Journal of Electrical Electronics and Communication Engineering
Volume 01, Issue 01, July 2025
www.ijeece.com

E-Mail Protection Using a Good Privacy Algorithm

G Mohit
Department of Electronics and Communication Engineering, Aditya University, Kakinada
Corresponding Author: gmohitece2123@gmail.com

To Cite this Article
Mohit, "Email Protection Using a Good Privacy Algorithm", Journal of Electrical Electronics and Communication Engineering, Vol. 01, Issue 01, July 2025, pp:01-03.

Abstract*: The purpose of this research is to discuss the growing issue of online communication security and privacy. Compared to other methods, we achieve a high level of security and privacy by using the Pretty Good Privacy (PGP) algorithm. Phil Zimmerman is credited with establishing this protocol. It protects files' integrity and encrypts them. This algorithm first transforms the file into ciphertext before sending it via conventional mailer. Every user possesses both a public key and a private key. The file is encrypted using the private key, which is kept confidential. Everyone is aware of the public key, which is used to decrypt the file that the user encrypted. This procedure operates more quickly than previously mentioned, despite the fact that it may appear drawn out and tiresome.*

Keywords*: E-Mail, Server access, Search engine, Optimization, Gmail*

I. Introduction

Nowadays, security is a significant problem that many consumers must consider. The likelihood that someone will read our content is very great because the number of users of the internet is increasing daily. There are numerous distinct protocols in use. Each has different methods and approaches to handling data. Phil Zimmerman, the creator, initially dubbed this Guerilla Freeware. This algorithm's primary tasks are encryption and decryption. The difficulty is that there may be numerous lengthy certificate chains extending from one individual to another because anyone can issue certificates. Ultimately, to think that the first link in the chain is trustworthy. The entire chain breaks down if someone gives someone a certificate incorrectly.

II. E-Mail Traffic Congestion

Another name for a hash is a message digest. It is a one-way application that performs encryption tasks. The procedure carried out at the sender's end is encryption. The PGP software receives the sender's original message as input. This turns this into some text that will appear to be complete garbage using its own methods. This is referred to as the cypher text or hash text. The user must utilize a code known as his public key in order to accomplish this. The traditional medium is then used to convey this cypher text. Nothing will make sense to anyone who intercepts this transmission.

Through a certificate known as a key certificate, each user's key is verified as authentic. This is one of PGP's most crucial features. Another unique feature is that the user can get this certificate from any server or similar source with no effort. A certificate can be given by any user to anybody. Because of this, PGP is a very useful protocol. However, these certificates are not absolutely required. All that is required to send a message to a user is the encoding of the recipient's public key. It is not necessary to keep the public key private. Because anyone can send me an encrypted message using this key, but nobody can see what I send. However, there is a drawback to this certification process as well.

III. Revoking a Certificate

A person has the right to revoke a certificate if they are aware that they have authenticated it to the incorrect individual. As a result, the whole chain that relied on this certificate is no longer legitimate. The chain breaks. Keys can be revoked in the same manner. A user has the right to quickly revoke their private key if it has been lost or stolen. uses a random ciphertext as the output and a message as the input. This has the unique quality that it is nearly impossible to identify which input produced a given result. The work that it performs has no precise mathematical meaning.

There is a degree of randomness in this. Furthermore, the hash text does not have to be as long as the message. Usually, it has a set length, such as 128 or 256 bits. The length of a message's hash text can be increased in proportion to how secure we need it to be. PGP's ability to compress files to half their original size after generating the hash text is another characteristic that contributes to its versatility. Thus, the gearbox is substantially quicker. Each user of PGP has the option to include their digital signature with the message they send. It improves the data's security and privacy even more. The signature field in PGP is typically only 8 bits long. Additionally, there is a feature that allows the software to produce the user's private key. The user only needs to indicate the private key's size. The MD 5 technique is then used to produce the private key after a password has been entered.

IV. Key Rings

A key ring is a type of data structure that includes certificates, user information, and public keys. Although it can be uploaded to the internet, this is often saved on the local computer. A user can have three different levels of confidence in his connections in PGP. They are None, Partial, and Complete. The user's level of confidence in a person determines how trustworthy the certificates they have signed.

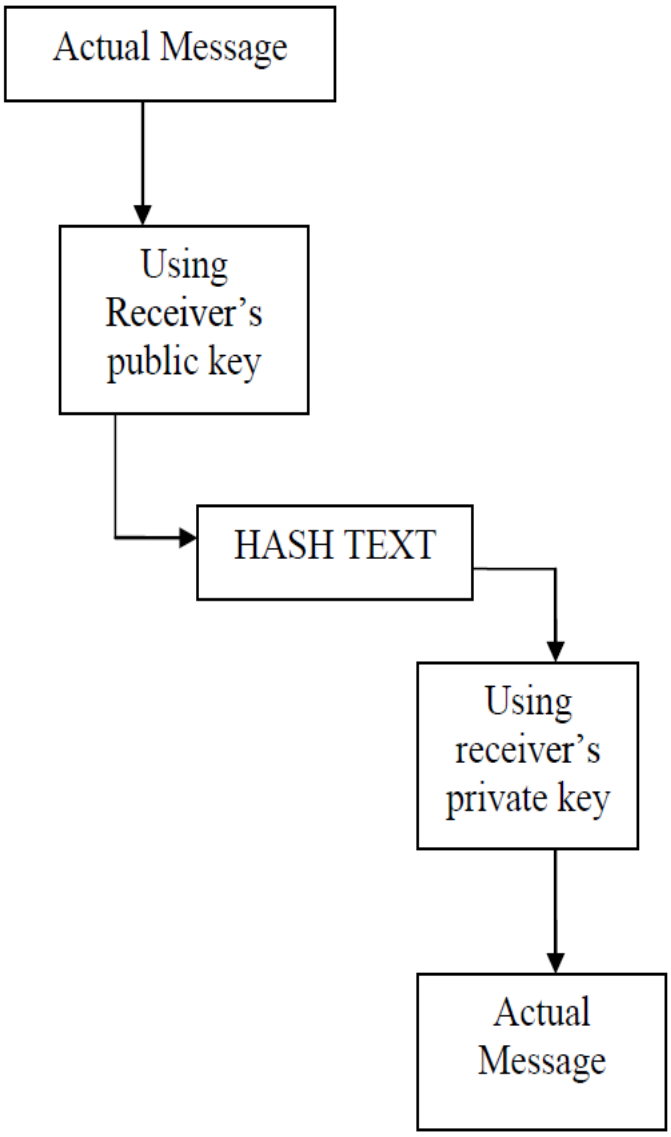

Fig 1: Block diagram for E-Mail congestion

V. Encrypted Message

IDEA (International Data Encryption Algorithm) handles the encryption procedure. After selecting the IDEA key for encryption, the sending PGP application encrypts it using the recipient's public key. This appears in the message's header. In order to verify the sender's identity to the recipient, the user in this communication utilizes his digital signature. The remainder of the process stays the same.

VI. Conclusion

We therefore draw the conclusion that this specific algorithm offers a very easy and safe means of private communication. There is no possibility of channel congestion or transmission slowdown because the message is compressed before being sent. Disregarded. The user has the last say on whether or not to trust. In the PGP algorithm, no message appears to be typical. It is made up of a series of simple items. This is a very helpful tool for safe and secure data transmission because it is freely accessible online.

References

[1] Mohan Kumar, Sasank and Sokamso "An Matrix Converter using Array System in Power Electronics in Communication Systems". Springer Conference in GMR University, Rajam, Andhra Pradesh, Vol. 4, No. 1, April 2019

[2] Saritha, Srikanth, Subhakar and Sunitha, "A Process control system in Industrial Applications using Thyristors in power electronics for PMSG",". IEEE Transactions 2015. India, 12 – 15, December 2014.

[3] Niharika, Lakshman Reddy and Shanchie, "A Novel of MIMO concepts in wireless relay networks in Space Time and Space Frequency in achieve diversity", " IEEE Conference Proceedings on Innovative Research in Communication Systems (IRCS), International Conference. vol. 2, pp. 67 – 75, January. 2010

[4] John Diesel, Shang Chee and Cooper Lee, "Standalone Grid system for On and OFF modes Using Renewable energy sources using PMMC Technology', "Springer Proceedings on Green Energy on World environmental Day", IEEE conference proceedings held at Madras University, on the 20tt Century. pp.10-19, 2020

[5] F Max Savio, M Sasi Kumar. "An Effective Control Technique for an Impedance Source Inverter Based Wind Energy System". 2012 IEEE International Conference on Emerging Trends in Electrical Engineering and Energy Management (ICETEEEM-2012)

[6] Sasikumar M and Chenthur Pandian S. "Characteristics Study of ZSI For PMSG Based Wind Energy Conversion Systems". Journal of Electrical Engineering (JEE). ISSN: 1582-4594.