IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661, ISBN: 2278-8727Volume 7, Issue 1 (Nov. - Dec. 2012), PP 47-52
www.iosrjournals.org

A New Efficient Digital Signature Scheme Algorithm based on Block cipher

[1]Prakash Kuppuswamy, [2] Peer Mohammad Appa,[3]Dr. Saeed Q Y Al-Khalidi
[1](Computer Engineering & Networks Department, Jazan Uuniversity, KSA)
[2](Computer Science Department, Jazan University, KSA)
[3](College of Computer Science & Information System, Jazan University, KSA)

Abstract: *The digital signature technique is essential for secure transactions over open networks. It is used in a variety of applications to ensure the integrity of data exchanged or stored and to prove to the recipient the originator's identity. Digital signature schemes are mostly used in cryptographic protocols to provide services like entity authentication, authenticated key transport and authenticated key agreement. This architecture is related with secure Hash Function and cryptographic algorithm. There are many other algorithms which are based on the hybrid combination of prime factorization and discrete logarithms, but different weaknesses and attacks have been developed against those algorithms. This Research paper presents a new variant of digital signature algorithm which is based on linear block cipher or Hill cipher initiate with Asymmetric algorithm using mod 37.*

Keywords:- *Digital Signature, Block cipher, Factorization, MD5, ECC.*

I. Introduction

Cryptography is the branch of cryptology dealing with the design of algorithms for encryption and decryption, intended to ensure the secrecy and/or authenticity of message. The DSA was proposed in August 1991 by the U.S.[2]

Emerging applications like electronic commerce and secure communications over open networks have made clear the fundamental role of public key cryptosystem as unique security solutions [7]. A Digital Signature is an important type of authentication in a public-key cryptographic system and it is in wide use [8]. A digital signature is a checksum which depends on the time period during which it was produced [9]. It depends on all bits of a transmitted message and also on a secret key but which can be checked without knowledge of the secret key. A digital signature is computed using a set of rules and a set of parameters such that the identity of the signatory and integrity of the data can be verified [6].

Cryptographers have been studying electronic signature technologies for decades since the discovery of one-way functions [11]. Several electronic signature schemes are proved to be secure under some complexity theoretical assumptions. They proposed a simple server-based electronic signature system in which a small number of common private keys were used. Another work was done on designing an off-line signature verification system based on a displacement extraction method in which a questionable signature is compared with a corresponding authentic one. In this paper we proposed a digital signature algorithm in which the new hash function generates dynamic and more efficient and secure than other methods [12].

II. Related Works

In the RSA Signature Scheme proposed combine signing and public-key encryption. For example, Alice wishes to send a signed, encrypted message to Bob. Given a plaintext x, Alice would compute her Signature $y = sig_{Alice}(x)$, and then encrypt both x and y using Bob's public encryption function e_{Bob}, obtaining $z = e_{Bob}(x, y)$. The ciphertext z would be transmitted to Bob. When Bob receives z, he first decrypts it with his decryption function d_{Bob} to get (x, y). Then he uses Alice's public verification function to check that $ver_{Alice}(x, y) = true$.

ElGamal Signature Scheme, described in a 1985 paper. A modification of this scheme has been adopted as a digital signature standard by the National Institute of Standards and Technology (NIST). The ElGamal Scheme is designed specifically for the purpose of signatures, as opposed to RSA, which can be used both as a public-key cryptosystem and a signature scheme. The ElGamal Signature Scheme is non-deterministic, as was the ElGamal Public-key Cryptosystem. This means that there are many valid signatures for any given message. [5]

Aqeel Khalique Kuldip Singh Sandeep Sood in 2010 proposed the implementation of ANSI X9.62 ECDSA over elliptic curve and discusses related security issues. The main reason for the attractiveness of ECDSA is the fact that there is no sub exponential algorithm known to solve the elliptic curve discrete logarithm problem on a properly chosen elliptic curve. Hence, it takes full exponential time to solve while the best

algorithm known for solving the underlying integer factorization for RSA and discrete logarithm problem in DSA both take sub exponential time. The key generated by the implementation is highly secured and it consumes lesser bandwidth because of small key size used by the elliptic curves. Significantly smaller parameters can be used in ECDSA than in other competitive systems such as RSA and DSA but with equivalent levels of security.[2]

Sushila Vishnoi, Vishal Shrivastava in 2012 presents a new variant of digital signature algorithm which is based on two hard problems, prime factorization and discrete logarithm. In this paper, a new variant of digital signature algorithm is proposed which is based on the two hard problems called prime factorization and discrete logarithm. It is shown that one have to solve both the problems simultaneously for cryptanalysis of this algorithm. The performance of the proposed algorithm is found to be competitive to the most of the digital signature algorithms which are based on multiple hard problems.[3]

Mr. Hemant Kumar, Dr. Ajit Singh proposed in June 2012 SRNN algorithm is based on RSA algorithm with some modification and included more security. In this algorithm we have an extremely large number that has two prime factors (similar to RSA). In addition of this we have used two natural numbers in pair of keys (public, private). This natural number increases the security of the cryptosystem. If the security of our method proves to be adequate, it permits secure communication to be established without the use of carriers to carry keys. In this paper, a new algorithm has been designed for generating signature that overcomes the Shortcomings of the RSA system, also the new algorithm can be achieves high security for digital signature.[1]

III. Proposed Technique

PKI is mainly used for secure transactions between companies or governmental agencies. An e-commerce Web site that uses SSL for encryption is a portion of PKI system. Encrypted e-mail is also another transaction that may be a part of a PKI system. Some companies or agencies may want all staff to digitally sign any documents they've created. Because a digital signature is derived from a Digital Certificate and its key, this is also part of a PKI system. There are so many possible scenarios and solutions it's almost impossible to list them all.

A signature scheme is a method of signing a message stored in electronic form. As such, a signed message can be transmitted over a computer network. In this chapter, we will study several signature schemes, but first we discuss some fundamental differences between conventional and digital signatures.

First is the question of signing a document. With a conventional signature, a signature is physically part of the document being signed. However, a digital signature s not attached physically to the message that is signed, so the algorithm that is used must somehow "bind" the signature to the message.

Second is the question of verification. A conventional signature is verified by comparing it to other, authentic signatures. For example, when someone signs a credit card purchase, the salesperson is supposed to compare the signature on the sales slip to the signature on the back of the credit card in order to verify the signature. Of course, this is not a very secure method as it is relatively easy to forge someone else's signature. Digital signatures, on the other hand, can be verified using a publicly known verification algorithm. Thus, "anyone" can verify a digital signature.

A. Key Generation

Selecting the r x r matrix is the key component of the new digital signature algorithm. Our algorithm based on the modulo 37. So therefore we can keep always public key as 37. It should be give the result $1=6x+37y$, $37=6 \times 6$ which gives $1 = 37-(6 \times 6)$, from which we see that $x = -6$ is a solution.

Step 1: Assign the value of n = 37
Step 2: Select invertible matrix i.e 'k'
Step 3: 'k' should be giving the result of $k*k^{-1} \bmod 37 = 1$
Step 4: Select any integer value and multiply with 'k' i.e., called 'd' private key
Step 5: Find inverse of the integer value and multiply with inverse matrix i.e called 'e' another public key

Now announce 'n' and 'e' as public key and 'd' as a private key

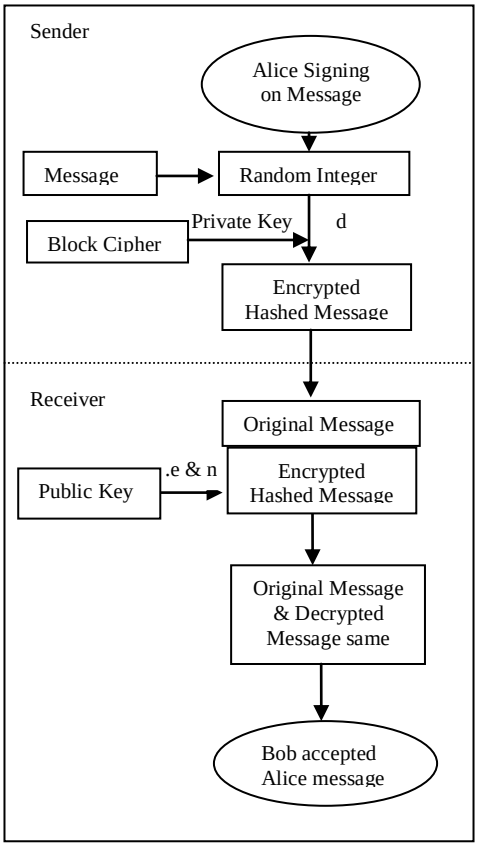

FIGURE.1 New Digital Signature Architecture

IV. Implementation

Select (r x r) invertible matrix and assume n =37. Then select any random integer value, Here we selected 3, Now multiply with selected invertible matrix.

$$3 * \begin{pmatrix} 2 & 1 \\ 4 & 5 \end{pmatrix} \quad \text{mod } 37 = \begin{pmatrix} 6 & 3 \\ 12 & 15 \end{pmatrix}$$

$$\text{Therefore private Key d} = \begin{pmatrix} 6 & 3 \\ 12 & 15 \end{pmatrix}$$

Now inverse of integer 3 = 25 ; Verify (3 *25) mod 37 =1

$$\text{Inverse of the matrix} = \begin{pmatrix} 7 & 6 \\ 24 & 25 \end{pmatrix}$$

$$\text{Calculate 'e' } = 25 * \begin{pmatrix} 7 & 6 \\ 24 & 25 \end{pmatrix} \quad \text{mod } 37 = \begin{pmatrix} 27 & 2 \\ 8 & 33 \end{pmatrix}$$

$$\text{Therefore another public key 'e'} = \begin{pmatrix} 27 & 2 \\ 8 & 33 \end{pmatrix}$$

Signature = (message * private key) mod n

Assume Signing message is 'DEAN OMAR' which is equivalent numerals are 4,5,1,14,15,13,1,18. Already we selected(r x r) matrix is r=2, Therefore, We are blocking entire message into 2 characters each block.

$$= \begin{pmatrix} 6 & 3 \\ 12 & 15 \end{pmatrix} * \begin{pmatrix} 4 \\ 5 \end{pmatrix} \bmod 37 = \begin{pmatrix} 39 \\ 123 \end{pmatrix} \bmod 37 = \begin{pmatrix} 2 \\ 12 \end{pmatrix}$$

Similarly other value have been calculated 2,12,11,0,18,5,23,23
Now message and signature sending to the Mr.Bob

Announce e $= \begin{pmatrix} 27 & 2 \\ 8 & 33 \end{pmatrix}$ and n=37 as a public key

Mr.Bob verifies Mr.A's signature using public key and message(message * e).

$$\begin{pmatrix} 2 \\ 12 \end{pmatrix} * \begin{pmatrix} 27 & 2 \\ 8 & 33 \end{pmatrix} \bmod 37 = \begin{pmatrix} 78 \\ 412 \end{pmatrix} \bmod 37 = \begin{pmatrix} 4 \\ 5 \end{pmatrix}$$

Similarly he derives others using public key 4,5,1,14,15,13,1,18. Now Received message and signature are same. Therefore his message has been verified and accepted.

V. Result Analysis

The proposed method of Digital Signature Scheme based on the linear block cipher or Hill cipher. It is basically symmetric key algorithm. But, Here we implemented the symmetric key algorithm as a Asymmetric key algorithm and used in Digital Signature scheme.

Digital Signatures can provide added assurances of the evidence to provenance, identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory. In Fig.1, It has been mentioned clearly architecture of the proposed Digital signature scheme and in Fig.2 shows the comparison performance of new Digital Signature Scheme.

The algorithm executes on PC computer of CPU Intel Pentium 4, 2.2 MHz Dual Core. The programs implemented using MATLAB. It is tested with messages and with different length of 100 characters.

TABLE I: Key Selection Procedure

Algorithm	Key Selection Procedure
RSA Digital Signature	Between any 2 large prime
Elgammal Digital Signature	Any one large prime and referring index value
Elliptic Curve	$Y^2 = x^3 + ax + b = 0$ on real numbers
Proposed Digital Signature	Using Block cipher symmetric algorithm

TABLE II: Comparison of Performance

Algorithm	No. of Character (Message)	Execution Timing
RSA Digital Signature	100	5.6 Seconds
Elgamal Digital Signature	100	6.2 Seconds
Elliptic Curve	100	5.4 Seconds
MD5	100	5.2 Seconds
Proposed DSS	100	5.2 Seconds

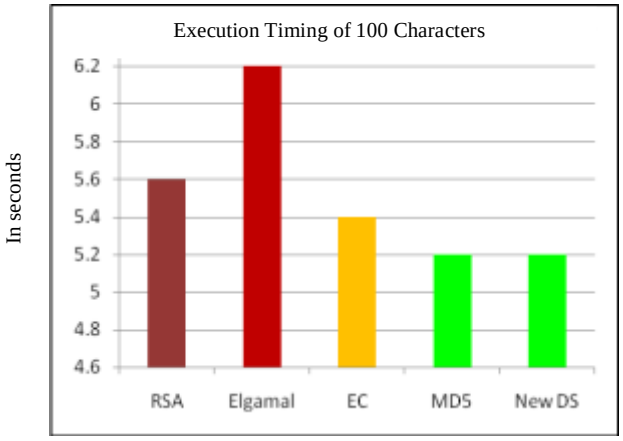

FIGURE.2 Performance evaluation

VI. Conclusion

The important concept of any algorithm satisfying security, it is one of the most important goals for digital signature scheme. The proposed method is increase the performance of new digital signature scheme security rapidly. Also it will ensure the confidentiality, integrity and authentication. It has been tested the algorithm for various sizes of messages and parameters. The experimental results shows that the proposed method is improved the interacting performance, while providing high quality of service and security for desired digital signature scheme.

Several points can be concluded from the experimental results. It has been concluded that the proposed method consumes least encryption time (computing time) and others has taken maximum time in encryption for same amount of the data. The performance of the proposed algorithm is found to be competitive to the most of the digital signature algorithms which are based on multiple hard problems.

Acknowledgement

The authors are extremely express gratitude to the University President, JAZAN University, Kingdom of Saudi Arabia for inspiration and persistent support directly or indirectly for the completion of this research.

References

Journal Papers:

[1] Mr. Hemant Kumar, Dr.Ajit Singh, *An Efficient Implementation of Digital Signature Algorithm with SRNN Public Key Cryptography*, IJRREST, June 2012.

[2] Aqeel Khalique, Kuldip Singh Sandeep Sood, *Implementation of Elliptic Curve Digital Signature Algorithm*, International Journal of Computer Applications, May 2010.

[3] Sushila Vishnoi, Vishal Shrivastava, *International Journal of Computer Trends and Technology*, ISSN: 2231-2803, 2012.

[4] W.Diffie and M. E. Hellman, *New directions in cryptography, IEEE Transactions on information theory*, vol.22,1976.

Books:

[5] Douglas Stinson, *Cryptography Theory and Practice*, by CRC Press, 1995.

[6] A. J. Menezes, P.C.V. Oorschot and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, 1996.

Proceedings Papers:

[7] P. Kitsos, N. Sklavos, and O. Koufopavlou, *An efficient implementation of the digital signature algorithm*, Electronics, Circuits and Systems, 2002.

[8] W.C.Cheng, C.-F.Chou and L.Golubchik, *Performance of Batch-based Digital Signatures* , 10th IEEE International Symposium on Modeling, 2002.

[9] S. Even, O. Goldreich, and S. Micali, *On-line/off-line digital signatures*, presented at Proceedings of CRYPTO'89 conference, 1990.

[10] R.Gennaro and P.Rohatgi, *How to sign digital streams, presented at Proceedings of CRYPTO'97*, Santa Barbara, CA, 1997.

[11] A. Buldas and M. Saarepera, *Electronic Signature System with Small Number of Private Keys*, presented at 2nd Annual PKI Research Workshop, 2003.

[12] Y. Mizukami, M. Yoshimura, H. Miike, and I. Yoshimura, *An Off-line Signature Verification System Using an Extracted Displacement Function*, 2004.

	**Dr. Saeed Q. Y. Al-Khalidi,** Vice-Dean of College of Computer Sciences and Information Systems, Jazan University. He published many National & International papers, Journals. Also, he participated as a Reviewer in many international conferences worldwide. He completed Master Degree and Doctor of Philosophy in University of East Anglia. His research interests include: Information System development, approaches to systems analysis and the early stages of systems development process, IT/IS evaluation practices, E-readiness assessment.
	**Prakash Kuppuswamy,** Lecturer, Computer Engineering & Networks Department in Jazan University, KSA. He is research Scholar proceeding in 'Dravidian University'. He has been published many journals/Technical papers and participated many international conference in Rep. of Maldives, Libya and Ethiopia. His research area Cryptography, Bio-informatics, Network algorithms etc.,
	**Peer Mohamed Appa** Lecturer, Computer Science Department in Jazan University, KSA. He has been published few journals/Technical papers and participated many national and international conference. His research area Cryptography, Bio-informatics, Network algorithms etc.,