Review Article

ACCENTS Transactions on Information Security, Vol 1(1)
ISSN (Online): 2455-7196

A comprehensive study on digital signature for internet security

Payel Saha*
Department of Computer Science, St. Xavier's College (Autonomous), Kolkata, India.

Abstract
For secure transactions over open networks, the Digital Signature technique is essential. It is having varieties of applications in order to ensure the integrity of data exchanged or stored and to prove the identity of the originator to the recipient. Digital Signature schemes are commonly used in cryptographic protocols to provide services like entity authentication, authenticated key transport and authenticated key agreement. This architecture is related to Cryptographic Algorithm and Hashing Algorithm. This Research paper presents a comprehensive study of Digital Signature and its Algorithm for Internet Security purpose.

Keywords
Cryptography, Digital signature, RSA, MD5.

1.Introduction
In our everyday life Internet became an integral part. Security is an important term in this regard. If serious attack occurs, communication, trade, transaction and other important functions will be affected.

Following are some Security requirements which must be taken into count during any type of communication through Internet:-

- **Integrity:** If the message content changes after being sent from the sender, and before reaching to the recipient, then we will take this as a loss of integrity. Hence the message content must not be affected during its travelling time.
- **Availability:** As per the principles of availability, resources should be available to authorized persons at all time.
- **Confidentiality**: It specifies that contents of message are accessible to nobody, except the sender and intended receiver.
- **Authentication**: It ensures the proof of identity. The sender and the intended receiver of the message must be correctly identified.
- **Nonrepudiation**: Neither sender nor receiver can deny the existence of message.

If someone changes one's document and pretending to be original person it does not validate. A malicious person can copy ones signature in their own document illegally, but in digital signature the intruder cannot do this.

A digital signature associates a digital sequence with an electronic document to represent a handwritten signature on a paper printed document. This computerized succession ought to be viewed as like a written by hand signature. A computerized mark depends on the utilization of two distinctive advanced keys. These keys are called key pair. The keypair consists of a private key and a public key [2, 3]. Both are interdependent but also can be used separately. Normally a key pair belongs to a specific key holder. The algorithm is so complicated so that a third party cannot derive it.

Compared to physical signatures, Digital Signatures are much more secure and 'fool-proof'. Physical signatures are easily replicated or 'forged'. The algorithm behind digital signature is difficult so that it is impossible to forge them. As a result of the higher security connected with Digital Signatures and the numerous points of interest connected with putting away reports electronically (rather than paper), governments in numerous nations have passed laws and regulations empowering (and now and again ordering) the utilization of digitally marked electronic archives rather than paper documents. In India the Income Tax returns or corporate returns are now uploaded electronically. A Digital Signature is a sequence of 'bytes' or a code that possess some special characteristics. A code generated is unique for a particular document by a particular signer. A different signer cannot generate an identical code [4] for the same document or by the same signer for another document. This means that a particular digital signature can be generated only by the unique

*Author for correspondence

combination of that particular document and that particular signer. Digital signatures are computed based on the documents (message/ information) that require signing on some private information held only by the sender. In practice, a hash function is applied to the message to obtain the message digest, instead of using the whole message. In this context, a hash function takes an arbitrary sized message as input and produces a fixed-size message digest as output. The commonly used hash functions are MD-5 i.e. Message Digest-5 and SHA or secure Hash Function. In digital signature computation there are two broad techniques [5] used —Symmetric-key Cryptosystem, and Public-key Cryptosystem. In the symmetric-key system, a secret key is used which is solely known to the sender and the intended receiver. However, between any two pairs of users there must be a unique key. Hence, due to the increasing number of user pairs, it becomes extremely difficult to generate, distribute, and keep a track of the secret keys. On the other hand, a public key cryptosystem uses a pair of keys — a private key, known only to its owner, and a public key, known to everyone who wishes to communicate with the owner. For confidentiality of the message to be sent to the owner, it would be encrypted with the owner's public key, which now could only be decrypted by the owner, the person with the corresponding private key. For authentication purpose, a message would be crypted with the private key of the originator or sender, who we will refer to as A. The encrypted message may be decrypted by public key A. On the off chance that this yields the right message, then it is obvious that the message was surely scrambled by the private key of An, and consequently just A could have sent it.

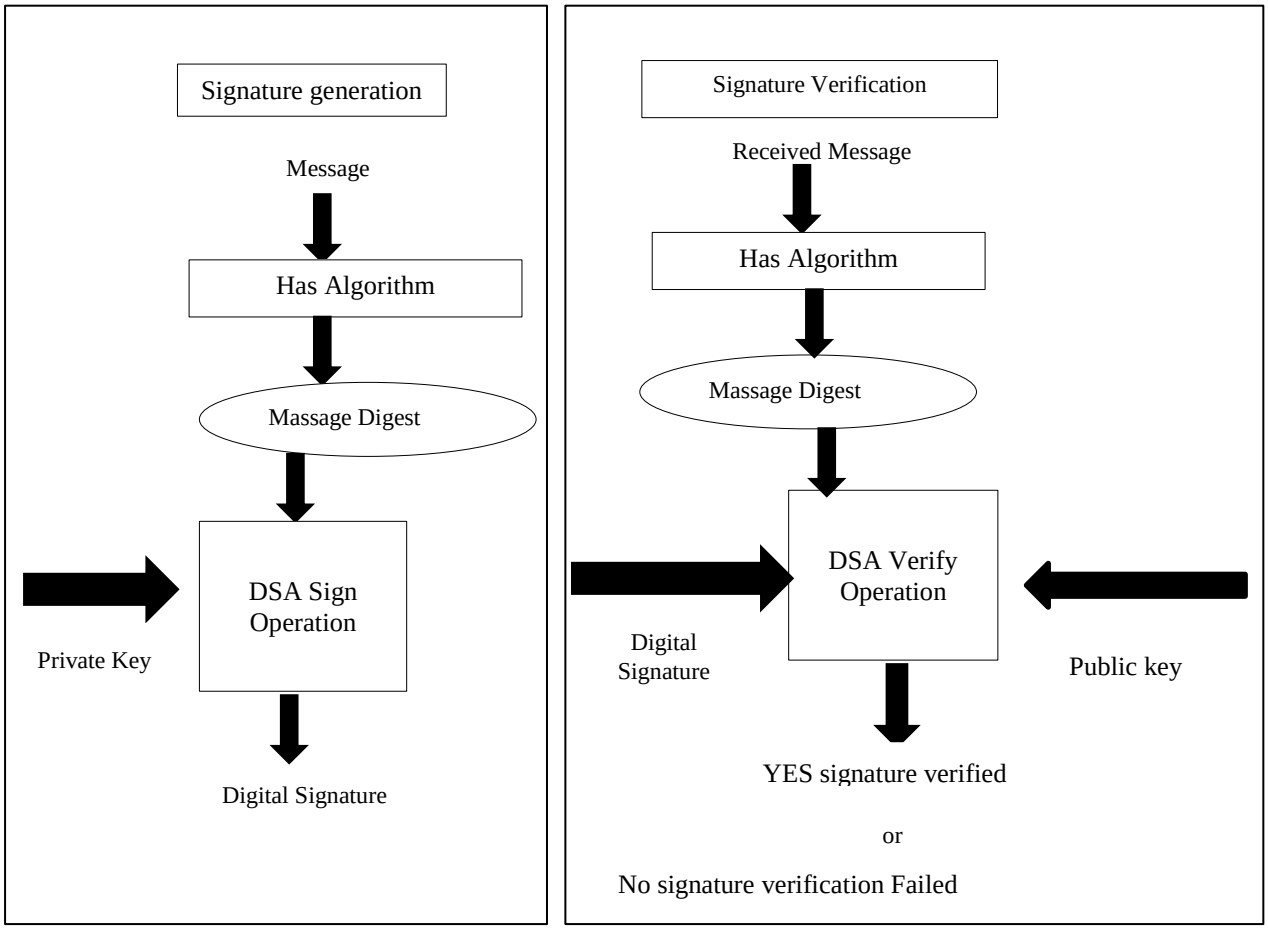

Figure 1 Digital signature generation and verification

2.Properties

Properties of Digital Signature can be described as follows for which it has been chosen in Internet Security:-

- The signature must be an authentic one that means the recipient should understand that the signer signed the document.
- The signature to be used for a particular transaction and it cannot be used in another document.
- It must not be unalterable, i.e. the electronic document should not be changed once it is signed by someone.
- Signature should be non-repudiatable, which means after the signer signs a document then the signer can not claim that he has not signed.

3.Related work

The German digital signature act came into force in the August of 1997 even before the EU's Directive; in fact the directive was adjusted to conform to the German Digital signature Act [14].

In the December of 1997 the European Union invited a proposal for its electronic signature directive with the purpose of making electronic signatures at least as binding as paper-based signatures in abide to facilitate "free movement of goods and service in the internal market". On the off chance that this yields the right message, then it is obvious that the message was surely scrambled by the private key of an, and consequently just A could have sent it.

Herzberg in a private communication [10] suggested signing the viewing program as well as the document, insuring that the data displayed is viewed as it was intended.

Austria fully implemented the directive in 1999; and concretized the malleability problem by specifying that only data formats may be used which have an "available specification" and which exclude"dynamic changes" or "invisibilities."

Ulrich Pordesch [13] a German researcher viewed it a risk to have other agencies verify and sign a document, "imbedding and using the schemes in application systems involves considerable risks, in particular, if the signer or the verifier uses an application environment which is maintained, used, or controlled, by other persons or organizations." He used personal signature for authentication purpose.

His scheme involved having a Personal Digital Assistant to which documents could be transmitted for scrutinization. This scenario would behave like a safe room where the documents are inspected and verified. This strategy though avoids the problem of how secure the Personal Digital Assistant is and whether it has the capability to process dynamic content.

Concurrent with the conference publication of the main results of this thesis, AudunJφsang [11], a senior research scientist with the "Distributed Systems Technology Centre", published a very interesting paper based on the same area but with orthogonal results. Audun Jφsang's approach differed in terms of the depth and direction of attacks proposed. In his example of changing content based on browser type he used the differences in handling of HTML tags in Netscape Communicator and in Internet Explorer. Thus showing that there are many ways to carry out attacks. In this paper he also considered various attacks on XML signatures. Sometimes the two XML documents may look same but may be used for two different applications.

4.Algorithms

Message Digest: A message digest algorithm takes input of any size and transforms it into a fixed string size. Since a million bytes or more of data is reduced to 128 or 160 bits, information is lost and the transformation is not reversible. A major property of a digest is that given a known input string, it is computationally infeasible to discover a different input string with the same digest. Since public key algorithms are so computationally expensive, the digest of a message is signed rather than the entire message. With a suitable digesting algorithm, the security properties of the message are not affected. The signature on the message still authenticates the message, and a valid signature still verifies that a message hasn't been altered [17].

4.1MD5 algorithm

MD5 algorithm was developed by Professor Ronald L. Rivest in 1991. In this algorithm, a message of arbitrary length is taken as an input and produces output as a 128-bit 'fingerprint' or 'message digest' of the input. The MD5 algorithm is intended for digital signature applications, where before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA, a large file must be compressed in a secure manner [6, 7].

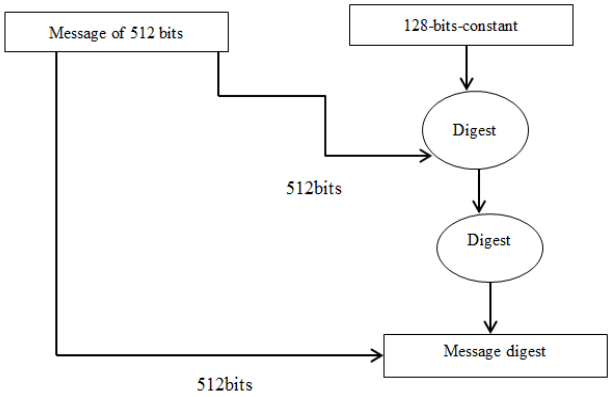

Figure 2 MD5 algorithm

Suppose there is a Sender A and a Receiver B Sender end:-
If A wants to send a message to B.

- Sender A input hash function, it generates random number of keys to a signature.
- Signature is formed with the help of private key encryption.
- Signature + Original message is send to the Receiver B.

Receiver end:-
When B receives the message from A.

- Signature is decrypted with public key.

When the received message from the decryption is matched with the original message and results to be same, we can say that the message has properly received from source to destination without losing it contents and provides all internet security requirements i.e. integrity, confidentiality, nonrepudiation, and authentication etc.

4.2RSA algorithm

RSA, named for Ronald Rivest, Adi Shamir, and Leonard Adleman, the developers of the algorithm, is the best known of all the public key algorithms [17]. The key feature of RSA is that it is a reversible algorithm. (Technically, RSA, or any public key algorithm, is not reversible. Public key algorithms are one-way functions. We say RSA is reversible because the data that was transformed with one key can be recovered with a different key.) With RSA, we can use a private key to recover the data that was previously encrypted using the public key. This concept is illustrated in *Figure 2* with RSA; the public key is used to encrypt data. The private key is used to decrypt the data. Since the public key is available to anyone, but only the owner of the key pair has the private key, anyone can encrypt data meant for the key's owner and only the key's owner can decrypt the data.

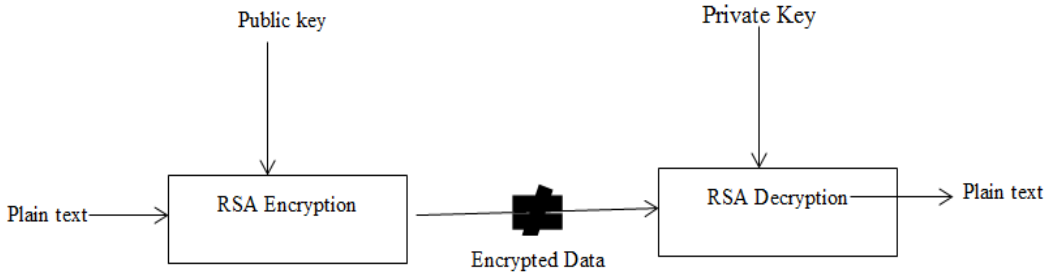

Figure 3 RSA encryption and decryption

The exact same RSA algorithm used for encryption can be used for digital signatures. Using RSA for a signature is shown in *Figure 3*.

1. Firstly, a message digest is being calculated.
2. Then to sign the digest of the message, a private key is used.
3. Before transmiting it to the recepient, the signature is appended to the message.
4. The digest of the received message is then being calculated by the recepient.
5. After that, verifying of the signature will require extracting of the signature from the message and using RSA on the signature with the public key.
6. If in case, the result of the transformation and the newly calculated digest are equal, the signature is valid.

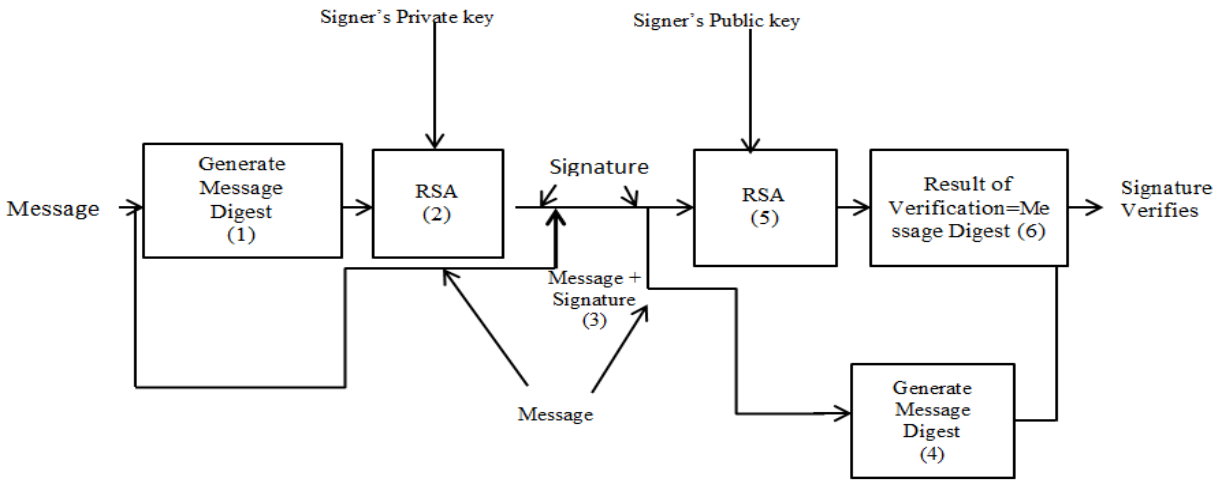

Figure 4 RSA digital signature

Sending the Signature:-
Taking (m, Y) where m is message, Y is signature.
$Y=m^d$.(modn)
Where (n, e, m, Y) are publicly declared, and (p, g, d) are privately declared, (p, and g) are large prime numbers, n = modulas = p.g, e = public exponent, d = private exponent (secret key) = e^{-1}. (modQ(n)) , and Q(n) = (p-1)(g-1).
Verifying the Signature:-
$Y = m^{d.e}$. (mod n)
Where, we must know from prior that, d.e=1; Hence, $m^{d.e} = m$.
If signature is valid, we have to check, whether,
$Y^e = m$.(mod n)

5.Application

Digital signatures are being increasingly used in secure e-mail and credit card transactions over the Internet. The two most common secure e-mail systems using digital signatures are Good Privacy and Secure/Multipurpose Internet Mail Extension. Both of these systems support the RSA based signature. The money transaction I credit card is done through Secure Electronic Transaction It consists of a set of security protocol and formats to enable prior existing credit card payment infrastructure to work on the Internet.

6. Conclusion

The digital signature has become a significant tool in international commerce. Additional businesses will likely use digital signatures in an increasing percentage of their commercial transactions As a digital signature provides the legal elements of a traditional handwritten signature and upgraded security, uprightness, and legitimacy, extra organizations will probably utilize advanced marks in an expanding percentage of their commercial transactions. A secure electronic commerce provides a "paperless" way of transacting business. Electronic communications must be sent in a fraction of a second so that the intruder will not be able to access any data during transmission of electronic data. A digitally signed contract may be e-mailed from a business in India to a recipient in New York in less than one minute, while the same document could take a day (or even longer) to arrive if sent through a commercial delivery service.

Appendix

- **Cryptography:** The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. If an user has private key then he can decipher the text. Cryptography systems can be broadly classified into **Symmetric key systems** and **public-key systems.**
- **Symmetric key Cryptography:** This is a system based on the sender and receiver of a message knowing and using the same secret key to encrypt and decrypt their messages. One weakness of this system is that the sender and receiver must trust some communications channel to transmit the secret key to prevent from disclosure. This form of cryptography ensures data integrity, data authentication and confidentiality.
- **Public – Key Cryptography:** This system is based on pairs of keys called public key and private key. The public key is published and known to everyone while the private key is kept secret with the owner. The need for a sender and a receiver to share a secret key and trust some communications channel is eliminated. This concept was introduced in 1976 by Whitfield Diffie and Martin Hellman.

- **Hash Function:** A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns afixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the "message", and the hash value is sometimes called the message digest or digest or hash.

Acknowledgment
I would like to thank Prof. Dr. Asoke Nath for his continuous valuable guidance and support.

Conflicts of interest
The author has no conflicts of interest to declare.

References
[1] Kumar MH, Singh DA. An efficient implementation of digital signature algorithm with SRNN public key cryptography. International Journal of Research Review in Engineering Science and Technology. 2012; 1(1):54-7.
[2] Kain K. Electronic documents and digital signatures.
[3] Rajapakse HS. Barriers to the public key infrastructure (PKI) deployment and usage for authentic document transaction in Sri Lankan banking sector.2007:18-28.
[4] Sakib AN, Mahmud T, Mountain Munim S, Rahman MM. Secure authentication & key exchange technique for IEEE 802.16 e by using cryptographic properties.
[5] Wong CK, Lam SS. Digital signatures for flows and multicasts. In network protocols. Proceedings. Sixth international conference on 1998 (pp. 198-209). IEEE.
[6] http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Presentations/MD5.pdf. Accessed 29 October 2015.
[7] Rivest R. The MD5 message-digest algorithm.1992.
[8] Felten EW, Balfanz D, Dean D, Wallach DS. Web spoofing: an internet con game. Software World. 1997; 28(2):6-8.
[9] Haber S, Stornetta WS. How to time-stamp a digital document. In conference on the theory and application of cryptography 1990 (pp. 437-55). Springer, Berlin, Heidelberg.
[10] Brickell EF, editor. Advances in cryptology-CRYPTO'92: 12th Annual international cryptology conference, santa barbara, California, USA. Proceedings. Springer; 2003.
[11] Jøsang A, Al Fayyadh B. Robust WYSIWYS: a method for ensuring that what you see is what you sign. In proceedings of the sixth australasian conference on information security (pp. 53-8). Australian Computer Society.
[12] Kain K, Smith SW, Asokan R. Digital signatures and electronic documents: a cautionary tale. In advanced communications and multimedia security 2002 (pp. 293-307). Springer US.
[13] Pordesch U, Berger A. Context-sensitive verification of the validity of digital signatures. Multilateral Security for Global Communication. 1999.
[14] Rossnagel A. Digital signature regulation and European trends. Multilateral Security in Communications.235-49.
[15] Smith RM. Distributing Word Documents with a locating beacon.2000.
[16] Ye E, Yuan Y, Smith S. Web spoofing revisited: SSL and beyond.2002.
[17] Hartman B, Flinn DJ, Beznosov K, Kawamoto S. Mastering web services security. John Wiley & Sons; 2003.

Payel Saha, born on 17th February, 1994, currently pursuing (2014-2016) M.Sc degree in Computer Science from St. Xavier's College, Kolkata, 700016

Email: payel17.10@gmail.com