Analysis of Digital Signature based Algorithm for Authentication and Privacy in Digital Data

Dimple Bansal
M.Tech Scholar
Dept. of Computer Science
Science MACERC, Jaipur

Manish Sharma
Assistant Professor
Department of Computer Engineering, Poornima Institute of Engineering & Technology, Jaipur

Aayushi Mishra
M.Tech Scholar
Dept. of Computer
MACERC, Jaipur

ABSTRACT
Digital signature methodology provides cryptographic services like entity authentication, authenticated key transmission and authenticated key agreement. A Digital Signature is used to provide authentication, non-repudiation & integrity over the digital data in data exchanged and to validate the recipient for the authorized identity over open network. The goal of a Digital signature algorithm is to provide security for message or data. The present paper focuses on a comparative study of some existing algorithms of digital signature on the basis of many hard problems.

Keywords
Digital signature, Authentication, Non-repudiation, Integrity

1. INTRODUCTION
In the current scenario, a variety of data transfer is made possible across the internet using various methods. From these data some of the information is highly secret which requires a great security, thus, an extensive security measures have to be adopted. Many algorithms and techniques can be used to secure our data or information from threats. These kinds of technologies and algorithms are collectively known as Cryptography.

Cryptography system can be widely categorized into two parts first one is symmetric key cryptography (single key system) which is possessed by both the sender and receiver and another one is public key system (asymmetric key cryptography) in which uses of two keys are provided, first is public key which is common for both the sender and receiver and other one is private key which is known to the individual only.

The ability of safeguarding information by modifying it (encoding it) into a non-readable pattern is termed as cipher text. Also, those who acquire a private key, can decode (or decrypt) the information into the plain text[2].Various techniques are included under the cryptography to provide security, digital signature is one of them.

2. DIGITAL SIGNATURE
Basically Digital signatures are based on asymmetric key cryptography.

Digital Signature is primarily a mathematical application of asymmetric cryptographic method over the digitized documents to certify its legitimacy and integrity to its users. Digital signature can be used to provide assertion that the claimed party authorized the information.

In addition to this, it can be used to identify whether or not the information was altered after it was signed (i.e., to detect the reliability of the signed information).A Digital signature algorithm consists key generation, Signature generation, Signature Verification algorithm. A Digital Signature should provide Authentication, Integrity and Non-repudiation.

2.1Authentication
Message authentication is a service used to verify the integrity of a message. Message authentication assures that the data received are exactly same as sent.

Hash function is used to provide message authentication. The hash code value is also called as message Digest. Hash function value is used for message authentication in terms of this: "The sender calculates a hash code value as a function of the bits in the message and transfer both the hash value and the message at the receiver side..

To calculate hash value of the original message, Digital Signature is used to choose the right information and authorized content which is encrypted with the sender's private key only known by the sender. At the receiver side hash value is calculated for the message bits and then resultant hash value is compared with the incoming hash value.. Therefore, a valid signature verifies that the message was created by the sender. The corresponding public key is used to verify the signature. If the signature is valid, the message is authenticated.

2.2 Integrity
Every message is unique in its behaviour, so we require a authenticity variant (integrity of the message) to secure the message for each sender, so to do this a digital signature is create. To generate a digital fingerprint of the message it's required that we need a cryptographic hash value. If it has been changed, then the hash value is not similar to the previous one since it is inappropriate to get another message which has a similar hash value. Cryptographic hash value must be secured So that it is not prone to any vulnerability (i.e., altering the messages and re-establishing the equivalent value of the hash). The private key is used to encrypt the message to generate a digital signature to generate a hash value. The attacker requires the sender's private key to modify the message and signature so to maintain the integrity of the message we require the above security concerns.

2.3 Non-repudiation
At the sender side, the data encoded using the private key of the sender may only be decoded with the interrelated public key. Sender sign a message with the private key of himself/herself and the public key of the sender is used to authenticate the validity of the signature. To authenticate the transmitting data generated from both sides; the sender cannot deny that the signature is sent by him/her.

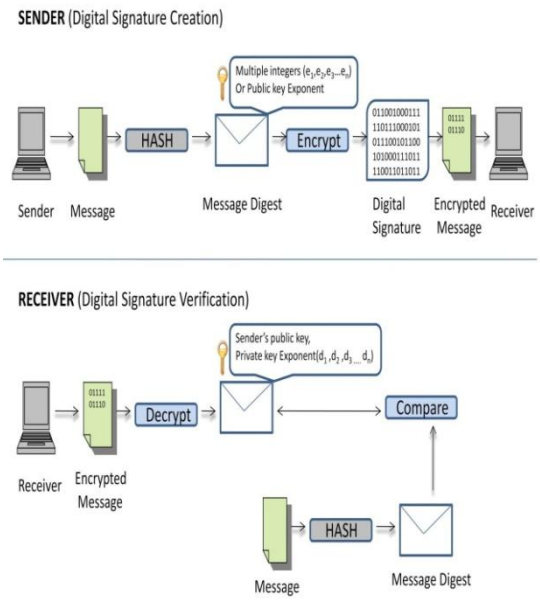

Figure1: Digital Signature Process

As shown in the above figure, the sender sends a message encrypted by his/her own private key and creates a signature and send it to the receiver. By using sender's public key at the receiver side message is decrypted and it verifies the signature and retrieves the original message being send by the sender.

3. APPROACHES

Digital signature algorithm (DSA) is the part of Digital Signature Standard (DSS) approach, which is developed by the U.S. National Security Agency (NSA).DSA is a Federal Information Processing Standard for digital signatures. in August 1991 DSA is developed by the National Institute of Standards and Technology (NIST).There are two different approaches to the Digital Signature:

3.1 RSA Approach

In this approach, the message to be signed is put in to a hash function which generates a secure hash code of fixed length. Using the sender's private key, this hash code is therefore encrypted to form the signature. Both the signature and message are then sending to the receiver. The receiver obtains the message and generates a hash code. Also, it decodes the signature by means of the sender's public key. hash code is found similar with the decoded signature, then this type of signature is admitted as legitimate [7]. Digital signature authorized legitimate user because only the sender knows the private key

3.2 DSS Approach

This approach makes usage of a hash code function. In the signature function hash code is given just as an input, additionally a random number is also produced on this specific signature. In the signature function, sender's private key (Pr) and set of constraints (we can say that this set is used to invent a global public key (PUG)) which are also called as batch of broadcasting principals plays a vital role. From this result is generated which is a signature comprising of two components s and r. Hash code value is generated at the receiver side for the entering messages. After that hash code value with the signature is transferred for the signature verification. In the phase of signature verification, verification function is depends on the sender's public key (Pu) paired with private key on the global public key. From the verification function, resultant value is generated which is same as the signature component r, this shows that the signature is legitimate [7].

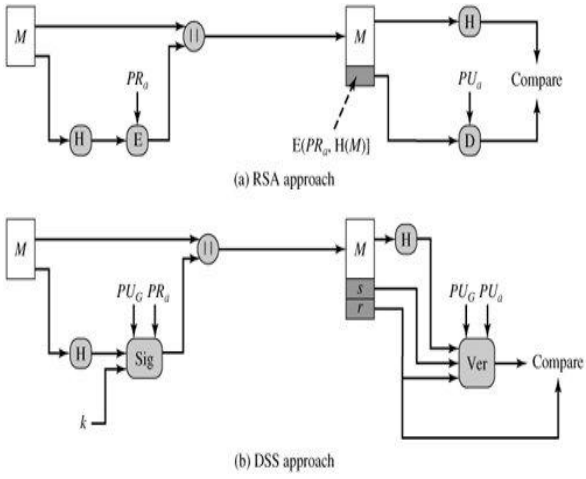

Figure2: Approaches

4. REVIEW ON VARIOUS DIGITAL SIGNATUREALGORITHMS

Some of the Digital Signature algorithms based on above approaches are discusses below:

Daniel Julius Bernstein proposed a **"Edwards-curve Digital Signature Algorithm** (**EdDSA**)" is a digital signature algorithm using a variant of Schnorr signature based on Twisted Edwards curves. It designs a fastest digital signature schemes without compromising security. Like other discrete-logarithm based signature schemes, EdDSA uses a secret value called a nonce unique to each signature. After generating a private key, there is no requirement of a random number generator for EdDSA .There is no risk of a broken random number which will be involved in revealing the private key in the digital signature process.

Kamal kr Agarwal proposed a**" digital signature algorithm based on xth root problem**". In this paper, he introduced a new theoretic problem based on hard number. This theoretic problem based on hard number can be used in the field of cryptography which is a new variant of algorithms of digital signature on the basis of the problems of elucidating the xth root problem. The paper also depicts a summarizing study of the xth root problem & the eth root problem. In this, a single signature is used for verification [5]. The functioning of the projected algorithm that are based on multiple hard problems are found to be competitive to the majority of the algorithms based on digital signature.

Ashish Vijay proposed a **"A New Variant of RSA Digital Signature"**. In this paper, he introduced a new alternative of the different algorithms of digital signature that are based on two hard problems, the xth root problem & the problem of prime factorization. The presented algorithm in this paper is an alteration of the original RSA based digital signature algorithm [3].In this algorithm, two signatures are used for verification. This algorithm is secure against various attacks while it is insecure against the Chosen-message attack like RSADSA [6].

Kapil Madhur proposed a **"Modified ElGamal over RSA Digital Signature Algorithm (MERDSA) "**This paper is based on two hard problems, prime factorization (FAC) and discrete logarithm (DL). In this algorithm two signatures is used for verification. The proposed algorithm carries out the security analysis and performance[4]. In this paper, we have reviewed that when an oracle 'O' splits Prime Factorization & Discrete

Logarithm then it can split the presented algorithm , if the public key of the scheme and a message madv [8] is provided.

Sushila Vishnoi proposed a**" A new Digital Signature Algorithm based on Factorization and Discrete Logarithm problem"** this paper also focuses on two multiple hard problems, the Discrete logarithm & the problem of prime factorization. Time complexity of the proposed algorithm is also calculated. In this algorithm a single signature is used for verification[1].

5. COMPARATIVE STUDY

Characteristics	**RSA Approach**	**DSA Approach**	**ElGamal Algorithm**	**Variant of RSA Digital Signature (Ashish Vijay)**	**Xth root problem (Kamal kr agarwal)**	**DSA based on Factorization and Discrete Logarithm (Sushila Vishnoi)**	**Edwards-curve Digital Signature Algorithm (EdDSA)**
Number of private keys	1	1	1	4	2	**3**	**1**
Number of public Keys/ Group key	1	1	1 group key	2	3	**6**	**1**
Hard problems being solved	Large number factorization	Discrete Logarithm	Discrete Logarithm	Prime factorization, Xth root	Prime factorization	Factorization and Discrete Logarithm	Elliptic curve Algorithm
Possible attacks	Chosen cipher text attack , Timing Attacks, Mathematical Attacks, , Brute Force	Fault Attacks	Plain Text Attack	Key only Attack, Key Attack, Blinding	Key only Attack, Chosen Message Attack, Blinding	Key only Attack, Chosen Message Attack, Blinding, known partial key attack	Brute Force Attack
Performance analysis	Signature generation and verification is very fast	Encryption, Decryption and Verification is very faster than other Algorithm	More Secure	Complexity is O(2×log3n) for generating a signature and O(log3n) for verifying a signature	Complexity is O(log3n) for generating a signature and O(4×log3n) for verifying a signature	Complexity is O(3×log3n) for generating a signature and O(5×log3n) for verifying a signature	Verification can be performed in batches of 64 signatures.
Communication Group	NO	YES	NO	NO	NO	NO	NO

6. CONCLUSION

In this paper, review on different algorithm of the Digital Signature which is based on RSA and DSA approach has been done. New variation of algorithms of digital signature that are based on multiple hard problems like the elliptic curve, discrete logarithm and prime factorization has also been discussed. Based on the comparative analysis, we showed the performances based on many characteristics.

7. REFERENCES

[1] ES Ismail, NMF Tahat, and RR Ahmad. A New Digital Signature Scheme Based on Factoring and Discrete Logarithms. Journal of Mathematics and Statistics, 4(4):222{225, 2008.

[2] D. Boneh and H. Shacham. Fast variants of RSA. CryptoBytes (RSA Laboratories), 5:1{9, 2002.

[3] Ashish Vijay, Priyanka Trikha , Kapil Madhur," A New Variant of RSA Digital Signature"https://www.ijarcsse.com/docs/papers/10_October2012/Volume_2_issue_10_October2012

[4] Kapil Madhur, Jitendra Singh Yadav,Ashish Vijay," Modified ElGamal over RSA Digital Signature Algorithm (MERDSA)"https://www.ijarcsse.com/docs/papers/8_August2012/Volume_2_issue_8

[5] Kamal kumar Agrawal, Ruchi Patira, Kapil Madhur," A Digital Signature Algorithm based on xthRootProblem"https://www.ijarcsse.com/docs/papers/11_November2012/Volume_2_issue_11_November2012

[6] Bernstein, Daniel J.; Duif, Niels; Lange, Tanja; Schwabe, Peter;Bo-YinYang (2012). "High-speedhigh-security signatures" . Journal of CryptographicEngineering. 2(2):7789. doi:10.1007/s13389-012-0027-1.

[7] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. Information Theory, IEEE Transactions on, 31(4):469{472, 2002