International Journal of Research in advance Engineering,
Volume -1 Isuue-2, Feb-2015, Available at www.knowledgecuddle.com

Analysis of Cryptography Techniques

Ravi K Sheth
Assistant Professor (IT)
Raksha Shakti University
Ahmedabad

Sarika P.Patel
M.E.(C.E.), student
B.V.M.Engineering College
V V Nagar

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. The protection of these confidential data from unauthorized access can be done with many encryption techniques. So for providing data security many cryptography techniques are employed, such as symmetric and asymmetric techniques. In this review paper different asymmetric cryptography techniques, such as RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA (Digital Signature Algorithm), ECC (Elliptic curve cryptography) are analyzed. Also in this paper, a survey on existing work which uses different techniques for image encryption is done and a general introduction about cryptography is also given. This study extends the performance parameters used in encryption processes and analyzing on their security issues.**

Keywords - **Asymmetric key cryptography, Symmetric key cryptography, RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA (Digital Signature Algorithm), ECC (Elliptic curve cryptography).**

I.INTRODUCTION

Cryptography enables the user to transmit confidential information across any insecure network so that it cannot be used by an intruder. Cryptography is the process that involves encryption and decryption of text using various mechanisms or algorithms. A cryptographic algorithm is a mathematical function that can be used in the process of encryption and decryption. Encryption is the process of converting the plain text into an unreadable form called a cipher text. This unreadable form cannot be easily understood by an intruder and sent across the insecure media. Decryption is the process of converting this unreadable form back into its original form, so that it can be easily understood by the intended recipient. The high growth in the networking technology leads a common culture for interchanging of the data very drastically. Hence it is more vulnerable of duplicating of data and re-distributed by hackers. Therefore the information has to be protected while transmitting it, Sensitive information like credit cards, banking transactions and social security numbers need to be protected. For this many encryption techniques are existing which are used to avoid the information theft. Cryptography classified as Symmetric cryptography and Asymmetric cryptography techniques. 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. 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. Further some types of asymmetric cryptography are given by different researchers. Some commonly used asymmetric cryptography techniques are RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA (Digital Signature Algorithm), ECC (Elliptic curve cryptography). Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

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. 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”.

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:

A. Secret key cryptography or symmetric key cryptography

B. Public key cryptography or asymmetric key cryptography

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.

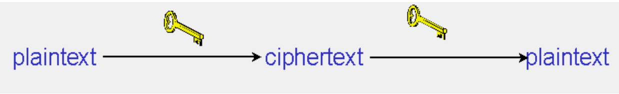

Figure 1: Secret key Cryptography

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 block 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.

Public-key cryptography: Public-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.

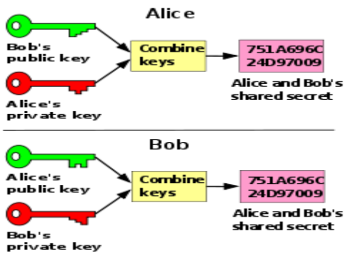

Figure2: Public Cryptography

plaintext
ciphertext
plaintext

Figure3: Block Diagram of Public Cryptography with Different Key.

Some commonly used asymmetric cryptography techniques are RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA (Digital Signature Algorithm). All these technique are discussed below in this paper.

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. 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 coprime. 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. 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. a. 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]. b. Hash function should be computed on the entire message [10]. c. Hash function should be a one-way function so that messages are not disclosed by their signatures [10]. d. Hash function should be computationally infeasible given a message and its hash value to compute another message with the same hash value [10]. e. 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 [10].

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. [6]. 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 [6]:

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

a. Known Session Key: This protocol has stored some previous session key.

b. (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.

c. Unknown Key Share: Suppose there are two users i and j then i cannot share the key with j without i's knowledge.

d. 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. e. Loss of Information: Compromise of other information that would not ordinarily be available to an adversary does not affect the security of the protocol.

f. 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 [7]. 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 [7]. In SSH (Secure Shell), client and server start their process by negotiating parameters (e.g., preferred encryption and compression algorithms, and certain random numbers) [7]. In IPsec (Internet Protocol Security), some preliminary information exchange is necessary for starting encrypting the data stream [7]. 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. 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 [11]. 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].

Table1: Analysis of different Techniques

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.

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] A. Perrig, J. Stankovic, and D. Wagner, "Security In Wireless Sensor Networks," ACM, Vol. 47, No.653.2004.

[4] Chandra M. Kota et al.,"Implementation of the RSA algorithm and its cryptanalysis," In proceedings of the 2002 ASEE Gulf-Southwest Annual Conference, March 20 – 22, 2002

[5]. Wikipedia,
"http://en.wikipedia.org/wiki/Diffie%E2%80%93 Hellman_key_exchange," Dated: 13-dec-2012 at 10:33.

[6]. Simon Blake Wilson et al., "Key agreement protocols and their security analysis," 9-sep-1997.

[7]. David A. Carts, "A Review of the Diffie- Hellman Algorithm and its Use in Secure Internet Protocols," SANS institute, 5-nov-2001.

[8].Vocal,"http://www.vocal.com/cryptography/dsadigital- signature-algorithm/," Dated: 13-dec-2012
at 13:18.

[9]. Erfaneh Noorouzil et al, "A New Digital Signature Algorithm", International Conference on Machine Learning and Computing, IPCSIT vol.3, 2011.

[10]. William-Stallings,
http://williamstallings.com/Extras/Security Notes/lectures/authent.html, Dated: 13-dec-2012 at 14:05.

[11]. Robert Zuccherato, "Elliptic Curve Cryptography Support in Entrust," Entrust ltd. in Canada, Dated : 9-may-2000.

[12]. Kristin Lauter, "The Advantages of Elliptic Curve Cryptography for Wirelesssecurity," IEEE Wireless Communication, Feb 2004.

[13]. Vivek Kapoor et al., "Elliptic CurveCryptography," ACM Ubiquity, Volume 9, Issue20, (20-26)-may-2008.