Digital Signature Algorithm: A Hybrid Approach

Prajwal Hegde N, Dr. Veena Devi Shastrimath V
Department of Electronics and Communication Engineering,
N.M.A.M Institute of Technology, Nitte, Karkala, Karnataka 574110, India
Visvesvaraya Technological University, Belagavi, Karnataka 590018, India

***Abstract*—Security is one of the most important issues in layout of a Digital System. Communication these days is digital. Consequently, utmost care must be taken to secure the information. This paper specializes in techniques used to defend the facts from thefts and hacks the use of quit-to-cease encryption and decryption. Cryptography is the important thing technique related to Encrypting and Decrypting messages. We use Digital Signature preferred (DSS) and the Digital Signature Algorithm (DSA). The code for this algorithm is written in MATLAB. The DSA Algorithm is commonly used in cryptographic applications to provide services such as entity authentication, key transit, and key agreement in an authenticated environment. This structure is related with steady Hash Function and cryptographic set of rules the government groups in USA as it is taken into consideration to be one of the safest approaches of protection system. This fashion- able could have a top notch effect on all of the Government Agencies and Banks for protective the facts.**

***Keywords*—DSA; digital signature algorithm; hash function; public key; private key; RSA**

I. Introduction

Cryptography is the system of conversion among undeniable text to cipher textual content and to straightforward text. Fig. 1 shows how Cryptographic manner is achieved:

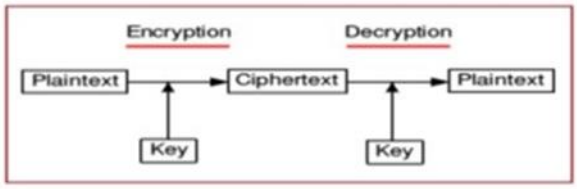

Fig. 1. Cryptographic operations.

- The sender converts the obvious textual content to its cipher shape with a key. This manner is called as Encryption.
- The cipher textual content is received through the receiver.
- The Received cipher text is transformed to a readable shape with a key. This technique is referred to as Decryption.

A. Types of Cryptography

As shown in the Fig. 2, the entirety of the cryptographic algorithms can be classified in to three main categories

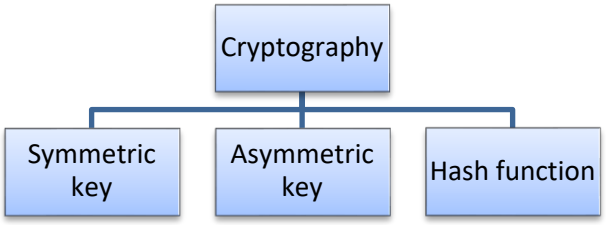

Fig. 2. Types of cryptography.

1) Private key cryptography: Private Key cryptography, also known as symmetric key cryptography, employs the same key for both message sign encryption and decryption. Symmetric key cryptography is tremendously effective since there may be no time put off for Encryption and Decryption of messages [1].

2) Asymmetric key: Asymmetric keys are the foundation of Public Key Infrastructure (PKI), a cryptographic scheme that requires two different keys, one to lock or encrypt the plaintext and one to unlock or decrypt the cipher text. It uses public key for Encrypting messages and Private key for the Decryption of messages. Public key can be shared to everybody but private key's kept secret [2].

3) Hash function: A hash function is a mathematical algorithm that takes an input, or message, and produces a fixed-size output, also known as a hash or digest. The output is deterministic, meaning that the same input always results in the same output, making it challenging to find two inputs that produce the same hash. This property makes hash functions useful in various applications, including data integrity verification and digital signature generation. Examples of widely-used hash functions include SHA-256, SHA-3, and MD5.The following picture illustrated hash function.

II. Related Work

Cryptography is a branch of cryptology that deals with designing algorithms for encryption and decryption to ensure the confidentiality and/or authenticity of messages. In 1991, the DSA was proposed by the U.S. [3]. The growing use of services like e-commerce and open network communications has highlighted the crucial role of public key cryptosystems as security solutions [4]. In public key cryptographic system, Digital Signature provides vital sort of authentication [2]. A digital signature generated as a checksum by making use of the text/data to which it will be later appended to and will look like a whole text [4]. Since the generation of this digital signature is dependent on the transmitted message along with the secrete

key, one cannot easily understand the transmitted data or can reproduce the signature nor can they be able to tamper the transmitted data without getting noticed by the transmitter/receiver. A virtual signature is computed using a set of regulations and a fixed of parameters so as to conceal the identity of the original signatory and also to prove the integrity of the records [4].

Digital signatures have been in use since the early days of digital data transmission, due to the discovery of one-way functions. Many digital signature schemes have been shown to be secure under certain theoretical assumptions. A recent advancement has been the development of an offline signature verification system based on a displacement extraction technique, where a questionable signature is compared to a valid one. The proposed digital signature uses a set of rules and generates dynamic values through a new hash feature.

A signature scheme is a technique for signing an electronic communication that has been saved. A signed communication can therefore be sent across a computer network. Prior to studying various signature methods in this section, let's first talk about some key distinctions between traditional and digital signatures. The first concern is file signing. A traditional signature is one where the document being signed really contains the signer's signature. However, a virtual signature is now not connected bodily to the message this is signed, so the set of rules this is used need to by some means bind the signature to the message. A virtual signature, however, is no longer physically attached to the message it is signed, therefore the set of rules that are utilized must somehow link the signature to the message. The verification issue comes next. By comparing it to other real signatures, a conventional signature is made legitimate.

For instance, when a customer conducts a credit card purchase, the salesperson is required to check the signature on the income slip against the signature on the bottom back of the credit card to confirm it. Of direction, this approach isn't always reliable because it's quite easy to fake another person's signature. In contrast, a publicly acknowledged set of verification procedures may be used to produce digital signatures. Thus, all and sundry can affirm a virtual signature [5].

Chaum is credited with originating the idea of blind signatures [9]. This technology enables a user to have a message signed by another user without divulging any details about the message. Blind signatures have a wide range of practical uses, including electronic cash, untraceable electronic mail, electronic voting systems, time-stamping and anonymous access control.

To overcome several security issues identified in RSA algorithm [1], Gupta et al. suggested an hybrid approach for encryption and decryption algorithms by making use of RSA and Diffie-Hellman algorithm[DH], Named after the founder by Whitfield Diffie and Martin Hellman. A DH algorithm is an extensive algorithm which is majorly used in several internet connectivity protocols. Several example protocols like SSL, IPsec, SSH [1,9,11]. The DH is based on two key principles, a public and a private key. The transmitter and the receiver exchange the secret value among them by making use of these available key values [10]. In the proposed algorithm [1], the authors have combined both algorithm to get a secure and efficient cryptographic environment by exploiting the benefit of security from public key system and the reduction of computing time from secret key system.

The primary goal of Gupta et.al, proposal's combination of these two algorithms is to create a better and more secure cryptosystem by using the speed and security of the secret key system and the public key system, respectively. Users often find it simple to interact securely across open networks using this hybrid technique, especially when sending confidential messages or information. For improved algorithm functioning, efficiency can be altered in terms of time complexity. Additionally, the size of the keys used for encryption and decryption can be further decreased [12].

In contrast to the original RSA technique, which relies on 1024-bit prime numbers, the Iswari et al approach uses 256-bit prime numbers to reduce the computing time needed for key creation. Due to problems with factorization and discrete logarithm calculations, RSA and ElGamal are combined to retain security factors and complexities even when little bit prime numbers are utilised [13].

Patidar and Bhartiya introduced an innovative concept to enhance the conventional RSA method during information transmission between two parties through a network. They utilized a third prime number to form a modulus n that is harder to decipher by outsiders. This improvement combines a refined version of RSA with a unique design approach. Although the technique speeds up communication encryption and decryption, maintaining secure key storage remains crucial as it safeguards against potential attacks [14].

Shikha et al. presents a modified approach to the traditional RSA algorithm that enhances its security by incorporating exponential powers, multiple public keys, and K-NN algorithm. The modified approach also provides verification at both sender and receiver sides, which ensures authenticity of a message. This approach reduces encryption and decryption time for encrypting and decrypting input messages while making it difficult for intruders to hack the information being transmitted [15].

Jaju et al. proposed an updated version of the RSA technique that utilizes three irreducible numbers instead of two prime random numbers for calculating the common modulus, and passing the value of X in both the public and private keys instead of n. This modification is believed to enhance security and improve speed compared to the original RSA technique. The three prime integers, p, q, and r, must be factored to determine the common modulus n, which is a computationally intensive task, making the system more secure. In case of a factorization attack, it becomes difficult to uncover the value of n as X is included in the public key, rather than n. While the new method offers improved security and faster key generation, the encryption and decryption processes take longer than in the original RSA approach [16].

By removing the distribution of n, a big number whose factor, if uncovered, weakens the RSA method, Minni et al. presented a different safe technique. The updated algorithm's

slower key generation time as compared to the RSA technique is one of its drawbacks [17].

Thangavel and colleagues proposed a modified version of the RSA public-key cryptography system, utilizing four prime numbers. The four primes are used to calculate the value of N and determine the values of E and D. The computation of E is more complex as it requires finding the values of e1 and e2 before calculating E1. This added step makes the system more secure and longer to attack. The only value made public is n, so an attacker with knowledge of n cannot determine the other primes and uncover the values of N and D. The system's complexity is further increased by the addition of the E1 parameter. The authors demonstrated the superior security of this approach, making it a safer alternative to the conventional RSA. [18].

Islam et al. proposed a modified RSA (MRSA) scheme to address some weaknesses in RSA algorithm computation. The MRSA approach uses 'n' unique prime numbers for key creation, with three components in both the private and public key. The component N is the product of four large prime integers (w, x, y, and z) selected randomly. The public key consists of three elements, e, f, and N, where e and f are selected randomly from a group of three. In their implementation, the authors noted that the MRSA has different crucial parameters that impact the security and speed of the algorithm. [19].

III. PROPOSED ALGORITHM

A. RSA Algorithm

RSA is named behalf of its inventors [6]. RSA is an era for Encryption and Decryption of messages. RSA is primarily based on Asymmetric Key Cryptography which means that it makes use of two keys, one for Encryption and Other for Decryption. One key is kept Secret and the other is kept Public [7]. The methods of cryptography may be demonstrated as steady until it's cracked. Since RSA uses very massive numbers it is difficult to think out which is the variety taken. For Example, if one hundred digit numbers are taken for p, q. The end result 'n' can be around 200-digit quantity. The recognized Factoring Algorithm will take a piece time for an attacker to crack the records. Any Cryptographic technique which cannot be cracked without difficulty are referred to as steady, as of now RSA algorithm is secured.

In the Standard RSA algorithm, two additional prime numbers are used in the Enhanced RSA (ERSA) [10] algorithm. This concept was inspired by the High Speed and Security RSA algorithm [11], which used two random numbers for key generation.

B. DSA Algorithm

Digital signature widespread (DSS) is used to verify the originality of the Digital Messages or the documents dispatched [8]. Digital signature is a cryptographic cost, which is observed the usage of most effective from the message signals and the private key owned via the non-public key holder. By virtual signature we can offer security for privacy, Authentication, Integrity, and Non-repudiation. There are three main virtual signature techniques below Digital Signature Standard. They are the DSA Algorithm, the RSA Algorithm.

DSA algorithm works on the premise of public key cryptography [4].DSA set of rules is used by the receiver of a message to verify whether the message is changed or is it in its unique form. DSA uses Public key to verify the sender's message, but verifying is complicated compared to RSA.DSA set of rules works on three steps like,

- Key generation
- Signing
- Verification

Fig. 3 shows how the Encryption of message sign is executed; the message sign is sent through Hash characteristic to generate a hash code [3].

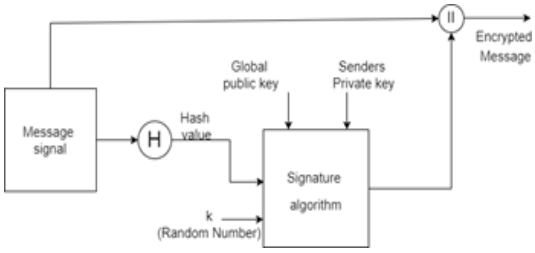

Fig. 3. DSA encryption process.

Then the hash code and random variety 'okay' is given as an input for signature algorithm in conjunction with worldwide public key and sender's private key. Then the message signal and signature could be appended to get an encrypted message.

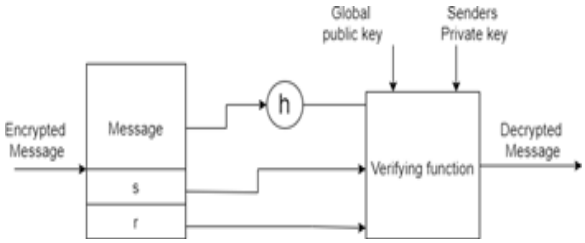

Fig. 4. DSA decryption process.

Fig. 4 shows how the Decryption of message sign is finished, once the Encrypted message is obtained with the resource of the receiver, he desires to decrypt the message to get decrease returned the unique message signal [4]. The Encrypted message signal will encompass the proper message sign, signature parameters like s and r. The message signal is given to the verifying characteristic, at the side of it global public key and sender's personal secret is given to it. And we get the decrypted fee that is not anything however the parameter "v".

C. Hash Functions

It is essentially meaningful for Hash features to compress data such that the output is comparatively shorter than the input, and possess the traits of a great hash function. There are three most important characteristics:

- The information that is being hashed needs to be fully determined via the hash fee.
- The hash characteristic makes use of all the enter records. The complete input statistics must be used by the hash characteristic.
- The hash function uniformly distributes the information across the entire set of possible hash values.

A Hash characteristic is a mathematical feature that converts an input fee into a compressed numerical value – a hash or hash fee. The period of the output always relies upon on the hashing set of rules. The maximum popular hashing algorithms may have a hash period ranging from 160 to 512.

IV. Result and Discussion

The following section discuss about the performance evaluation of proposed algorithm in comparison with standard RSA algorithm.

A. Execution Time Analysis

Table I depicts the overall time taken for the process of encryption and decryption using various algorithms. In the proposed algorithm the Block cipher symmetric algorithm is used for key selecting technique. It can be observed that even though Enhanced RSA has less computation time. In spite of using the block cipher approach for encryption and decryption the proposed algorithm still gives a better time results when compared to either the RSA algorithm or DSA algorithm alone.

TABLE I. Key Selection Procedure and Execution Timing

Algorithm	Key Selection Procedure	Execution Timing
RSA	Any two significant primes	5.9 Seconds
Enhanced RSA	Any two significant primes	2.9 Seconds
DSA	Using Block cipher symmetric algorithm	5.9 Seconds
Proposed DSS with E-RSA	Using Block cipher symmetric algorithm	3.9 Seconds

B. Visual Analysis of Digital Signature

The proposed approach of Digital Signature Scheme based totally on the linear block cipher RSA basically symmetric key set of rules. However, in this case, we employed an asymmetric key set of rules to create the symmetric key technique and applied it in a digital signature scheme. In addition to acknowledging informed agreement and acceptance by a signatory, digital signatures can offer added guarantees of the proof of provenance, identity, and standing of a digital document. The suggested digital signature scheme's actual structure is shown in Fig. 5 to Fig. 9 depicts the assessment performance of recent Digital Signature Scheme. Algorithms are simulated using MATLAB Tool.

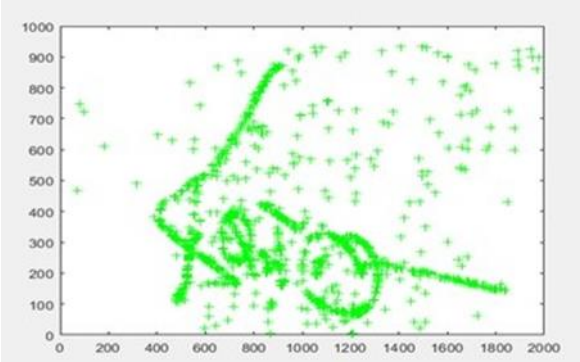

Fig. 5. Signing of sample signature.

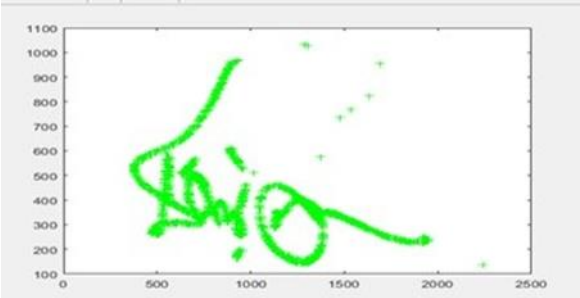

Fig. 6. Identification process of sample signature.

Fig. 7. Signature verification 1.

Fig. 8. Signature verification 2.

Fig. 9. Verified signature.

V. Conclusion and Future Scope

In this research article a technique has been implemented to evaluate the performance of DSA with RSA. In order to further improve the efficiency in terms of execution time, we have modified the existing signature scheme by incorporating Lightweight hash function. The proposed technique is validated by performing the comparative investigations with other existing techniques. The outcomes achieved validated that we have achieved the better performance than other techniques. Even though the research work accomplishes the primary objective of attaining the improved time efficiency, there is a scope of improvement in transaction of data integrity. Hence in future the proposed system can be extended to focus on the integrity of data by improving the Hash function that is suitable for the Digital signature scheme.

References

[1] A. Nist, "proposed federal information processing standard for digital signature standard (dss)," Federal Register, vol. 56, no. 1692, pp. 42980–42982, 1991.

[2] W. C. Cheng, C.-F. Chou, and L. Golubchik, "Performance of batch-based digital signa- tures," in Proceedings. 10th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunications Systems, pp. 291–299, IEEE, 2002.

[3] S. Singh, M. S. Iqbal, and A. Jaiswal, "Survey on techniques developed using digital signa- ture: public key cryptography," International Journal of Computer Applications, vol. 117, no. 16, 2015.

[4] P. Kitsos, N. Sklavos, and O. Koufopavlou, "An efficient implementation of the digital signature algorithm," in 9th International Conference on Electronics, Circuits and Systems, vol. 3, pp. 1151–1154, IEEE, 2002.

[5] R. Kasodhan and N. Gupta, "A new approach of digital signature verification based on biogamal algorithm," in 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), pp. 10–15, IEEE, 2019.

[6] A. Khalique, K. Singh, and S. Sood, "Implementation of elliptic curve digital signature algorithm," International journal of computer applications, vol. 2, no. 2, pp. 21–27, 2010.

[7] R. Soram and E. S. Meitei, "On the performance of rsa in virtual banking," in 2015 Inter- national Symposium on Advanced Computing and Communication (ISACC), pp. 352–359, IEEE, 2015.

[8] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, Handbook of applied cryptography. CRC press, 2018.

[9] G. Wang, Bibliography on Blind Signatures [Online]. Available: http://www.i2r.a-star.edu.sg/icsd/staff/ guilin/bible/blind-sign.htm [ONLINE], Available

[10] Amalarethinam, DI George, and H. M. Leena. "Enhanced RSA algorithm for data security in cloud." International Journal of Control Theory and Applications 9 (2016): 147-152.

[11] Sarthak R Patel, Khushbu Shah, "Security Enhancement and Speed Monitoring of RSA Algorithm", "International Journal of Engineering Development and Research", vol. 2, 2057-2063, 2014.

[12] Gupta, Shilpi, and Jaya Sharma. "A hybrid encryption algorithm based on RSA and Diffie-Hellman." 2012 IEEE International Conference on Computational Intelligence and Computing Research. IEEE, 2012.

[13] Iswari, N.M.S., "Key generation algorithm design combination of RSA and ElGamal algorithm." 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE). IEEE, 2016.

[14] Patidar, Ritu, and Rupali Bhartiya. "Modified RSA cryptosystem based on offline storage and prime number." 2013 IEEE International Conference on Computational Intelligence and Computing Research. IEEE, 2013.

[15] Mathur, Shikha, et al. "Analysis and design of enhanced RSA algorithm to improve the security." 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT). IEEE, 2017.

[16] Jaju, Sangita A., and Santosh S. Chowhan. "A Modified RSA algorithm to enhance security for digital signature." 2015 international conference and workshop on computing and communication (IEMCON). IEEE, 2015.

[17] Minni, R., Sultania, K., Mishra, S., and Vincent, D. R. "An algorithm to enhance security in RSA." 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT). IEEE, 2013.

[18] Thangavel, M., Varalakshmi, P., Murrali, M., & Nithya, K. (2015). An enhanced and secured RSA key generation scheme (ESRKGS). Journal of information security and applications, 20, 3-10.

[19] Islam, M. A., Islam, M. A., Islam, N., & Shabnam, B. (2018). A modified and secured RSA public key cryptosystem based on "n" prime numbers. Journal of Computer and Communications, 6(03), 78.