International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 01 (January- February, 2018)

Analysis of Cryptography and Digital Signature Algorithms on Performance and Computation

Shivnarayan Singh Gour
M. Tech Scholar (CSE)
RKDF (SOE) Indore, India
cs.sgour@gmail.com

Prof. Rahul Sharma
Assistant Professor (CSE)
RKDF (SOE) Indore, India
sharma.rahul5656@gmail.com

Abstract:- *This is the age of digital communication in World Wide Web as soon as the digital communication is increasing it required more security. As concern with the security it required to achieve security goals Confidentiality, Integrity, Authentication, Authorization and Accessibility to provide the proper security. There are many techniques and algorithms available for achieving the security goals. Many algorithms use technique to increase the data secrecy and privacy by making the information unreadable which can be only be decoded or decrypted by those party whose possesses the related key. For these activity same time, algorithms takes a considerable amount of computation time and resources such as processed time, memory, CPU time, and battery power and many more things. There for we require assessing the performance of different cryptographic algorithms to find out best and reliable algorithm to use in digital communication. This survey demonstrate the evaluation of both types of cryptography as symmetric key cryptography (AES, DES, Blowfish) as well as asymmetric (RSA) key cryptography algorithms by taking different types of files and formats like text, audio, video and image files. An evaluation has been conducted for that encryption algorithms using evaluation parameters like as time of encryption, time of decryption and computing of throughput.*

Keywords: Security, RSA algorithm, AES, DES, Encryption, Decryption, Key.

I. INTRODUCTION

As the extreme change and development in technology, The Internet has developed into attractive way for data transmission. A large amount of data is commuted every second over internet that may not be safe. It is essential to protect the data from unofficial users. To defend, data techniques as cryptography and stenography can be used. Cryptography deals with defending data by implementing conversion and encoding methods. Network security consists of a clearly defined and specific set of rules, for influential authorization as a basis for making access control and authentication decisions. Security policy captures the security requirements of an organization or describes the steps that have to be taken to archive the desired level of security. Cryptography algorithms are relegated to symmetric key and public key cryptography as basis on the number of keys used. Symmetric key cryptography is based on the single key is used for encryption and decryption. Single key algorithms also known as single key cryptography, where as in public key cryptography have two keys known public and private and it, uses two key. Sender uses the public key of receiver for encryption and other side receiver uses his/her private key for decryptions. As discussed in this section in order to improve security with using of cryptography [1].

II. LITERATURE REVIEW

In this section we discuss many authors describe about different technologies and algorithms related to security in electronic communication. Warakorn Srichavengsup and Wimol San-Um discuses in his research paper, Cryptography in recent times played a significant function in secure data transmissions, Communication and storages. Most activist data encryption schemes are comparatively complicated and complexity in encrypted keys are not enough, resultant in long computational time and it is somehow a low degree of security alongside all types of attacks. As a result, an extremely secured and robust data encryption scheme is necessary require. In this research they present the data encryption method based on a combination of Cellular Automata (CA) and a robust disorganized system that employs complete value piecewise-linear nonlinearity. They proposed encryption method is not only appropriate to image encryption but also extendable to text and Excel files and etc. [2]

Madhumita Panda describe in his dissertation algorithms use technique to improve the data confidentiality and privacy as making the information unreadable which can be only be decoded or decrypted by party those possesses the related key. But at the same time, these algorithms consume important amount of computing resources such as CPU time, memory, and battery power. So we require estimating the performance of different cryptographic algorithms to find out best algorithm to use in future. This dissertation provide assessment of both symmetric (AES, DES, Blowfish) as well as asymmetric (RSA) cryptographic algorithms by taking dissimilar types of files like Binary, text and image files. An evaluation has been conducted for these encryption algorithms using assessment parameters such as encryption time, decryption time and throughput. [3]

Li Hui-na and Ping Yuan discuss about the elliptic curved digital signature algorithm. One-time limited authorization mechanism based on ECDSA is proposed by them, which give access to password-owner and contribution his right to a provisional user without release any information and data about the original password and confine the time slice or occurrence easily. Based on the alteration of ECDSA, the mechanism is feasible for being put into exercise, can generate limited authorization password safely without being forged or re-used successfully. [4]

III. WORKING MODEL OF CRYPTOGRAPHY

Cryptography model or basic principal of cryptography is shown in figure 1this technique is used for converting a plain text in to the cipher text. Cipher text is nothing but a text which is not in readable form it required the sender and receiver for communication and the sender side is convert the plain text in to the cipher text that is called encryption and the receiver side convert the cipher text to plain text is called the decryption. The complete process is called cryptography through this practices we can achieve the goal of security. Cryptography required a secret key for encryption and decryption. The encryption method hides the original data from the unauthorized user because data is encrypted.

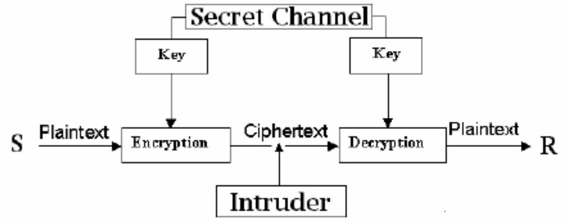

Fig.1

IV. METHODOLOGIES IN SECURITY

Under the tree of security many technology and algorithms has been doing magnificent job these algorithms are improving day by day some of the algorithms are describe below.

A) RSA

The RSA public-key cryptosystem which have two keys concept involves exponentiation modulo a number *n* that is the product of two large prime numbers. This algorithm takes plaintext is encrypted in blocks, with each block having a binary value less than the number *n*. That is, the block size must be less than or equal to log2(n); in practice, the block size is *i* bits, where $2i<n\leq2i+1$. Encryption and Decryption are of the following form, for some plaintext block M and cipher text block *C*:

$$C = M^e \bmod n$$

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

Both the side's sender and receiver must know about the value of *n*. The sender knows the value of *e*, and receiver should know the value of *d* only. Thus, this is a public-key encryption algorithm with a public key which is given as $PU = \{e,n\}$ and a private key which is given as $PR =\{d,n\}$. When referring to the key size for RSA, that is the length of the modulus *n* in bits. A classic key size for RSA is 1024 bits. RSA can be used for encryption and decryption, and also for be used in digital signature.[5]

Key Generation

1. Choose two different large arbitrary prime numbers k & j such that it should be $k \neq j$.
2. Compute $n= k \times j$.
3. Analyse phi, $\varphi= (k - 1) (j - 1)$ where φ is Euler's Totient Function
4. Choose public exponent e such that $1 < e < \varphi$ and $\gcd(e, \varphi) = 1$
5. Calculate private exponent $d = e^{-1} \bmod \varphi$
6. Public key is {n, e}, private key is d.

Encryption: $c = m^e (\text{mod } n)$.
Decryption: $m = c^d (\text{mod } n)$.[3]

B) DSA

DSA (Digital Signature Algorithm) is suitable for applications requiring a signature, digital rather than hand written signature. The DSA is public-key cryptography technique based on exponentiation modulo a large prime number p. For this method, the key size is the length of the prime p in bits, and a typical value is 1024 bits. The digital signature is computed using a set of rules and regulations, a set of parameters such that the identity of the applicant and integrity of the data can be verified. DSA provides the ability to produce and verify signatures. Digital Signature generate by the help of private key and the signature verification take place with the help of public key so the both keys are important, Each and every user use a private key and public key pair. Public keys are implicit to be known for the public in general. Private keys are never shared with anyone; it can verify the signature of a user by employing that user's public key. Signature generation can be performed only by use of the user's private key. The condition for testing individual DSA mechanism of the IUT. These mechanisms are domain parameter generation, domain parameter verification, key pair generation, signature generation, and signature verification [6] [7].

C) ECDSA

Elliptic Curves:- Elliptic curves are an important branch of algebra and geometry. The research on elliptic curves has been taking on for many years and has been obtained plentiful productions. Cryptography has a vast exciting in elliptic curves (E) in finite fields (F), such as: F(p), $F(2^m)$, $F(p^m)$. Finite fields are recognized with the notation F(p^m), where p is a prime and m is a positive integer. It is well known that finite fields exist for any choice of prime *p* and integer *m*. The adding together of points on an elliptic curve is defined with chord contact method, which made Abel groups. Elliptic curve cryptosystems (ECCs) is based on the Abel group. Defining *k*P means P adding itself for *k* times (k ϵ F, P ϵ E (F)), then given a pair of points P, Q ϵ E (F) and Q=*k*P, seeking *k*, which is a base of ECCs [8], because it is a problem being difficult to solve. Based on this difficult problem, it will be more secure to construct the public key cryptosystem with elliptic curves. The existing study shows that the key with 160 bits long of ECCs has the same security with the other two public key cryptosystem which the key needs 1024 bits long[9]. So ECCs has more advantages in security and prosperous trend.

D) SHA

The SHA (Secure Hash Algorithm) is one of the cryptographic hash functions published by the National Institute of Standards and Technology as a U.S. Federal Information Processing Standard. There are currently three generations of Secure Hash Algorithm:

SHA-1 is the original 160-bit hash function. It is like the earlier MD5 algorithm, this was designed by the National Security Agency (NSA) to be the part of Digital Signature Algorithm. Originally it is just called "SHA"; it was inhibited shortly after publication due to an undisclosed "significant flaw" and replaced by the slightly revised version as SHA-1. The original inhibited algorithm is now known by the SHA-0.

SHA-2 is a family of two similar hash functions there for it known as SHA-2, it have two different block sizes, known as SHA-256 and SHA-512. They differ in the word size; SHA-256 uses 32-bit words and where as SHA-512 uses 64-bit words. There are also truncated versions of each standardized, known as SHA-224 and SHA-384. These were also designed by the NSA.

SHA-3 comes in a light after the SHA-2. It is a future of hash function standard the development is still in progress. This is being selected in a public review process from non-government designers. An ongoing NIST hash function competition is planned to end with the assortment of a winning function, which will be given the name SHA-3, in 2012. SHA is a close relation of MD5, sharing much common design, although they are having differences.SHA has very recently been subject to amendment following NIST identification of some concerns, the exact nature of which is not public, current version is regarded as secure. It produces 160-bit hash values. SHA overview

- pad message so its length is a multiple of 512 bits
- initialize the 5-word (160-bit) buffer (A,B,C,D,E) to (67452301,efcdab89,98badcfe,10325476, c3d2e1f)
- This method use message in 16-word (512-bit) chunks, using 4 rounds of 20 bit operations each on the chunk & buffer output hash value is the final buffer value.

E) PHAL

Family of parameterized hash algorithms - PHAL is an application of a new dedicated hash algorithm designed as an answer to weaknesses of MD/SHA hash function family. Recently proposed attacks on well known and widely used hash functions motivate a design of new hash functions. Where a few elements of hash function are parameterized. This approach makes the hash algorithm more secure and more flexible. PHAL consists of two mechanisms: new iteration schema and dedicated compression function [10]. For PHAL hash algorithm a similar approach was chosen. Additionally, the number of rounds was added as a parameter. The design goals of this hash algorithm are determined as follows:

- Hash algorithm must provide message digests of 224, 256, 384 and 512 bits and shall support a maximum message length of at least 264–1 bits.
- Its iteration structure should be resistant against known attack against the MD-type structure.
- Its compression function should be resistant against known attack.
- Its structure should be parameterized, to reach flexibility between performance and security [11].

Parameterized Hash Algorithm is described.

- *w* : length of a word (32 or 64 bits),
- *m* : length of the message block (512 or 1024 bits),
- *n* : length of the chaining variable (256 or 512 bits),
- *d* : length of the digest (224, 256, 384 or 512 bits),
- *s* : length of the *salt* (128 or 256 bits),

X +Y : addition mod 2^w of vectors X and Y,
X -Y : subtraction mod 2^w of vectors X and Y,
X ⊕ Y: bitwise XOR of vectors X and Y,
X<< *s:* *s*-bit left rotation for a *w*-bit vector X,
X >>*s:* *s*-bit left rotation for a *w*-bit vector X,
X « (») *s:* *s*-bit left (right) shift for a *w*-bit vector X.

V. CONCLUSION

Cryptography is a technique which provides the security and digital signature for the digital communication. As per the analysis of all algorithms it is find that these algorithms helps to achieve the goals of security. Combinations of these algorithms can get a great success in security of digital data communication. It is the age of digitalization and security is an important concern so many researchers are doing a great job in this filed.

REFERENCES

[1]. R. Pranesh, V. Harish, M. Vigneshwaran and G. Manikandan "A New Approach for Secure Data Transmission" International Conference on Circuit, Power and Computing Technologies [ICCPCT] 978-1-5090-1277-0/16/$31.00 ©2016 IEEE

[2]. Warakorn Srichavengsup and Wimol San-Um "Data Encryption Scheme Based on Rules of Cellular Automata and Chaotic Map Function for Information Security" International Journal of Network Security, Vol.18, No.6, PP.1130-1142, Nov. 2016.

[3]. Madhumita Panda" Performance Analysis of Encryption Algorithms for Security" International conference on Signal Processing, Communication, Power and Embedded System (SCOPES) - 978-1-5090-4620-1/16/$31.00 ©2016 IEEE.

[4]. Li Hui-na, and Ping Yuan"A Simple One-time Limited Authorization Mechanism based on ECDSA" ICACT 2010 ISBN 978-89-5519-146-2 IEEE Xplore Feb. 7-10.

[5]. Na Zhu, GuoXi Xiao "The Application of a Scheme of Digital Signature in Electronic Government" International Conference on Computer Science and Software Engineering.2008.

[6]. Lawrence E. Bassham III "The Digital Signature Algorithm Validation System (DSAVS)" National Institute of Standards and Technology Information Technology Laboratory Computer Security Division (March 10, 2004).

[7]. Ranjeet Osari, Prof. Bhola Nath Roy "Improving Security and Reducing Computation Time using the ECDSA and PHAL" International Journal of Computational Intelligence and Information Security, Vol. 1 No. 5, July 2010 .

[8]. Qiuliang Xu. "Elliptic curves cryptography." Computer research and development, vol. 36, Feb. 1999, pp. 1281-1288.

[9]. R. Cramer and V. Shoup. "A practical public key cryptosystem provably secure against adaptive chosen cipher text attack." Advances in Cryptology-Crypto'98, 1998, pp.13-25.

[10]. P. Rodwald, J. Stoklosa, "PHAL-256 Parameterized Hash Algorithm," IAS, pp.50-55, 2008 The Fourth International Conference on Information Assurance and Security, 2008.

[11]. NIST, Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) Family. http://www.nist.gov/ hashcompetition2007.