International Journal of Research
Available at http://internationaljournalofresearch.org/
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 02 Issue 05
May 2015

Review paper on cryptography

Vishakha & RishabhSharma

Dronacharay college of engineering , Gurgaon

Vishakha1360@gmai.com, rishabhsharma.244@gmail.com

1 Introduction

Digital signature is a mathematical technique used to provide **authenticity** and **validation** to digital messages such as email, documents and code distributed via the Internet. To protect data that is transferred electronically digital signatures can be used. A digital signature is a stamp that identifies the sender or the receiver of the electronic document. These are attached to the document to prove the document is original and it has not been tempered. A digital signature scheme typically consists of three algorithms. A **key generation** algorithm that selects a private key randomly from a set of private keys, the algorithm produces the **private key** and a corresponding **public key** and a signing algorithm that produces a signature for a given electronic document. A signature **verifying algorithm** that given a message, public key and a signature, either accepts or rejects the message's claim to authenticity. Digital signatures use private and public key pairs; the sender of the document will have the private segment of the digital signature scheme which is encoded onto the document when it is signed and the recipient of the electronic document would receive the public key of the digital signature scheme. This would allow the recipient to know that the document is authentic and really comes from the sender. The purpose of the signature is to verify that the signer is the originator of the document and sometimes require signatures in person to have a witness to the signature. The public and the private key pair allow electronic documents to be verified in the same way.

2 How digital signature works

The two processes that are performed are –2.1 Digital signing of a message.

The first step is to **calculate the message digest**. A hash-value often called a message digest is calculated via some cryptographic hashing algorithm. The calculated hash-value is a sequence of bits that is extracted in some manner from the message.

The second step is to calculate the **digital signature**. The message digest obtained from the first step is encrypted with the private key of the person who signs the message and a hash-value is obtained. The obtained hash-value is known as the digital signature.

2.2 Verifying digital signatures

The first step is to calculate the **current hash-value**. This is done by applying the same hashing algorithm that was used during the signing process. The obtained hash-value is known as the current hash-value as it calculated from the current state of the message

The second step is to calculate the **original hash-value**.the digital signature s decrypted using the same encryption algorithm that was used for the signing. This is performed by the public key that corresponds to the private key used for signing.

The final step is to **compare the current and the original hash-values**. If the current and the original hash-value match the document original but if it does not match then the document is invalid.

3 Some digital signature algorithms

3.1 Undeniable signatures

Undeniable signatures are signatures that have two properties:

- A signature can be verified only at the cooperation with the signer – by means of a challenge-and-response protocol.
- Signer cannot deny a correct signature. To achieve that steps are a part of the protocol that force the signer to cooperate – by means of a disavowal protocol – this protocol makes possible to prove the invalidity of a signature and to show that it is a forgery. (If the signer refuses to take part in the disavowal protocol, then the signature is considered to be genuine.)

Undeniable signature protocol of **Chaum and van Antwerpen (1989)** is again based on infeasibility of the computation of the discrete logarithm.

Undeniable signatures consist:

- Signing algorithm
- Verification protocol, that is a challenge-and-response protocol.

In this case it is required that a signature cannot be verified without a cooperation of the signer (Bob).

This protects Bob against the possibility that documents signed by him are duplicated and distributed without his approval.

- Disavowal protocol, by which Bob can prove that a signature is aforgery.

This is to prevent Bob from disavowing a signature he made at an earlier time.

3.2 Aggregate signature

A signature scheme that supports aggregation: Given n signatures on n messages from n users, it is possible to aggregate all these signatures into a single signature whose size is constant in the number of users. This single signature will convince the verifier that the n users did indeed sign the n original messages.

3.3 RSA

RSA is one of the **first practical public-key cryptosystems** and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.

3.4 Digital Signature Algorithm (DSA)

DSA is a **Federal Information Processing Standard** for digital signatures. It was proposed by the **National Institute of Standards and Technology (NIST)** in August 1991 for use in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993.

4 References

- J. Katz and Y. Lindell, "Introduction to Modern Cryptography" (Chapman & Hall/CRC Press, 2007)
- Stephen Mason, Electronic Signatures in Law (3rd edition, Cambridge University Press, 2012)
- Lorna Brazell, Electronic Signatures and Identities Law and Regulation (2nd edn, London: Sweet & Maxwell, 2008);
- Dennis Campbell, editor, E-Commerce and the Law of Digital Signatures (Oceana Publications, 2005).
- M. H. M Schellenkens, Electronic Signatures Authentication Technology from a Legal Perspective, (TMC Asser Press, 2004).
- Jeremiah S. Buckley, John P. Kromer, Margo H. K. Tank, and R. David Whitaker, The Law of Electronic Signatures (3rd Edition, West Publishing, 2010).
- Subhra Garg, Internet Fundamentals and Concepts