International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 02 (March- April, 2018)

Investigation of Asymmetric Key cryptography with Hybrid Algorithm

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

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

Abstract: *In the inclusive networked world, there is a phenomenal development in data transfer and sharing. Security plays a very important role in transmitting the confidential data over the communication medium which tends to be open and insecure. The risk posed by an intruder in accessing the "not to be disclosed data" has been a genuine apprehension for the communication specialists. In this paper we propose a new approach for security enhancement Investigation of Asymmetric Key cryptography With Hybrid Algorithm. Before the encryption process the data to be transferred is rearranged which results in a customized data. The customized data is given as input for the encryption algorithm. For experimental purpose we use RSA algorithm for encryption and decryption and for overcome the computation problem use a hybrid algorithms ECDSA and PHAL.*

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

I. INTRODUCTION

The Advances communications have led to great demand for secured data transmissions and storage for a variety of applications such as medical, industrial and military systems. The secured data transmissions greatly require reliable, fast and robust security systems, and can be achieved through cryptography, which is a technique of information privacy protection under hostile conditions. Cryptography can perform on text, audio, video and images. The main focus is on encryption and decryption time constraints. Because the computation time is plays an important role in security. Conventional cryptography such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), and RSA algorithm may not be applicable in real-time image encryption due to high computational time and high computing power, especially for the images with large data capacity and high correlation among the plain text and cipher text. This all algorithms are convert plain text in to cipher text but it does not focus on computation time which is highly required [1].

II. LITERATURE REVIEW

This Part of the paper is describing the study of different algorithms and methods according to researches. Francesco Buccafurri and Gianluca Lax discuses in his research paper, Digital signature are the key issue of a number of innovative processes involving different components of the economic-social-administrative system. In particular, egovernment activities should receive from digital signature a strong hint to enlarge significantly their action and their effectiveness [2].

Chen Hai-peng, Shen Xuan-jing and Wei Wei describe in his dissertation Among the comparatively mature and frequently used digital signature algorithms, RSA scheme holds the characteristic of homeostasis, and is consequently weak to active attack and impersonation attack Meanwhile, ELGamal digital signature algorithm has severe technological defect although no detailed cryptanalysis test is employed. It is very fragile to substitution attack and forgery attack. In addition, DSS, one variation of ELGamal scheme, suffers the same attacks as ELGamal. Worse still, the public modulus and too short secret key leaves a further security risk to DSS [3].

Chin-Ming Hsu', Shih-Hsiung Twu', and Hui-Mei Chao discuss about the popularity of the Internet and the legislation of digital signatures in Taiwan, transmitting official electronic documentation among different departments to increase the productivity of an institution is encouraged. This encouragement therefore brings group signature authentication problems. Some general properties of group signatures are briefly introduced as follows Anonymity, Un-link ability, Unforgeability, Traceability and Coalition-resistance [4].

HONG Jingxin find in his research the widely used public key digital signature scheme is designed on the *NP* problem in mathematics. The ECC Digital Signature constructs discrete logarithm problem by using the Abel additive group composed of the points on elliptic curve with the development of computer sciences and the communication business, digital signature becomes one of the most important means to guarantee the security of communication [5].

Madhumita Panda describe in his paper, about algorithms use techniques to enhance the data confidentiality and privacy by making the information indecipherable which can be only be decoded or decrypted by party those possesses the associated key. But at the same time, these algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. So we need to evaluate the performance of different cryptographic algorithms to

find out best algorithm to use in future. This paper provides evaluation of both symmetric (AES, DES, Blowfish) as well as asymmetric (RSA) cryptographic algorithms by taking different types of files like binary, text and image files. A comparison has been conducted for these encryption algorithms using evaluation parameters such as encryption time, decryption time and throughput. Simulation results are given to demonstrate the effectiveness of each [6].

III. METHODOLOGY USED IN SECURITY

The internet has been spread in all areas for the information transmitting and accessing for widely uses, the organizations increase their confidence on, possibly circulated, information systems for daily business, they become more vulnerable to security breaches even as they gain productivity and efficiency advantages. It becomes big issues that how to protect the confidential data or information while transmitting and receiving. The security is based on the reliability, functionality and accuracy of the system.

A) Digital Signatures

A digital signature is a digest calculated from a signed document (typically a one-way hash function) which is then signed (encrypted with private key). The client verifies the digest signature by decrypting it with the server's public key and compares it to the digest value calculated from the message received. The signature can also be used by the server to verify data the client is sending.

B) Group Digital Signatures

A group digital signature technique using a digital signature algorithm and a challenge-response identification protocol is proposed to provide effective authentication. The proposed digital signature algorithm is based on solving quadratic congruence, factorization and discrete logarithm problems. Based on the public key infrastructure, group members generate their public-private keys first. The designed authority generates the group member's identity code (ID), the group identity mark, and the group secret key. Every group member keeps his/her private key and the ID for signing. These parameters can ensure only members who can make signatures and provide data authenticity and non-repudiation for any signer. The challenge-response identification protocol with overlapping-shifting-EXOR logical operations is proposed to ensure the signer to obtain group secret key securely and prevent any signer from making false claims. According to the security analysis, the processing time of the proposed approach is faster than the existing RSA and ElGamal group digital signature systems. Moreover, the proposed method would be suited to microprocessor-based devices such as smart cards, computer systems, networks and control systems because of its simplicity, confidentiality, and fast processing speed [4].

C) 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 $2i<n\leq 2i+1$. 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 [7].

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: $c = m^e \pmod n$.
Decryption: $m = c^d \pmod n$.[6]

D) 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 [8].

E) 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 ∈ F, P ∈ E (F)), then given a pair of points P, Q ∈ E (F) and Q=*k*P, seeking *k*, which is a base of ECCs [9], 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[10]. So ECCs has more advantages in security and prosperous trend.

F) 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.

G) 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 [11]. 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 [12].

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.

IV PROPOSED SYSTEM

This is found that if we put the three technologies RSA, DSA and SHA together for Digital Signature, Encryption, Decryption and Computation. Figure 1 show the traditional methods through that sender can encrypt the plain text and convert it in to the cipher text using RSA, DSA and SHA. It provide the security and try to achieve security goal but it have the computation time is higher.

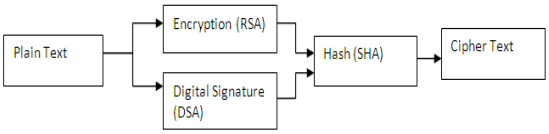

Figure 1 RSA, DSA, and SHA Model

Figure 2 is proposed to solve the problem of computation in which Plain text converted in cipher text using ECDSA and PHAL.

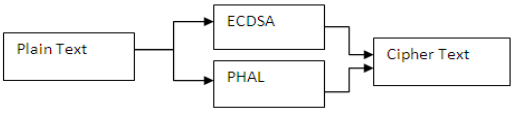

Figure 2 New Hybrid Model ECDSA and PHAL

V Result Analysis

The proposed work is based on a Hybrid Model of ECDSA and PHAL the digital signature using ECDSA for improving security and PHAL for reducing computation time.The analysis of the time computation is based on the algorithms which generated the time as given in the table 1 to table 6.

Analysis of File 1

Encryption

Algorithms	Key Size	Total Bytes	Time*
RSA DSA SHA	30	26202	0.03625738
ECDSA PHAL	30	26202	0.02014288
***micro second**			

Table 1 Encryption Computation Time

Decryption

Algorithms	Key Size	Total Bytes	Time*
RSA DSA SHA	30	26208	0.03613235
ECDSA PHAL	30	26208	0.02007352
***micro second**			

Table 2 Decryption Computation Time

Analysis of File 2

Encryption

Algorithms	Key Size	Total Bytes	Time*
RSA DSA SHA	20	55808	0.0327
ECDSA PHAL	20	55808	0.01816
***Micro seconds**			

Table 3 Encryption Computation Time

Decryption

Algorithms	Key Size	Total Bytes	Time*
RSA DSA SHA	20	55824	0.03520621
ECDSA PHAL	20	55824	0.01805900
***Micro seconds**			

Table 4 Decryption Computation Time

Analysis of File 3

Encryption

Algorithms	Key Size	Total Bytes	Time *
RSA DSA SHA	10	388704	0.07921956
ECDSA PHAL	10	388704	0.04401086
***Micro seconds**			

Table 5 Encryption Computation Time

Decryption

Algorithms	Key Size	Total Bytes	Time*
RSA DSA SHA	10	388720	0.07887987
ECDSA PHAL	10	388720	0.04382215
***Micro seconds**			

Table 6 Decryption Computation Time

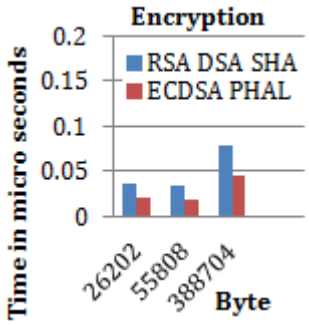

Figure 3 Computation time comparisons at Encryption

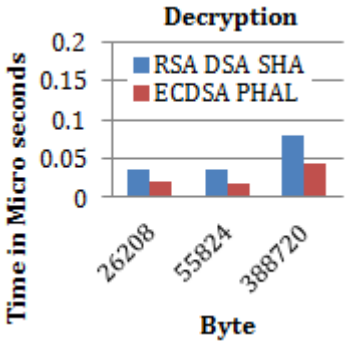

Figure 4 Computation time comparisons at Decryption

V Conclusion

This chapter shows that the proposed Hybrid architecture of Asymmetric Key cryptography for provides the high security and computation time for encryption and decryption. This approach is a based on ECDSA and PHAL Algorithms for authentication and verification. This hybrid architecture gives the comparatively high security compare to RSA, DSA and SHA. Investigation of Asymmetric Key cryptography With Hybrid Algorithm approach work on computation which calculates the total data before the encryption and calculate after the decryption. it also fixed data size Through that this mechanism find out the different computation time between the Hybrid model RSA, DSA, SHA and Hybrid model ECDSA, PHAL. It is work on all the documents like doc, pdf, word and etc. it also work on Audio and Video files.

REFERENCES

[1]. 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.

[2]. Francesco Buccafurri and Gianluca Lax "Hardening Digital Signatures against Entrusted Signature Software" 1-4244-1476-8/07/$25.00 ©2007 IEEE.

[3]. Chen Hai-peng, Shen Xuan-jing and Wei Wei "Digital Signature Algorithm Based on Hash Round Function and Self-certified Public Key System" First International Workshop on Education Technology and Computer Science 978-0-7695-3557-9/09 $25.00 © 2009 IEEE

[4]. Chin-Ming Hsu', Shih-Hsiung Twu', and Hui-Mei Chao "A Group Digital Signature Technique for Authentication" 0-7803-7882-2 /03/$17.0002003 IEEE.

[5]. HONG Jingxin "A New Forward-Secure Digital Signature Scheme" Ayadi Wael and Seddik Hassene "1-4244-1035-5/07/$25.00 .2007 IEEE.

[6]. 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.

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

[8]. 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).

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

[10]. 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.

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

[12]. NIST, Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) Family. http://www.nist.gov /hashcompetition 2007.