ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 10, October 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Elgamal Based PGP in Email System

Upakar Paudel
Department of Computer Science
BESE Student, Gandaki College of Engineering and Science(GCES)
Pokhara – Nepal

Abstract: Email, even though, being widely used network application, it is heavily insecure. PGP is an outstanding scheme which provides service of confidentiality and authentication for electronic mail and file storage application. PGP uses algorithms like AES(for confidentiality), SHA-1(for authentication) and RSA(public-private key generation to maintain both confidentiality and authentication).

This paper approaches the idea of using asymmetric encryption called ElGamal in place of RSA within PGP to overcome the several limitations found within RSA approach.

Keywords: RSA, AES, SHA-1, session key, public key, private key, confidentiality, authentication.

I. INTRODUCTION

PGP(Pretty Good Privacy) is developed by Phil Zimmerman in 1991 to provide services of security mostly in email system. Features of PGP like wide range of applicability, survival of extensive reviews, free worldwide are some reason for it's growth. PGP is on Internet standards track(RFC 3156) and is widely popular among individuals rather than corporation. The major criteria for measuring security of any system is confidentiality and authentication. PGP thrives to provide high quality of these services(confidentiality and authentication).

ElGamal is a asymmetric key encryption algorithm for public-key cryptography based on Diffie-Hellman key exchange. Taher ElGamal described this approach in 1985. Similar to RSA, ElGamal encryption have 3 different steps: key generation, encryption and decryption. ElGamal can be defined over any cyclic group and its strength depends upon discrete logarithmic on elliptic curve.

Normally, PGP uses RSA algorithm for generating public-private keys and encrypting certain session keys or messages. This paper present the idea to replace RSA and use ElGamal instead of it. The description of RSA and other algorithms used in PGP like AES, SHA-1 etc are beyond the scope of this paper but this paper will provide the working of ElGamal encryption.

II. WORKING OF PGP WITH ELGAMA

Operation of PGP with ElGamal for authentication and confidentiality service is described below:

Authentication:

For authentication digital signature is used by PGP. The process to maintain authentication is PGP with ElGamal is

- The message written by sender is passed to hashing algorithm(SHA-1, MD5) to generate 160-bit hash code of the message.
- The generated hash code is encrypted with ElGamal encryption algorithm using sender's private key which is also generated by ElGamal.
- The result is send to the receiver.

- Receiver uses sender's public key to decrypt and achieve hash code.
- Receiver compares decrypted hash code with previously generated hash code. If they match with each other, the message is accepted to be authentic.

Confidentiality:

Another important service provided by PGP is confidentiality. To maintain confidentiality, session key is used which is a onetime key generated randomly and uniquely every time a message is to be sent. Session key are normally 128-bit keys. The confidentiality service as provided by PGP with ElGamal is described in following steps:

- Message is written by sender and a random 128 bit session key is generated by sender.
- The message is encrypted using AES or 3DES or some other symmetric algorithm using key as the generated session key.
- The session key is then encrypted with ElGamal encryption using the public key of receiver.
- Receiver receivers encrypted session key and encrypted message.
- The receiver uses his private key as generated by ElGamal to decrypt encrypted session key.
- Thus, obtained session key is used to decrypt encrypted message.

This process guarantees confidentiality as message is always encrypted during the network path. Confidentiality and authentication service are both used together in PGP for increased security.

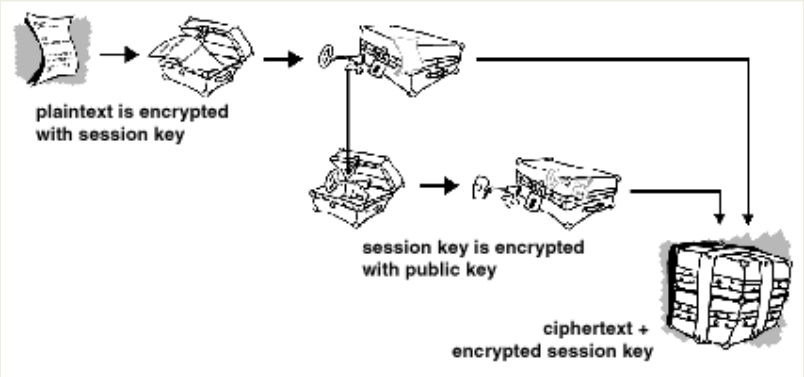

Fig : Encryption process for confidentiality

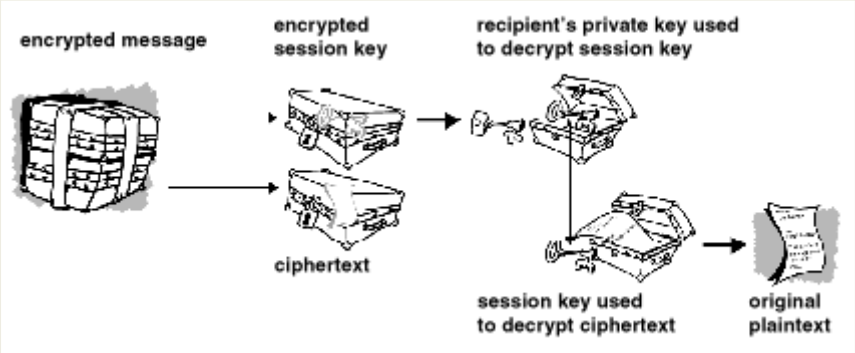

Fig : Decryption Process for Confidentiality

III. Benefit of ElGamal over RSA

ElGamal possess various benefits over RSA. Use of ElGamal over RSA can increase the performance as well as maintain high security. Some reason to consider ElGamal over RSA in PGP are:

- RSA encryption is faster than ElGamal encryption but RSA decryption is slower than ElGamal decryption. Since, decryption needs to be performed multiple times than encryption, ElGamal approach has a slight benefit over RSA.
- RSA encrypted message is larger than ElGamal encrypted message even though level of security is same.

- ElGamal rely on hardness of discrete logarithmic on elliptic curves. Although, the mathematics are complex in elliptic curve it have high performance.

IV. ELGAMAL ALGORITHM

ElGamal Algorithm have 3 components: key generation, encryption algorithm and decryption algorithm.

Key Generation:

- Generate an efficient description of cyclic group G of order q with generator(this is a subset such that every element of group can be expressed in combination) g.
- Choose x randomly from 1 to q-1.
- Calculate $h = g^x$
- (G,q,g,h) is public key and x is kept as private key

Encryption:

- Use receivers public key to encrypt message. Let it be (G,g,q,h).
- Choose y randomly from 1 to q-1.
- Calcualte $c1 = g^y$
- Calculate $s = h^y$
- Map secret message m onto an element m' of G.
- Calculate $c2 = m'*s$
- Ciphertext is $(c1,c2) = (g^y , m'*h^y)$ where $h = g^x$.

Decryption:

- Ciphertext be (c1,c2) and private key be x.
- Calculate $s = c1^x$
- Compute $c2 * s^{-1}$ where $c2 = m' * h^y$. This gives m'.

$$c2 * s^{-1} = m' * h^y * (g^{xy})^{-1}$$
$$= m' * g^{xy} * g^{-xy}$$
$$= m'$$

m' is the intended message.

V. CONCLUSION

This paper approaches the idea of using ElGamal encryption within PGP system instead of RSA to improve performance and security of PGP. RSA algorithm consist of many limitations. The major limitation of RSA is if public and private key are of higher bit size than decryption is slower. To overcome this ElGamal technique can play an important role.

PGP thrives to provide confidentiality and authentication services. These two services can be provided in high standard by PGP system completely based on ElGamal.

References

1. William Stallings, "Cryptography and Network Security: Principles and Practices, Third Edition." Upper Saddle River, NJ: Prentice Hall, 2003.
2. Tutorialspoint, "Cryptography" www.tutorialspoint.com/cryptography/
3. D.A Atkins, W.Stallings, P.Zimmerman, "PGP Message Exchange Formats", http://www.ietf.org/rfc/rfc1991.txt
4. http://www.pgpi.org/doc/pgpintro
5. http://en.wikipedia.org/wiki/Pretty_Good_Privacy
6. http://en.wikipedia.org/wiki/ElGamal_encryption
7. http://en.wikipedia.org/wiki/RSA_(cryptosystem)
8. W Diffie, M. E. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory
9. T ElGamal, "A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms", IEEE Transactions on Information Theory.

10. Mini Malhotra, Aman Singh, Department of Computer Science, Lovely Professional University, Punjab, India "Study of Various Cryptographic Algorithms", International Journal of Scientific Engineering and Research
11. Annapoorna Shettry, Shravya Shetty, Krithika K, Department of Information Technology, St. A loysius Institue of Management of Information Technology, Beeri, Mangalore, India, "A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm", International Journal of Innovative Research in Computer and Communication Engineering.
12. Rashmi Singh, Shiv Kumar, Mewar University NH – 79 Gangrar, (Rajasthan), India, "ElGamal's Algorithm in Cryptography", International Journal of Scientific and Engineering Research.

AUTHOR(S) PROFILE

Upakar Paudel, currently pursuing Bachelor of Engineering in Software Engineering(BESE) from Gandaki College of Engineering and Science(GCES) have completed +2 in Science from SOS and SLC from Global Collegiate Higher Secondary School. His area of interest is machine learning, cryptography and network security.

