International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064

Digital Signature Scheme Using Two Hash Functions

Mohammad Amir[1], Jarrar Ahmed [2], Sham Bansal[3], Ashish Kumar Garg[4], Man Singh[5]

[1] Delhi University, Department of Mathematics, IP College for Women, Civil Lines, New Delhi – 110054, India

[2] Delhi University, Department of Mathematics, Dyal Singh College, Lodhi Road, New Delhi - 110003, India

[3] Delhi University, Department of Mathematics, Bharti College, C4, Janakpuri, New Delhi - 110058, India

[4] Delhi University, Department of Mathematics, JDM College, Rajinder Nagar, New Delhi – 110060, India

[5] Delhi University, Department of Mathematics, SPM College, West Punjabi bagh, New Delhi - 110026, India

Abstract: ***Digital signature scheme is a fundamental cryptographic tool which allows one to sign an electronic message and later the produced signature can be verified by the owner of the message. This latter present a digital signature scheme and discuss the security aspects of proposed digital signature scheme. In this scheme any third party can verify the signature validity only with the help of signature receiver. The security of proposed digital scheme is based on the difficult problem of computing discrete logarithms over finite fields (e.g. DSA and ElGamal).***

Keywords: Digital Signature, One-way hash function, discrete logarithms**,** Security, Message.

1. Introduction

In general, a hand-written signature or a seal is attached to a document to indicate the owner's identity. As we move to the world where our decision and agreements are communicated electronically, we need to counterfeit these procedures. Public key cryptography (*PKC*) provides mechanism for such procedure through digital signature scheme. A digital signature scheme is the most important cryptographic tools in *PKC*, In order to prove the authenticity of transmitted electronic message; the digital signature is often employed. The digital signature schemes ensure the integrity of data and prove the authenticity of the users. Because of the essential need, many digital signature schemes [1], [3]-[8] have been proposed. A digital signature schemes consists of the following:

- A signature generation algorithm, which is a method for producing a digital signature. A signature verification algorithm, which is a method for verifying a digital signature.
- There are two general modes of digital signature schemes: Appendix mode and message recovery mode. Digital signature schemes with appendix rely on cryptographic hash function and require the original message as input to the verification algorithm. The hash value of signed message is usually involved in signature process to prevent message forgery attacks. Hash functions are useful in signature schemes for several reasons. First of all, public-key signing algorithms tend to be very slow, so taking the hash value of a large message and signing the (small) resulting value is much more efficient than simply signing the whole message. Secondly, if you wanted to add multiple signatures to a document, without the use of hash functions, the resulting signed message would be many times the size of the original.

If you did the same thing, only signing the hash value of the message, you would only be adding a small (320 bit for DSS) overhead for each signature added. We want our hash function to be collision free so that "any change to a message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify". DSA, ElGamal [8] and Schnorr signature scheme [7] are such digital signature schemes. In message recovery mode the signed message is recovered by the receiver from the received signature. A prior knowledge of the message is not required for the verification algorithm. The RSA, Nyberg-Ruppel and Rabin are such digital signature schemes. This paper proposed a digital signature scheme, in this scheme; any third party can check the signature validity with the help of signature receiver or the signer. Both the signer and signature receiver have full authority over the signature verification process.

2. Proposed Digital Signature Scheme

We use the following settings throughout the paper

- A large prime modulus p, where $2^{511} < p < 2^{512}$.
- A number g is the generator of Z_p^*.
- Collision free one-way hash functions [2] h_1 and h_2. The parameters p, g and h_2 are common to all users. For our proposed digital signature scheme, we use Schnorr's signature scheme which is a well-known variant of ElGamal

signature scheme. Suppose that user A wants to generate a signature on the message m such a way that only receiver B can direct verify the signature and B can also prove the validity of signature to any third party C, whenever necessary. To increase the security we use two different one-way hash functions h_1 and h_2, where h_1 is private hash function of A. The signing and verification processes are as follows:

2.1 Signature Generation by A

- A picks random $k \in Z_p$ and computes
- $\alpha = g^{-k} \bmod p$ and $\beta = g^{h_1(m)}.y_B^k \bmod p$. Where y_B is public key of B.
- Using a one-way hash `function h_2, A computes a secret value $S_A = h_2(m).g^{h_1(m)}$.
- A computes $Z = h_1(m) + x_A.S_A \bmod \phi(p)$

Here x_A is the private key of signer. Public key and private key are related by the equations:

$y_A = g^{x_A} \bmod p$ and $y_B = g^{x_B} \bmod p$

$\{Z, \alpha, \beta, m\}$ is the signature of A on the message m.

2.2 Signature verification by B

- Using his private key x_B, B computes $N = \beta(\alpha)^{x_B} \bmod p$ and recovers $S_A = h_2(m).N$
- B checks the congruence $g^Z \equiv N.y_A^{S_A} \bmod p$ for a valid signature.
- If this congruence holds then $\{Z, \alpha, \beta, m\}$ is a valid signature.

2.3 Signature Validation

Since $N = \beta(\alpha)^{x_B}$

$= g^{h_1(m)}.(y_B)^k.(g^{-k})^{x_B}$

$= g^{h_1(m)}.(g^{x_B})^k.(g^{-k})^{x_B}$

$= g^{h_1(m)}.$

then B recover $S_A = h_2(m).N$

$= h_2(m).g^{h_1(m)}$

And checks $g^Z \equiv N.y_A^{S_A} \bmod p$

L.H.S = g^Z

$= g^{h_1(m)+x_A.S_A}$

R.H.S = $N.y_A^{S_A}$

$= g^{h_1(m)}.g^{x_A.S_A}$

L.H.S = R.H.S it implies the validity of signature scheme.

2.3 Proof of validity by B to C

- B picks random $k \in Z_p$ and computes $\alpha_C = g^{-k} \bmod p$, $\beta_C = N.y_C^k \bmod p$ and send to C.
- C uses (α_C, β_C) in place of (α, β) to check the validity of signature by using his secret key. The process of signature verification will remain same as above verification,

3. Security Discussions

In this section , we will discuss the security of this proposed Signature Scheme.

- $Z = h_1(m) + x_A.S_A \bmod \phi(p)$?

Here the number of unknown variables are three ,Equation is one and h_1 is private hash function of A so it is computationally infeasible for a forger to get the private key x_A, hash value $h_1(m)$ and secret value S_A from the equation.

- Can anyone forge a signature $\{Z, \alpha, \beta, m\}$ by the equation $g^Z \equiv N.y_A^{S_A} \bmod p$?

Obviously to compute the integer S_A is equivalent to solving the discrete logarithm problem. Thus the proposed digital signature scheme is secure.

4. Conclusion

In this paper, we discussed a digital signature scheme. In this scheme, the signature receiver has full authority over the signature verification process. Nobody can check the validity of signature without his co-operation. Security of this scheme is based on discrete logarithm problems. Hence security level of this scheme is similar to other discrete logarithm based schemes like ElGamal and DSA.

5. Future Research

Implementation of Digital Signature Scheme in real world problem. And to search a Digital Signature Scheme ,in which security is not based on the solving problem of factoring integer(RSA) or finding discrete logarithm over finite fields.

References

[1] C.-G. Kang, “New digital multi signature scheme in electronic contract systems,” in Proc. 1995 IEEE Int. Symp. on Information Theory, Whistler, BC, Canada, Sept. 1995, pp. 486–486.
[2] Damgard I.B. (1987). Collision free hash function and public key signature scheme Advance
[3] in Cryptology - Eurocrypt - 87, Springer Verlag, p.p. 203-216.
[4] J. M. Piveteau, “New signature scheme with message recovery,” Electron. Lett., vol. 29, no. 25, pp. 2185–2185, Dec. 1993.

[5] K. Nyberg and R. A. Rueppel, “Message recovery for signature schemes based on the discrete logarithm problem,” in Proc. Eurocrypt’94, Perugia, Italy, May 1994, pp. 182-193.
[6] L. Harn, “New digital signature scheme based on discrete logarithm,” Electron. Lett., vol. 30, no. 5, pp. 296–298, Mar. 1994.
[7] NIST. (1994). Digital signature standard, U.S Department of Commerence, FIPS PUB, 186.
[8] Schnorr C.P. (1991). Efficient signature generation by Smart cards, Journal of Cryptology -4(3), p.p. 161-174.
[9] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithm,” IEEE Trans. Inform. Theory, vol. 31, pp. 469–472, July 1985
[10] Z. Shao, “Signature scheme based on discrete logarithm without using one-way hash function,” Electron. Lett, vol. 34, no. 11, pp. 1079–1080, May 1998.

Author Profile

Mohammad Amir received the M.Tech. degree in Computer Applications from Indian Institute of Technology Delhi in 2012.