarcsse.com, Volume 2, Issue 1, January 2012 ISSN: 2277 128X.

[4] [5] Siddharth Ghansela, Network Security: Attacks, Tools and Techniques, www.ijarcsse.com, Volume 3, Issue 6, June 2013 ISSN: 2277 128X.

[5] [6] http://www.crypto-it.net/eng/theory/introduction.html.

[6] [7] Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha, “Throughput Analysis of Various Encryption Algorithms”, International Journal of Computer Science and Technology, Vol. 2, Issue 3, Septemver 2011.

[7] [8] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud, “Evaluating the Performance of Symmetric Encryption Algorithms”, International Journal of Network Security, Vol.10, No.3, PP.216–222, May 2010.

[8] [9] Gary C. Kessler “An Overview of Cryptography , May 1998.

[9]

[10] H. Daren, L. Jifuen,H. Jiwu, and L. Hongmei, "A DWT-Based Image Watermarking Algorithm", in *Proceedings of the IEEE International Conference on Multimedia and Expo*, pp. 429-432, 2001.

[11] C. Hsu and J. Wu, "Multi-resolution Watermarking for Digital Images", *IEEE Transactions on Circuits and Systems- II*, Vol. 45, No. 8, pp. 1097-1101, August 1998.

[12] R. Mehul, "Discrete Wavelet Transform Based Multiple Watermarking Scheme", in *Proceedings of the 2003 IEEE TENCON*, pp. 935-938, 2003.

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE AND TECHNOLOGY

AUTHORS

Rajendra Kumar

Namrata Dhanda

ABOUT IJEAST

International journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high - quality research paper in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

JOURNAL METRICS

H-INDEX	i10-INDEX	IJEAST CITATIONS	PEER-REVIEWED & OPEN ACCESS
33	154	9,647 (IJEAST CITATIONS)	PUBLISHED MONTHLY

PEER REVIEWED

All submission are rigorously peer reviewed to ensure quality.

AUTHORS ARE OUR PRIORITY

We value our authors and recognize their contribution to the advancement of research and knowledge.

OPEN ACCESS

Free and unrestricted access to research for all.

GLOBAL REACH

Connecting researchers and professionals worldwide.

TIMELY PUBLICATION

We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

editor@ijeast.com

www.ijeast.com

India

2455-2143