Secure Multisignature Generation for Group Communication

Rutba Maqsood, Surabhi Thukral, Divya Upadhyay

Abstract- Multi-signature is a signature scheme in which signers jointly generate a signature on a message. Our project applies Multisignature scheme for sending messages in a group. Multisignature is more secure and eliminates the latest attacks. Individual signers are identified by the information contained in Multisignature. Our project provides an overview and comparison between the RSA cryptosystem and Elgamal cryptosystem applied on groups for sending and receiving messages. The basic theories of the RSA cryptosystem[4] and Elgamal cryptography are explored. The RSA cryptosystem and Elgamal cryptography theories are quite similar. The idea of the RSA cryptosystem is to secure communication via networks by using public keys to encrypt and decrypt messages, where a private key is kept secret. This shows that the reliability and strong security of the RSA cryptosystem depends on the degree of difficulty of integer factorization. Therefore, in this paper the methods for integer factorization are discussed. In addition this paper also represents how the security of Elgamal cryptography is based on the difficulty of discrete logarithm problem where it is straight forward to raise numbers to large powers but it is much harder to do the inverse computation of the discrete logarithm. Through this paper we tried to provides an overview and comparison between the RSA cryptosystem and Elgamal cryptosystem applied on groups for sending and receiving messages.

Keywords: Digital Signature, Elgamal Cryptosystem, Multi Signature, RSA

I. INTRODUCTION

In distributed systems it is sometimes necessary for users to share the power to use a cryptosystem. The system secret is divided up into shares and securely stored by the entities forming the distributed cryptosystem. The main advantage of a distributed cryptosystem is that the secret is never computed, reconstructed, or stored in a single location, making the secret more difficult to compromise. Investigations within the fields of threshold group-oriented signature schemes, threshold group signature schemes, Multisignature schemes, and Threshold-Multisignature schemes resulted in explicitly defining the properties of threshold multisignature schemes.

The RSA cryptosystem and Elgamal cryptography theories are quite similar. The idea of the RSA cryptosystem is to secure communication via networks by using public keys to encrypt and decrypt messages, where a private key is kept secret. This shows that the reliability and strong security of the RSA cryptosystem depends on the degree of difficulty of integer factorization. Therefore, methods for integer factorization are discussed. In addition we show how the security of Elgamal cryptography is based on the difficulty of discrete logarithm problem where it is straight forward to raise numbers to large powers but it is much harder to do the inverse computation of the discrete logarithm

II. OVERVIEW OF DIGITAL SIGNATURES

Digital signatures[5] are one of the most important inventions of modern cryptography. The problem is how can a user sign a message such that everybody (or the intended addressee only) can verify the digital signature and the signature is good enough also for legal purposes.Assume that all users use a public-key cryptosystem. Signing a message w by a user A so that any user can verify the signature;dA(w) Signing a message w by a user A so that only user B can verify the signature;eB (dA(w)) Sending a message w and a signed message digest of w obtained by using a hash function standard h:(w, dA(h(w))) Digital sigantures should be such that each user should be able to verify signatures of other users, but that should give him/her no information how to sign a message on behind of other users.The main difference from a handwritten signature is that digital signature of a message is intimately connected with the message, and for different messages is different, whereas the handwritten signature is adjoined to the message and always looks the same. Technically, digital signature is performed by a signing algorithm and it is verified by a verification algorithm.A copy of digital (conventional) signature is identical (usually distinguishable) to (from) the origin. A care has therefore to be made that a classical signature is not misused.This chapter contains an overview of the main techniques for design and verification of digital signatures (as well as some attacks to them). If only signature (but not the encryption of the message) are of importance, then it suffices that Alice sends to Bob(w, dA(w)) Caution: Signing a message w by A for B byeB(dA(w)) is O.K., bat the symmetric solution with encoding was c = dA(eB(w)) is not good.Any public-key cryptosystem in which the plaintext and cryptotext spaces are the same can be used for digital signature.

III. THRESHOLD SIGNATURE SCHEMES

In many applications, a threshold or more shareholders are required to cooperatively generate a digital signature, in contrast to the conventional single signer.

Manuscript received on February, 2013.
Rutba Maqsood, M.Tech CSE, AmityUniversity, Noida, India.
Surabhi Thukral, M.Tech CSE,Amity University, Noida, India.
Divya Upadhyay, Assistant Professor CSE, Amity University, Noida, India.

This may also be seen as a distribution of trust since the shareholders must collaborate and contribute equally to produce a valid multiparty signature. Threshold Multisignature schemes combine the properties of threshold group-oriented signature schemes and multisignature schemes. In the literature, Multisignature schemes are also referred to as threshold signature schemes with traceability. The combined properties guarantee the signature verifier that at least t members participated in the generation of the group-oriented signature and that the identities of the signers can be easily established. The majority of the existing Multisignature schemes belong to variants of the single signatory, generalized ElGamal signatures extended to a group/multiparty setting. In our project the basic theories of the RSA cryptosystem and Elgamal cryptography are explored. The RSA cryptosystem and Elgamal cryptography theories are quite similar. The idea of the RSA cryptosystem is to secure communication via networks by using public keys to encrypt and decrypt messages, where a private key is kept secret. This shows that the reliability and strong security of the RSA cryptosystem depends on the degree of difficulty of integer factorization. Therefore, methods for integer factorization are discussed. In addition we show how the security of Elgamal cryptography is based on the difficulty of discrete logarithm problem where it is straight forward to raise numbers to large powers but it is much harder to do the inverse computation of the discrete logarithm.

a) RSA Algorithm

"Public key cryptography," a method for encrypting messages to be transmitted over an insecure channel, and "digital signatures," a method for authenticating the author of a message transmitted over an insecure channel, are emerging as fundamental tools for conducting business securely over the Internet.The RSA Algorithm [1] was named after Ronald Rivest, Adi Shamir and Leonard Adelman, who first published the algorithm in April, 1977.Since that time, the algorithm has been employed in the most widely-used Internet electronic communications encryption program, Pretty Good Privacy (PGP).It is also employed in both the Netscape Navigator and Microsoft Explorer web browsing programs in their implementations of the Secure Sockets Layer (SSL), and by Mastercard and VISA in the Secure Electronic Transactions (SET) protocol for credit card transactions.

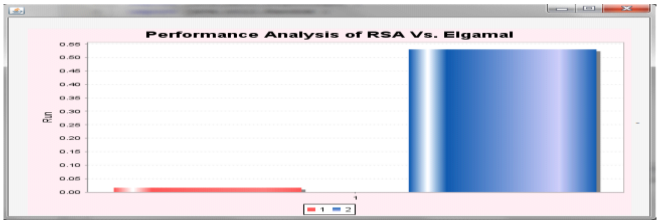
b) El Gamal algorithm

The ElGamal system [2] is a public-key cryptosystem based on the discrete logarithm problem. It consists of both encryption and signature algorithms. The encryption algorithm is similar in nature to the Diffie-Hellman key agreement protocol.

The system parameters consist of a prime p and an integer g, whose powers modulo p generate a large number of elements, as in Diffie-Hellman. Alice has a private keya and a public key y, where y = ga (mod p). Suppose Bob wishes to send a message m to Alice. Bob first generates a random number k less than p. He then computes y1 = gk (mod p) and y2 = m xor yk,

where xor denotes the bit-wise exclusive-or. Bob sends (y1 ,y2) to Alice. Upon receiving the ciphertext, Alice computes m = (y1a mod p) xor y2 .

IV. PERFORMANCE ANALYSIS



1: RSA 2: Elgamal

It is visible from the above graph that the performance of RSA is much better than the performance of Elgamal when compared on the basis of encryption time.

V. CONCLUSION

An efficiency analysis was conducted between RSA and Elgamal algorithms on the basis of their execution time and it was analyzed that the ELGAMAL algorithm, takes a lot of time in data encryption as compared to RSA algorithm when implemented on a system for sending and receiving e-mails. The time taken by the RSA is less than .05ms and by Elgamal is .55ms.

REFERENCES

1. H.L. Nguyen, " RSA Threshold Cryptography",May 2005
2. Allam Mousa,"Security and performance of elgamal encryption parameters", Journal of Applied Sciences 5(5),2005
3. Bruce Scheneir, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition
4. Q. Wang, Z.F. Cao, "Formal model of proxymulti-signature and a construction", Chinese Journal ofComputers. vol. 29, no. 9, pp. 1628-1635, 2006
5. X. F. Yuan, R. Y. Sun, J. Q. Sun, Y. H. Yang, "Signature scheme with message recovery based on discrete logarithms and factoring", Computer Applications. vol. 27, no.10, pp. 2460-2463, 2007.
6. Ian, A.G and P.M. Grant, 2004. Digital Communications 2nd Edn, Prentice Hall.
7. Webno Mano, 2004. Modern Cryptography Theory and Practice , Prentice Hall
8. Hoang Long Nguyen. Partially Interactive Threshold RSA Signatures.Cryptography and Coding. Institute of Mathematics and its application,IMA 2005.
9. Adam Barnett and Nigel P.Smart. Mental Poker Revisited. Cryptography and Coding 2003, Springer-Verlag LNCS 2898, pp. 370-383, 2003.
10. Dan Boneh and Matthew Franklin. Efficient Generation of shared RSA keys. J. ACM, 48, 702-722, 2001.

AUTHORS PROFILE

Ms. Rutba Maqsood is doing her M.Tech. from Computer Science and Engineering, Amity School of Engineering and Technology, Amity University, Uttar Pradesh. She would be pursuing PHD in Computer Engineering. Her research area is Cryptography and network Security.

Ms. Surabhi Thukral is doing her M.Tech. from Computer Science and Engineering, Amity School of Engineering and Technology, Amity University, Uttar Pradesh. She would be pursuing PHD in Computer Engineering. Her research area is Cryptography and network Security.

Divya Upadhyay received her M.Tech in Information Security from GGSIP University, New Delhi. Presently she is working as an Assistant Professor in CSE Department, Amity University, Noida, Uttar Pradesh, India. Her Research area includes Information Security and Security Engineering.