International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 5, Issue 3 (September '2019)

NETWORK SECURITY WITH CRYPTOGRAPHY ANALYSIS TECHNIQUES

Gulshan Kumar,
Assistant Professor in Computer Department,
Swami Premanand Mahavidyalaya (SPN College),
Mukerian, Punjab, India.

Abstract: Cryptography is a technique used today hiding any confidential information from the attack of an intruder. Today data communication mainly depends upon digital data communication, where prior requirement is data security, so that data should reach to the intended user. The protection of multimedia data, sensitive information like credit cards, banking transactions and social security numbers is becoming very important. Data is any type of stored digital information. Security is about the protection of assets. Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, personal databases and websites. Cryptography is evergreen and developments. Cryptography protects users by providing functionality for the encryption of data and authentication of other users. Compression is the process of reducing the number of bits or bytes needed to represent a given set of data. It allows saving more data. Cryptography is a popular ways of sending vital information in a secret way. There are many cryptographic techniques available and among them AES is one of the most powerful techniques. The scenario of present day of information security system includes confidentiality, authenticity, integrity, no repudiation. The security of communication is a crucial issue on World Wide Web. It is about confidentiality, integrity, authentication during access or editing of confidential internal documents.

Keywords: Cryptography, Data Encryption, Data Decryption, Digital Signature, Security, Integrity.

I. INTRODUCTION

The fast development of the modern Internet technology and information technology cause the individual, enterprise, school and government department joining the Internet, Which cause more illegal users to attack and destroy the network by using the fake websites, fake mail, Trojan horse and backdoor virus at the same time. Target of the attacks and intrusion on the network are computers, so once the intruders succeed, it will cause thousands of network computers in a paralyzed state In addition, some invaders with ulterior motives look upon the military and government department as the target which cause enormous threats for the social and national security [1].

Cryptography means "Hidden Secrets" is concerned with encryption. Cryptography, the investigation of systems for secure correspondence. It is helpful for examining those conventions, that are identified with different viewpoints in data security, for example, verification, classification of information, non-denial and information uprightness.

II. BASIC TERMS IN CRYPTOGRAPHY

a) Plain Text: The original message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text. For example, Alice is a person wishes to send "Hello Friend how are you" message to the person Bob. Here "Hello Friend how are you" is a plain text message.

b) Cipher Text: The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text [2]. In Cryptography the original message is transformed into non readable message before the transmission of actual message. For example, "Ajd672#@91ukl8*^5%" is a Cipher Text produced for "Hello Friend how are you".

c) Encryption: A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

d) Decryption: A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.

e) Key: A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it. For example, if the Alice uses a key of 3 to encrypt the Plain Text "President" then Cipher Text produced will be "Suhvlghqw".

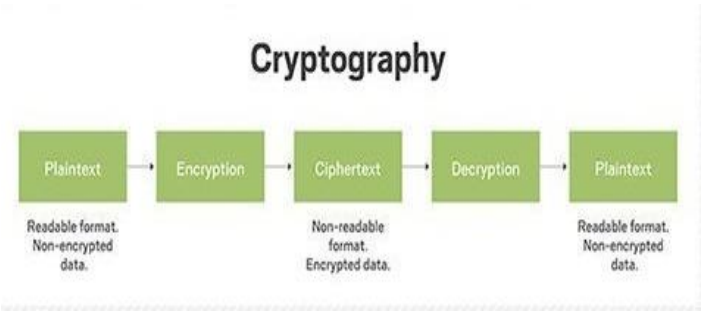

Figure1: Basic method of cryptography

IJCRCST © 2019 | All Rights Reserved

III. PURPOSE OF CRYPTOGRAPHY

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography.

a) Confidentiality: Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

b) Authentication: The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.

c) Integrity: Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

d) Non Repudiation: Ensures that neither the sender, nor the receiver of message should be able to deny the transmission. Access Control Only the authorized parties are able to access the given information.

IV. TYPES OF CRYPTOGRAPHY

There are two main types of cryptography:

- Secret key cryptography or symmetric key cryptography
- Public key cryptography or asymmetric key cryptography

A) Symmetric-key cryptography: Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. This was the only kind of encryption publicly known until June 1976.

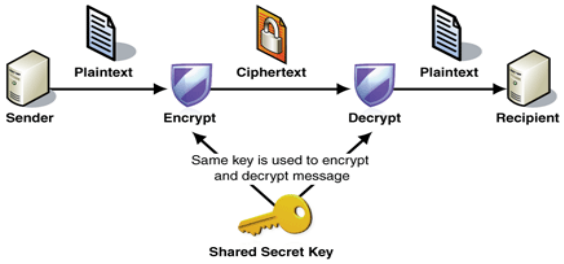

Figure 2: Symmetric-key Cryptography

Symmetric key ciphers are implemented as either block cipher or stream cipher. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher. The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are blocking cipher designs. Stream ciphers, in contrast to the 'block' type, create an arbitrarily long stream of key material, which is combined with the plaintext bit-by-bit or character-by character. In a stream cipher, the output stream is created based on a hidden internal state which changes as the cipher operates. That internal state is initially set up using the secret key material.

A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps each cipher text exchanged as well. The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all straight and secret.

B) Asymmetric key cryptography: Asymmetric key cryptography where different keys are used for encryption and decryption. In asymmetric or public-key cryptography, there are two keys: a private key and a public key are used. The private key is kept by the receiver and public key is announced to the public.

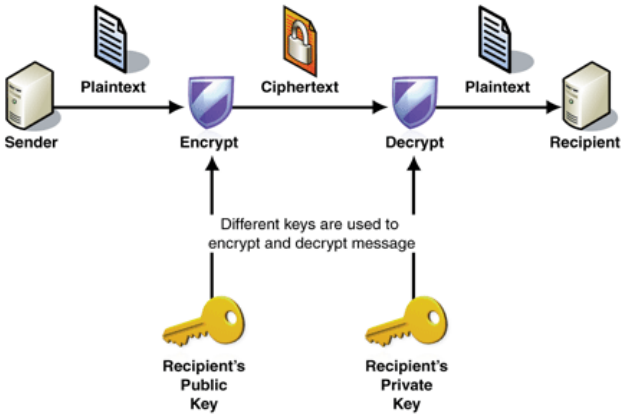

Figure 3: Asymmetric key cryptography

Figure 4: Block Diagram of Public Cryptography with Different Key.

V. ANALYSES OF DIFFERENT TECHNIQUES

In this review paper above described techniques of cryptography are analyzed based on different research paper in respective journals.

1. RSA (Rivest Shamir and Adleman) Algorithm

RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem [3]. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977.

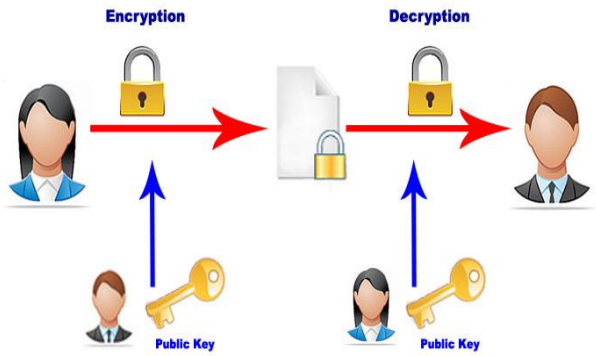

Figure 5.1 : RSA (Rivest Shamir and Adleman) Algorithm

A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their

public key [4]. The prime factors must be kept secret. Anyone can use the public key to encrypt a message.
The RSA algorithm involves three Steps:
1.1 key generations 1.2 Encryption 1.3 Decryption.

1.1. 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:
- Choose two distinct prime numbers p and q.
- For security purposes, the integers p and q should be chosen at random.
- Compute n = pq, where n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
- Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$, where φ is Euler's totient function.
- Choose an integer e such that $1 < e < \varphi(n)$ and gcd(e, $\varphi(n)$) = 1; i.e. e and φ(n) are cop rime. e is released as the public key exponent.
- Determine d as $d-1 \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo φ(n)). This is more clearly stated as solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$, where d is kept as the private key exponent.
- By construction, $d \cdot e \equiv 1 \pmod{\varphi(n)}$. The public key consists of the modulus n and the public (or encryption) exponent e. 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 calculate d.

1.2. Encryption

Alice transmits her public key (n, e) to Bob and keeps the private key secret. Bob then wishes to send message M to Alice. He then computes the cipher text c corresponding to Bob then transmits c to Alice.

1.3. Decryption

Alice can recover m from c by using her private key exponent d via computing given m, she can recover the original message M by reversing the padding scheme.

2. Digital Signature Algorithm (DSA)

It is used by receiver of a message to verify that the message has not been altered during transit as well as certain the sender's identity.

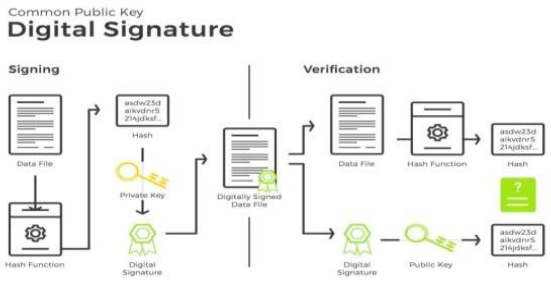

Figure 5.2: Digital Signature Algorithm

A digital signature is an electronic version of a written signature in that the digital signature can be used in proving to the recipient or a third party that the message was, in fact, signed by the sender. Digital signatures may also be generated for stored data and programs so that the integrity of the data and programs may be verified at any later time [8]. One method for sending low size and capacity data by using DSA is proposed by Erfaneh Noorouzil et al. "Hash function" is used in this method and it generates dynamic and smaller size of bits which depends on each byte of data.

The main function which is used for hashing is bitwise or and multiply functions. If hashed file sized is 4% of the original file in the messages with size lower than 1600 bytes. This algorithm can be used in several applications which have low file size for sending and want simple and fast algorithms for generating digital signature [9]. Hash function follows some properties, which are given below.

- Hash function should destroy all homomorphism structures in the underlying public key cryptosystem (be unable to compute hash value of 2 messages combined given their individual hash values) [10].
- Hash function should be computed on the entire message.
- Hash function should be a one-way function so that messages are not disclosed by their signatures.
- Hash function should be computationally infeasible given a message and its hash value to compute another message with the same hash value.
- Hash function should resist birthday attacks (finding any 2 messages with the same hash value, perhaps by iterating through minor permutations of two messages) [10]. This algorithm works on ".doc, .pdf, .txt" and other types of files, and hash function can be used for dynamic size of data. The term dynamic means, results of hash function depends on size of the data.

3. Diffie–Hellman Algorithm

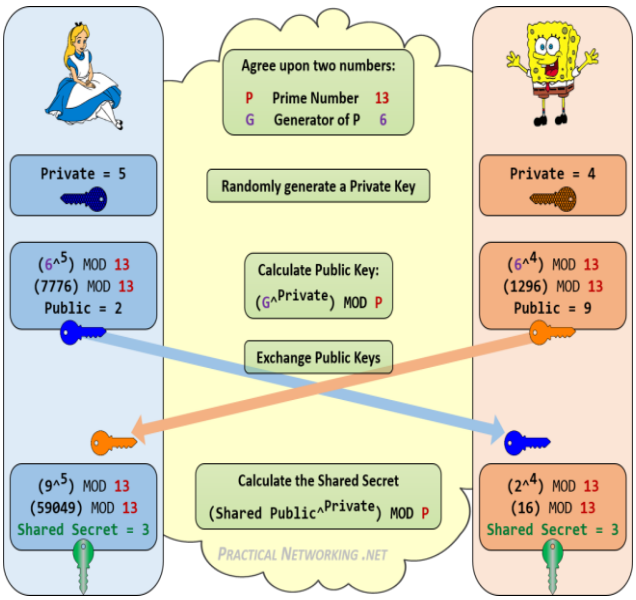

Figure 5.3: Diffie–Hellman Algorithm

This algorithm is used for exchanging cryptography keys between two users. Here user doesn't have any knowledge

about the keys used by each other and they use a shared secret key over an insecure communication channel, then this key is used to encrypt subsequent communications using a symmetric key cipher [5]. New protocol proposed for two goals: authenticated key agreement and authenticated key agreement with key confirmation in the asymmetric (public-key) setting is given by Simon Blake-Wilson et al.

Here they have proposed formal definitions of secure AK (Authenticated Key Agreement) and AKC (Authenticated Key agreement with key confirmation) protocols within a formal model of distributed computing and a unified model of key agreement is proposed with several variants of this model are demonstrated to provide secure AK and AKC protocol in the random oracle model. Here AK and AKC are made secure by providing clear, formal definitions of the goals of AK and AKC protocols, and secondly by furnishing practical, provably secure solutions in the random oracle model [6]. Briefly speaking; the process of providing security can be explained in five steps:

a) Specification of model
b) Definition of goals within this model
c) Statement of assumptions
d) Description of protocol
e) Proof that the protocol meets its goals within the model.

3.1. Properties of Key agreement algorithm

- Known Session Key: This protocol has stored some previous session key.
- (Perfect) Forward Secrecy: This protocol can be compromised in long term secrets of one or more entities then secrecy of previous key is not affected.
- Unknown Key Share: Suppose there are two users i and j then i cannot share the key with j without i's knowledge.
- Key-Compromise Impersonation: If the value of i is disclosed, and can be copied by intruders. But the nature of i should be like that the other properties of i can't be copied and affected.
- Loss of Information: Compromise of other information that would not ordinarily be available to an adversary does not affect the security of the protocol.
- Message Independence: This protocol run between two users are unrelated. This algorithm can be practically implemented with increased security as compared to the currently used protocol [6].

Another way of implementation of Diffie- Hellman algorithm in internet is given [7]. It can be used nearly in every encryption technology used in the Internet today, including SSL, SSH, IPSec, PKI, and everything else that depends on these protocols. In SSL (Secure Sockets Layer), Today in communication process client and server exchanges unencrypted messages. The asymmetric key is used in exchange process and compression option they each accept and prefer. In SSH (Secure Shell), client and server start their process by negotiating parameters (e.g., preferred encryption and compression algorithms, and certain random numbers). In IPSec (Internet Protocol Security), some preliminary information exchange is necessary for starting encrypting the data stream. In PKI (Public Key Infrastructure), two complementary uses can be made of public key cryptography. If one encrypts a message with the public key of another person, only that person can decrypt it because only that person knows his private key [7].

4. Elliptic Curve Cryptography (ECC)

Elliptic curve cryptography is a relatively new family of public-key algorithms that can provide shorter key lengths and, depending upon the environment and application in which it is used, improved performance over system based on integer factorization and discrete logarithms [11]. Here its security, advantages and performance [12] are discussed. ECC has its security problems based on some difficult mathematical. Elliptic curve is based on a mathematical structure in which certain operation can be defined.

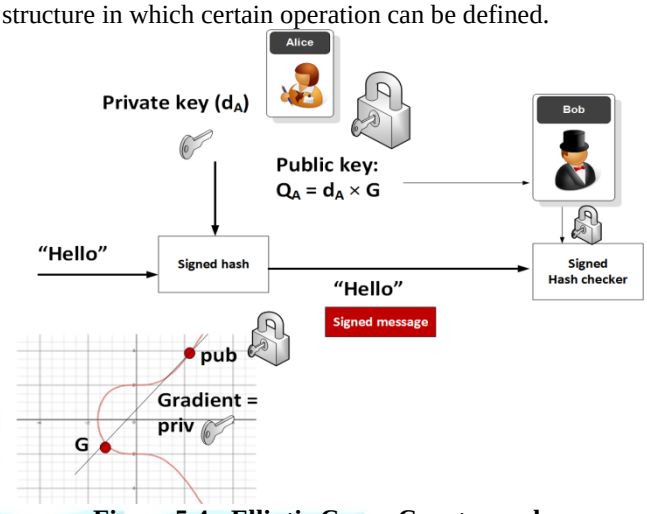

Figure 5.4: Elliptic Curve Cryptography

These operations provide a one way function that can be used to produce efficient cryptographic systems. ECC uses this one way function is called Elliptic Curve Discrete logarithm Problem (ECDLP). The ECDLP is similar to the one way function on which DSA and Diffie-Hellman are based, and hence, elliptic curve analogs of each of these algorithms have been defined [11]. Security and advantages of using elliptic curve based cryptographic systems instead of integer factorization and discrete logarithm based methods is that they provide similar security levels using smaller key lengths. Most people consider the integer factorization and discrete logarithm problems to have approximately equivalent security. Performance of ECC with other algorithms is it is 5 to 15, 20 and 60, and sometimes 400 times faster than others depend on ECC bit [12]. Elliptic Curve Cryptography algorithm is also suitable for smart card application, as it is faster and occupies less memory than RSA [13].

Sr.No.	Cryptography techniques	Analysis
1.	Rivest Shamir and Adleman (RSA) Algorithm	RSA can be used in Mobile nodes; because they are vulnerable to many attacks due to their broadcast nature [1]. RSA is not suitable for WSN because of high time complexity and consumption demand [2].
2.	Diffie-Hellman Algorithm	Here keys are exchanged between two users;

		unknown to each other [5]. It can be used in Internet and nearly in every encryption technology used in the Internet today, including SSL, SSH, IPSec, PKI [7].
3.	Digital Signature Algorithm	Set by the receiver to verify that the message received is unaltered; a digital signature is used for performing this task [8]. Hash function is used to generate dynamic and smaller size of bits which depends on each byte of data [9].
4.	Elliptic Curve Cryptography	Public-key algorithms that can provide shorter key lengths and, depending upon the environment and application in which it is used, improved performance over system based on integer factorization and discrete logarithms [11].

VI. CONCLUSION

After reviewing all the above defined cryptography techniques it can be concluded that ECC is faster than RSA, because it uses small key. But its mathematically operation is complex as compare to RSA. In Diffie-Hellman cryptography algorithm secret keys are exchanged between two users. Whereas a digital signature is used by receiver in DSA to confirm that the signal received is unaltered.

VII. REFERENCES

[1]. A. Perrig, J. Stankovic, and D. Wagner, "Security In Wireless Sensor Networks," ACM, Vol. 47, No.653.2004.
[2]. F. Amin, A. H. Jahangir and H. Rasifard, "Analysis Of Publickey Cryptography For Wireless Sensor Networks Security," In Proceedings of World Academy of Science, Engineering and Technology, ISSN 1 307-6884,2008.
[3]. Simon Blake Wilson et al., "Key agreement protocols and their security analysis," 9-sep-1997.
[4]. David A. Carts, "A Review of the Diffie- Hellman Algorithm and its Use in Secure Internet Protocols," SANS institute, 5-nov-2001.
[5]. Vocal,"http://www.vocal.com/cryptography/dsadigital- signature-algorithm/," Dated: 13-dec-2012 at 13:18.
[6]. Erfaneh Noorouzil et al, "A New Digital Signature Algorithm", International Conference on Machine Learning and Computing, IPCSIT vol.3, 2011.
[7]. B.Nithya, Dr.P.Sripriya, "A Review of Cryptographic Algorithms in Network Security" International
[8]. Journal of Engineering and Technology (IJET) Vol 8 No 1 Feb-Mar 2016.
[9]. Dr. T. Christopher, Mohana Priya. A, " Study of Symmetric Key Network Security Algorithms"IJSRD
[10]. International Journal for Scientific Research & Development Vol. 3, Issue 11, 2016.
[11]. Shaina Arora, Pooja, "Enhancing Cryptographic Security using Novel Approach based on. Enhanced – RSA and Elgamal : Analysis and Comparison " International Journal of Computer Applications (0975 – 8887) Volume 112 – No 13, February 2015.
[12]. 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.213-219, May 2010.
[13]. Shashi Mehrotra Seth, Rajan Mishra, "Comparative Analysis of Encryption Algorithms for Data Communication" IJCST Vol. 2, Issue 2, June 2011.
[14]. Pratap Chandra Mandal, "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish" Journal of Global Research in Computer Science Volume 3, No. 8, August 2012.
[15]. Lalit Singh Dr. R.K. Bharti, "Comparative Performance Analysis of Cryptographic Algorithms" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013.
[16]. https://msdn.microsoft.com/en-us/library/windows/desktop/aa381939(v=vs.85).aspx
[17]. https://www.techopedia.com/definition/1773/decryption
[18]. www.computerhope.com/jargon/d/decrypti.htm
[19]. https://en.wikipedia.org/wiki/Cryptography

Authors Profile

Mr. Gulshan Kumar completed Bachelor of Computer Applications from Panjab University Chandigarh, in year 2012 and Master of Computer Applications from Panjab University in year 2015. He is currently working as Assistant Professor in Department of Computer Applications at Swami Premanand Mahavidayalaya (S.P.N. College) Mukerian under the affiliation of Panjab University Chandigarh since 2016. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, IoT and Blockchain Technology. He has more than three years of teaching experience.