Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 2, Number 12; July-September, 2015 pp. 8-10

http://www.krishisanskriti.org/acsit.html

Digital Signature: Network Security Solution

Asfia Sabahath

King Khalid University
E-mail: asfia.saba@gmail.com

Abstract—*Digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.*

This project has been developed keeping in view of the security features that need to be implemented in the network to fulfill the following objectives:

To develop an application that deals with the security threats that arises in the network.

To enable the end -users as well as the organizations come with the safe messaging communication without any threats from the intruders or unauthorized people.

To deal with the four inter twinned areas of the network security namely Secrecy, Authentication, Non-repudiation, Integrity.

To implement Digital Signature algorithm, the hash value was calculated from the document and converted it into the smart cards. This is important that we have to activate the smart card by entering a personal identification number or PIN code. Here the private key will be generated and stored on smart card and the PIN code will be with the user because the public key and private key are mathematically linked. Once the PIN code has been entered the card will be activated and smart card is ready to use.

1. INTRODUCTION

Now-a-days the necessity of network security has been raised. Most of the fields like organizations, business fields, military and educational sectors are needed to use network to transfer data.

As the communication and data transfer is becoming easier at the same time the network security question is arising. Since unauthorized users can hack the information (or) modify the information that was made to move through network.

In order to rectify these problems we use digital signature, through which the data can be secure and send to a specified user.

The digital signature mainly deals with the development of security features there by allowing the user as well as network organization to keep track of intrusions and thereby enhancing the security features.

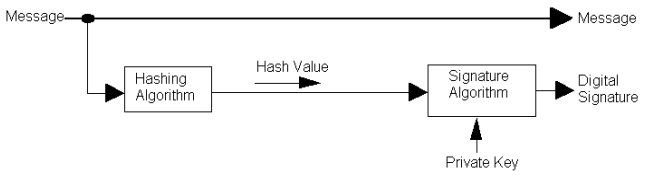
By using the following four models Digital Signature will send data through network in a Safe mode

1. Secrecy 2. Authentication 3. Non-repudiation 4. Integrity if your print area fits within the space allowed.

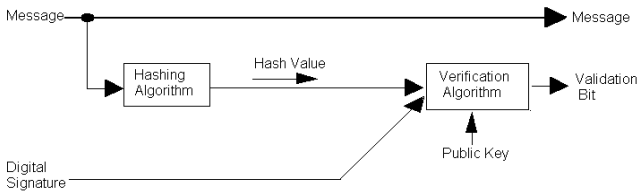
2. MAIN TITLE

2.1 Methodology and Plan:-

There are two steps involved in creating a digital signature from a message. The first step involves creating a hash value (also known as a message digest) from the message this hash value is then signed, using the signer's private key. The following is an illustration of the steps involved in creating a digital signature.



To verify a signature, both the message and the signature are required. First, a hash value must be created from the message in the same way the signature was created. This hash value is then verified against the signature by using the public key of the signer.



If the hash value and the signature match, you can be confident that the message is indeed the one the signer originally signed and that it has not been tampered with.

3. HASH FUNCTION

A hash value h is generated by a function H of the form

$$h = H(M)$$

Where M is a variable-length message and H(M) is the fixed-length hash value. The hash is appended to the message at the source at a time when the message is assumed or known to be correct. The receiver authenticates that message by re-computing the hash value. Because the hash function itself is not considered to be secret, some means is required to protect the hash value.

We begin by examining the requirements for a hash function to be used for message authentication. Because hash functions are, typically, quite complex, it is useful to examine some very simple hash function design.

Requirements for a Hash Function

The purpose of a hash function is to produce a "fingerprint" of a file, message, or other of data, to be useful for message authentication; a hash function H must have the following properties

1. H can be applied to a block of data of any size.
2. H produces a fixed-length output.
3. H(*x*) is relatively easy to compute for any given *x*, making both a hardware and software implementations practical.
4. For any given value *h*, it is computationally infeasible to find *x* such that H(*x*) = *h*. This is sometimes referred to in the literature as the **one-way** property.
5. For any given block *x*, it is computationally infeasible to find y! =x with H(*y*) = H(*x*). This is sometimes referred to as **weak collision resistance**.
6. It is computationally infeasible to find any pair (*x, y*) such that H(*x*) = H(*y*). This is sometimes referred to as **strong collision resistance**

Hash Values

Hash algorithms map binary values of an arbitrary length to small binary values of a fixed length, known as hash values. A hash value is a unique and extremely compact numerical representation of a piece of data. If you hash a paragraph of plain text and change even one letter of the paragraph, a subsequent hash will produce a different value. It is computationally improbable to find two distinct inputs that hash to the same value.

Message authentication code (MAC) hash functions are commonly used with digital signatures to sign data, while message detection code (MDC) hash functions are used for data integrity.

DSA PARAMETERS

The DSA makes use of the following parameters:

1. p=a prime modulus, where 2^L-1<p<2^L for 512<=L<=1024 and L a multiple of 64
2. q=a prime divisor of p-1, where 2^159<q<2^160.
3. g=h^ (p-1)/q mod p, where h is any integer with 1<h<p-1 such that h^(p-1)/q mod p>1.
   (g has order q and p).
4. x = a randomly or pseudo randomly generated integer with 0<x<q.
5. y = g^x mod p.
6. k = a randomly or pseudo randomly generated integer with 0<k<q.

The integers 'p','q', and 'g' can be public and can be common to a group of users. A user's private and public keys are 'x' and 'y', respectively. They are normally fixed for a period of time. Parameters 'x' and k' are used for signature generation only, and must be kept secret. Parameter 'k' must be regenerated for each signature.

DSA SIGNATURE GENERATION

The signature of a message M is the pair of numbers r and s computed according to the equations below:

r = (g^k mod p) mod q and

s = (k^-1(SHA-1(M) + xr)) mod q.

In the above,K^-1 is the multiplicative inverse of k, mod q;i.e.,(K^-1 K) mod q=1 and 0<K^-1<q.

As an option, one may wish to check if r=0 or s=0. If either r=0 or s=0, a new value of k should be generated and the signature should be recalculated (it is extremely unlikely that r=0 or s=0 if signatures are generated properly).The signature is transmitted along with the message to the verifier.

s = f1(H(M) ,k , x ,r , q) = (k^-1(H(M) + xr))mod q

r = f2 (k , p , q ,g) = (g^k mod p)mod q

DSA SIGNATURE VERIFICATION

Prior to verifying the signature in a signed message, p, q and g plus the sender's public key and identity are made available to the verifier in an authenticated manner.

Let M', r', and s' be the received versions of M, r, and s, respectively, and let y be the public key of the signatory. To verify the signature, the verifier first checks to see that 0<r'<and 0<s'<q;

if either condition is violated the signature shall be rejected. If these two conditions are satisfied, the verifier computes.

w = (s') ^-1 mod q

u1 = ((SHA-1(M')) w) mod q

u2 = ((r') w) mod q

v = (((g) ^u1 (y) ^u2) mod p) mod q.

If v=r',then the signature is verified and the verifier can have high confidence that the received message was sent by the

party holding the secret key x corresponding to y. For a proof that v=r' when M'=M, r'=r, and s'=s,

If v does not equal r', then the message may have been modified, the message may have been incorrectly signed by the signatory, or the message may have been signed by an impostor. The message should be considered invalid.

w = f3(s',q) = (s')^-1 mod q

v = f4(y,q ,g ,H(M'),w,r')

= ((g(H(M')w)mod q yr' w mod q)mod p)mod q.

Correctness of the algorithm

The signature scheme is correct in the sense that the verifier will always accept genuine signatures. This can be shown as follows:

From $g = h^z \bmod p$ follows $g^q \equiv h^{qz} \equiv h^{p-1} \equiv 1 \pmod p$ by Fermat's little theorem. Since $g>1$ and q is prime it follows that g has order q.

The signer computes

$$s = k^{-1}(\text{SHA-1}(m) + xr) \mod q.$$

Thus

$$\begin{aligned} k &\equiv \text{SHA-1}(m)s^{-1} + xrs^{-1} \\ &\equiv \text{SHA-1}(m)w + xrw \pmod q. \end{aligned}$$

Since g has order q we have

$$\begin{aligned} g^k &\equiv g^{\text{SHA-1}(m)w} g^{xrw} \\ &\equiv g^{\text{SHA-1}(m)w} y^{rw} \\ &\equiv g^{u1} y^{u2} \pmod p. \end{aligned}$$

Finally, the correctness of DSA follows from

$$r = (g^k \bmod p) \bmod q = (g^{u1} y^{u2} \bmod p) \bmod q = v.$$

My Work

Digital signature has created on smart card. The hash value was calculated from the document and converted it into the smart cards. This is important that we have to activate the smart card by entering a personal identification number or PIN code. Here the private key will be generated and stored on smart card and the PIN code will be with the user because the public key and private key are mathematically linked. Once the PIN code has been entered the card will verify both the keys and activate the smart card. The card is ready to use.

4. ACKNOWLEDGEMENTS

I have proposed a method for implementing a network security system which provides the security to the labs in the form of smart cards. The methodology is that the smart card will be activated for a particular lab by entering the pin code. Once the pin code entered the both keys will be verified. Now the smart card is ready to use.

The problem here in this proposed system is to activate smart cards. Some times when enter the pin code it will not activate. Again it has to re activate by giving the other pin code.

The security of this system needs to be examined in more detail. The reader is urged to find a way to break the system. Once the method has withstood all attacks for a sufficient length of time it may be used with a reasonable amount of confidence.

REFERENCES

[1] Cryptography and Network Security: Principles and Practice, by William Stallings

[2] Network Security , by M.V. Arun Kumar

[3] Cryptography and Network Security , by Behrouz A. Forouzan , Debdeep Mukhopadhyay

[4] Cryptography for the Internet, by Philip R. Zimmermann.

[5] Privacy on the Line," by Whitfield Diffie and Susan Eva Landau.

[6] Firewalls and Internet Security: Repelling the Wily Hacker," by William R.

[7] Google.com