A Secured Digital Signature Scheme using Masked Technique

[1]Jyotirmoy Das , [2]Dr.Sangeeta Kakoty, [3]Dr. Lakshmi Prasad Saikia
[1]Research Scholar, Department of Computer Science & Engineering, Assam Downtown University.
[2]Dr.Sangeeta Kakoty, Dy. Director- Multimedia, Krishna Kanta Handiqui State Open University.
[3]Dr. Lakshmi Prasad Saikia, Professor and Dean, Engineering & Technology, Assam Downtown University.

Abstract : The information handled electronically requires protection as well as authentication. Digital signature is a tool which can be thought of as some extra functionality on to traditional cryptography of encryption and decryption. Digital Signature provides security for electronic transaction by using private and public key. Functions of a Digital signature include confidentiality, authenticity, data integrity and non-repudiation. This paper discusses the role of Digital Signatures in today's world and will also analyze a new method for safe and effective information exchange.

IndexTerms - **Cryptography, Public key, Diffie Hellman, RSA, Digital Signatures**

I. INTRODUCTION

Cryptography is a branch of information security. Cryptography includes techniques which can turn a message into some unreadable format which is called ciphertext. In networking and communication the use of cryptographic protocols are in great demand. Cryptography is important for more than just privacy. Cryptography protects the world's banking system as well. Without the ability to protect bank transactions and communications, criminals could interfere with the transactions and steal the money without trace. Cryptography can be classified into two categories - Symmetric Key Cryptography and Asymmetric Key Cryptography. The field of cryptography, in recent times, has expanded a lot and many security services have been added to ensure security apart from encryption and decryption. Cryptographic protocols such as Signature Schemes deal with the application of cryptographic algorithms for ensuring the privacy, confidentiality, authentication of information. Symmetric and asymmetric algorithms can be viewed as primitives to develop various applications for secured communication over insecure channels. Cryptographic protocols use these primitives as building blocks to build secure modern services. Every Web browser uses the Transport Layer Security scheme, which is an example of a cryptographic protocol. The introduction of cryptographic protocols such as signature schemes can be considered as one of the major development in the field of cryptography. In order to provide secure communication for various applications, protocols such as digital signatures have been employed in critical applications such as secure web browsing for e-commerce like applications and hence they have become an essential part of modern crypto-systems.

II. DIGITAL SIGNATURES

A Digital Signature is a cryptographic security scheme which demonstrates the authenticity of a message that is being transferred from a sender to a receiver over an insecure network such as the Internet. A digital signature provides reasons for the receiver to believe that the message received, was really sent by the claimed sender which provides a way to detect forgery or tampering. Here, a signer *U1* has a private key and a public key. A user *U2* wants to get a message *m* signed by *U1*. So *U1* generates the signature *S* with an algorithm which takes input *m* and *U1*'s private key and sends *S* to *U2*. On the other end *U2* can verify using a verification algorithm which uses *U1*'s public key. There are many applications of Digital signatures in information security, which includes authentication, data integrity, and non-repudiation [14]. Among others, one of the significant applications of digital signatures is the certification of public keys in large networks. The first signature scheme was the RSA Signature scheme which was proposed by Rivest, Shamir and Adleman. The security of the RSA signature scheme was based on the well-known RSA assumption. The RSA scheme is subject to forgery and so it is not secured. In other words, it is easy to create a valid message-signature pair without asking the signer directly. Moreover, it is seen that if the message is too long then the signature takes a long time to be computed or the message does not remain in the domain of the signing function.

III. PROPOSED DIGITAL SIGNATURE SCHEME USING THE MASKING TECHNIQUE

The RSA Digital Signature Scheme generally shows us the basic architecture of how to use and implement a signature scheme. In this paper we propose a new and secured technique for implementing the RSA Digital Signature Scheme using by masking the signature for improving security of the scheme. The steps are as follows :

Step 1: Implement Diffie Hellman Key Exchange protocol and obtain a shared secret key K.

Step 2: Implement RSA algorithm to generate the public key pair (n,e) and private key (p,q,d).

Step 3: Generate the signature S with the help of the RSA digital signature scheme

Step 4: Mask the signature S to to get S~and send it to the other user alongwith message X.

Step 5: Unmask the signature S~ to obtain S on the other end.

Step 6: Verify the Signature is valid or not.

Following is a mathematical example used to show the working of the proposed scheme :

User 1

P=23, g=11

a = 6

U1 = g^amod p

= 11^6 mod 23

= 9

User 2

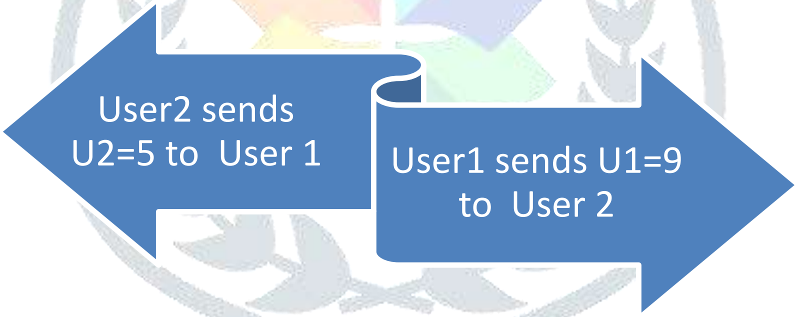
P=23, g=11

b = 5

U2 = g^amod p

= 11^5 mod 23

= 5



User 1

K= U2^a mod p

= 5^6 mod 23

= 8

User 2

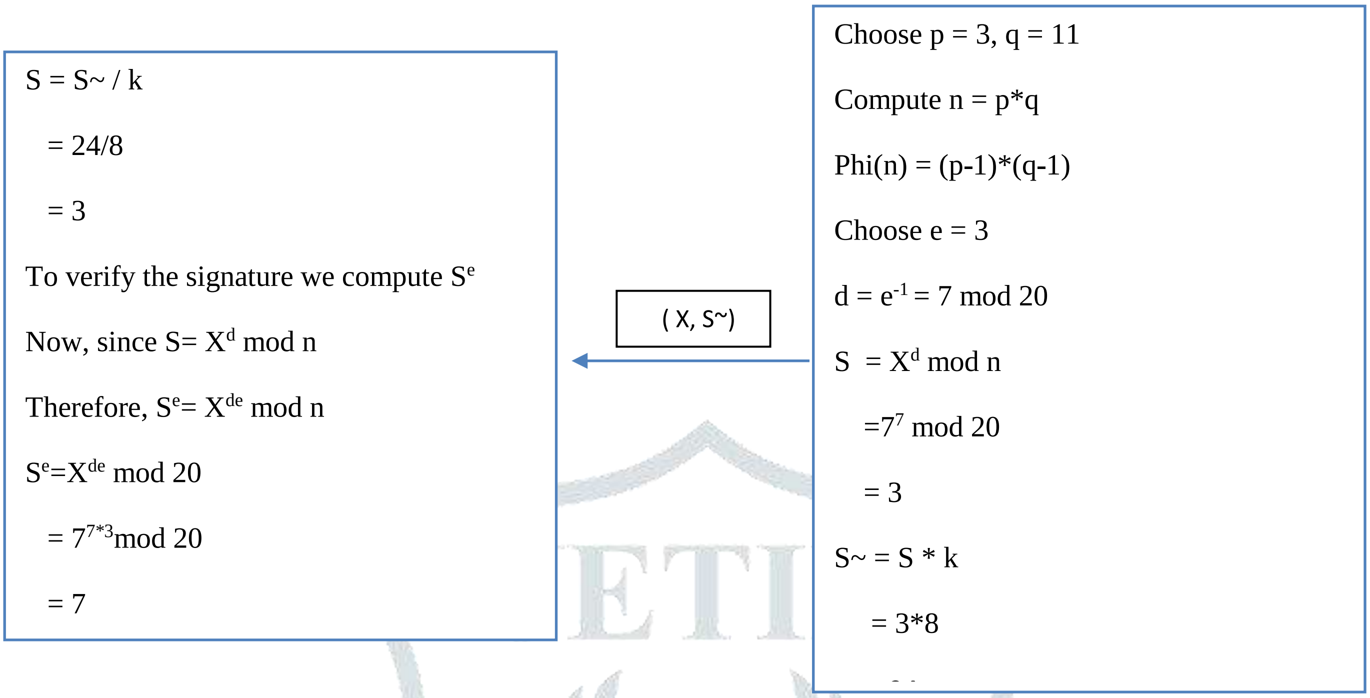
K= U1^b mod p

= 9^5 mod 23

= 8

Therefore, the shared secret key K=8

Now let us implement the RSA and then mask the Signature, Let the message be X=7



Choose p = 3, q = 11

Compute n = p*q

Phi(n) = (p-1)*(q-1)

Choose e = 3

d = e^{-1} = 7 mod 20

S = X^d mod n

=7^7 mod 20

= 3

S~ = S * k

= 3*8

(X, S~)

S = S~ / k

= 24/8

= 3

To verify the signature we compute S^e

Now, since S= X^d mod n

Therefore, S^e= X^{de} mod n

S^e=X^{de} mod 20

= 7^{7*3}mod 20

= 7

Now if S^e = X, then we can conclude that the signature is valid.

IV. CONCLUSION

The proposed model is likely to provide more security than the normal RSA Digital Signature Scheme the signature is masked using the shared secret key obtained from Diffie Hellman Key Exchange protocol. Since the signature is masked, hence it becomes more difficult for anyone to generate another copy of the genuine signaturewhich provides more security to the overall cryptosystem.

V. ACKNOWLEDGMENT

The first author acknowledges the academic support of second and third author and Assam Downtown University during the preparation of this paper.

REFERENCES

[1] Arya, P.K., Aswal, M.S., Kumar, V., "Comparative Study of Asymmetric Key Cryptographic Algorithms", International Journal of Computer Science & Communication Networks,Vol 5(1),17-21

[2] Asghar N., 2011, "A Survey on Blind Digital Signatures"

[3] Bhattacharya, P., Debbabi, M. Otrok, H., "Improving the Diffie-Heliman Secure Key Exchange", 2005 International Conference on Wireless Networks, Communications and Mobile Computing

[4] Carts, D., "A Review of the Diffie Hellman Algorithm and its Use in Secure Internet Protocols", SANS Institute, 2001.

[5] Das, J., Kakoty, S., Ahmed, M, " A Modified Public Key Encryption Technique using Masked Keys", World Wide Journal of Multidisciplinary Research and Development, 2017; 3(11): 28-30

[6] Diffie, W., Hellman, M.E., "New Directions in Cryptography". IEEE Transaction on information theory, IT-22, pp. 472-492, 1978.

[7] Garg, V., Rishu, "Improved Diffie-Hellman Algorithm for Network Security Enhancement", International Journal Computer Technology & Applications, Vol 3 (4), 1327-1331

[8] Internet Engineering Task Force (IETF) Working Group. Diffie-Hellman Key Agreement Method, RFC 2631, June 1999.

[9] Paar, Jan Pelzl, J.. "Understanding Cryptography-A Textbook for Students and Practitioners", Springer; 1st ed. 2010 edition

[10] Zhou, X., Tang, X., "Research and Implementation of RSA Algorithm for Encryption and Decryption", 2011 the 6th International Forum on Strategic Technology. DOI: 10.1109/IFOST.2011.6021216.