

# Building an Encrypted E-Mail System using PGP

Naman Gautam<sup>1</sup>, Shagun Verma<sup>2</sup>, Manan Shori<sup>3</sup>

<sup>1,2,3</sup>Student, Department of Computer Science & Engineering, Manav Rachna International Institute of Research & Studies, Sector-43, Surajkund Road, Faridabad, Haryana, India

\*\*\*

**Abstract** - Secure & encrypted communication is when two individuals or two parties connect with each other, and even including the medium of the communication service itself, the connection that is established between these two entities is completely protected from a third party. This method of exchanging process can be accomplished using the system of encryption and decryption. The paper aims to explain how it is achieved by using a chrome extension generated using PGP (an encryption software) to demonstrate how it continues to operate by using authentication of private and public keys. This extension layer further facilitates us to help accomplish the entire contact with these PGP standards' protection. This paper will be focusing on the techniques that can also be found with any email service provider of their initial choice to start enforcing the framework.

**Key Words:** Encrypted Communication, Encryption, Decryption, Cryptography, Security, PGP standards, Email.

## 1. INTRODUCTION

Communication with encryption is alluded to as cryptography and is a science and technology for developing a framework that will provide us with information security. The information would therefore be communicated as an indecipherable text rather than an unprotected plain text while two or more computers connect with an application that has some type of encryption.

By using the necessary method of encryption, a network may be set up where the accurate data or information can only be easily obtained by those interested in personal correspondence.[1] The types of encryption algorithms are currently recognized in two broad categories: symmetric key encryption and asymmetric key encryption.

In the asymmetric key encryption technique, only one hidden key is shared between the users and is used for encryption and decryption. Two keys are used to encrypt and decrypt the message through a public key and a private key in the case of asymmetric key encryption technique.

Pretty Good Privacy is a recognized, general-purpose application to encrypt files, emails, and confidential data.[2] Strong cryptographic algorithms like RSA, SHA-1 are used for its implementation of the algorithm.

## 2. LITERATURE REVIEW

Encryption of user data is established and supported by far too many email applications or websites. It could have been a myth because, even though encryption is complete, the organization will quickly decipher encrypted data whenever they have private keys on hand.[3]

There have been several protocols developed and implemented to assure the security of such communication. These protocols provide the security services of message confidentiality and message authentication for an e-mail message.

Primarily focused on those possibilities, a chrome extension has been developed to catch and fully run its analysis of the real-life Gmail e-mail encryption and decryption process. We have also attempted to demonstrate another extension known as Mailvelope, which is currently the most used by many customers as well as software developers.

## 3. CRYPTOGRAPHY

The basic idea of a cryptographic system is to cipher information or data in such a way as to ensure the confidentiality of information that an unauthorized person would not be able to derive its meaning.[4] Two of the most common uses of cryptography will be to use it to transfer data through an unsafe medium, like the Internet, or to ensure that unauthorized people do not understand what they are looking at in a situation in which they have access to information.

Modern cryptography does not only enable you to protect your data on the Internet or to authenticate for certain services, but also evaluate a function on private inputs of multiple parties, without anyone being able to learn something about these inputs.

The secret information is usually called "plaintext" in cryptography, and the procedure of attempting to disguise the plaintext is known as "encryption"; the encrypted plaintext is referred to as "ciphertext." "A range of rules known as" encryption algorithms "accomplish this method. The encryption process typically relies on an "encryption key" that is then given as an input to the encryption process along with the data. [5] The receiving side can get the data through a "decryption key" Using the "decryption algorithm".

The art and science of keeping messages safe is cryptography and is studied by cryptographers. Cryptanalysts are cryptanalytic experts, who are the art and science of cracking ciphertext. Cryptology is the field of mathematics, which involves both cryptography and cryptanalysis.

### 3.1 The cryptography priorities are:

- **Privacy:** To preserve the secrecy of hidden messages.
- **Authentication:** To confirm the origins of the post.
- **Integrity:** To ensure a message was not changed, the accuracy remains intact
- **Key management:** To distribute cryptographic algorithms of the hidden keys.

### 3.2 Cryptographic algorithms used to maintain confidentiality fall into one of two categories:

- **Symmetric-key Cryptography (use of a single private key)**
- **Asymmetric-key Cryptography (use of two keys: public & private keys)**

For the sake of building email encryption, we use Asymmetric-key Cryptography. It works on a simple principle which is a sender encrypts some data with some user's public key. Text once encrypted cannot be decrypted by anything other than the private key of the user. Even the public key which was used to encrypt the data cannot decrypt it. That is how it is ensured that the email we send can only be viewed by the user it is being sent to.

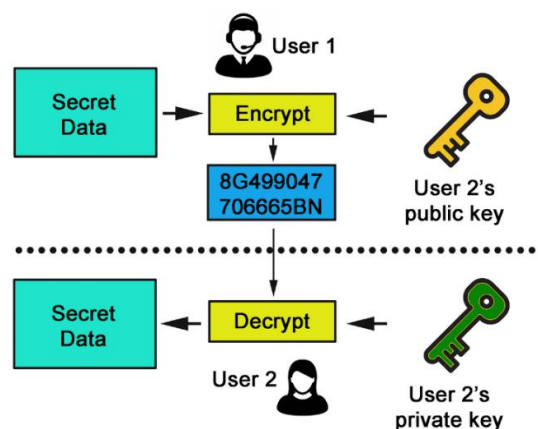


Figure 1. Asymmetric Cryptography

## 4. PGP – PRETTY GOOD PRIVACY

PGP stands for pretty good privacy. It is an encryption system that is used for sending encrypted emails as well as for encryption sensitive files. It was developed by Philip R. Zimmermann in the early 1990s.

In the early periods of PGP, it was used by activists, columnists, and by those who use it to manage confidential information.

#### 4.1 Working of PGP:

Initially, a huge, numbered key is generated which is a random session key. This random session key is generated through main algorithms and is not easily guessed.[6]

Then the encryption of this session key is done by the public key of the recipient. A public key is used for encrypting data. The public key is attached to a specific individual's identity, and anybody can use it to send them a message.

After this, the PGP session key is being sent by the sender to the recipient. The recipient becomes capable of decrypting it using their private key. By using the PGP session key, the recipient can decrypt the real message.

### 5. EMAIL ENCRYPTION IMPLEMENTATION

We developed a chrome extension that helped us implement the PGP Standards. Using this extension, a key pair can be generated for any email id, and it can be protected with a passphrase.

The user can encrypt the data which is being sent in the mail using the receiver's public key and it can be decrypted at the receiver's end using their private key.

Even if a third party has access to the key with which the text was encrypted it cannot be decrypted by it. Only the private key of the receiver can be used to do it.

#### 5.1. Project Files:

The project is completely open-source and can be downloaded from GitHub [here](#). Please note that to install the extension, Chrome Developer Mode must be switched on, and then it can be loaded unpacked. After it is loaded into Chrome, it needs to be turned on after which it will appear like in fig 2.

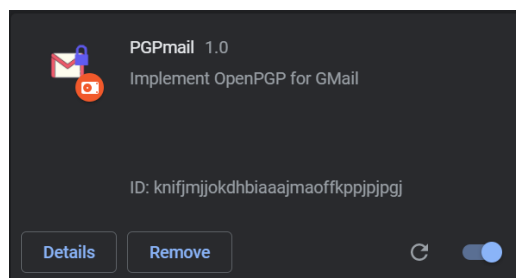


Figure 2. THE EXTENSION

#### 5.2. Extension Implementation:

1. We can see a key symbol in the extensions tab. This is the main extension and on clicking it we can use the extension and create keys for the recipient and the sender.

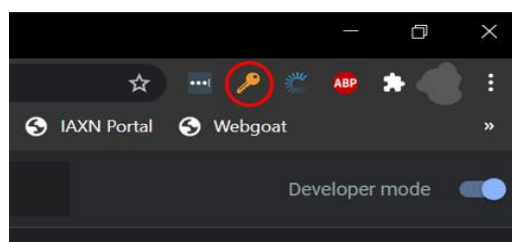


Figure 3. PGP MAIL ENCRYPTION BUTTON

2. As soon as we click the extension button, a new window is displayed which lets us see the existing PGP keys and make new ones.

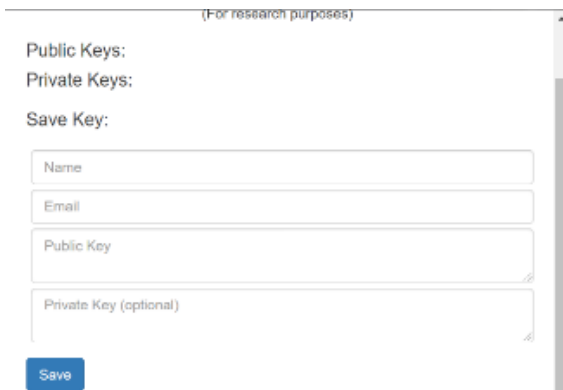


Fig 4. KEYS CAROUSEL.

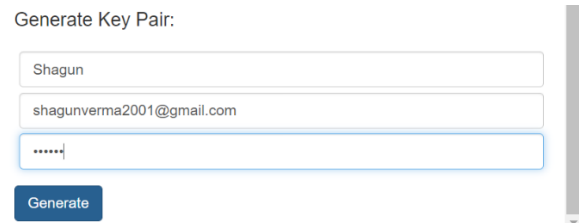


Fig 5. GENERATE KEY PAIR

3. There are four sections in the extension.
- a. **Public Keys:** This section displays the public keys we import using the Save key section.
  - b. **Private Keys:** This section displays the private keys that were imported from another extension or were generated using the Generate key pair.
  - c. **Save Key:** This section can be used to enter the name, email, and the public key and then save these details so that the extension.
  - d. **Generate Key Pair:** This section can be used to generate a key pair, a public and a private key associated with a name that can be locked with a passphrase.

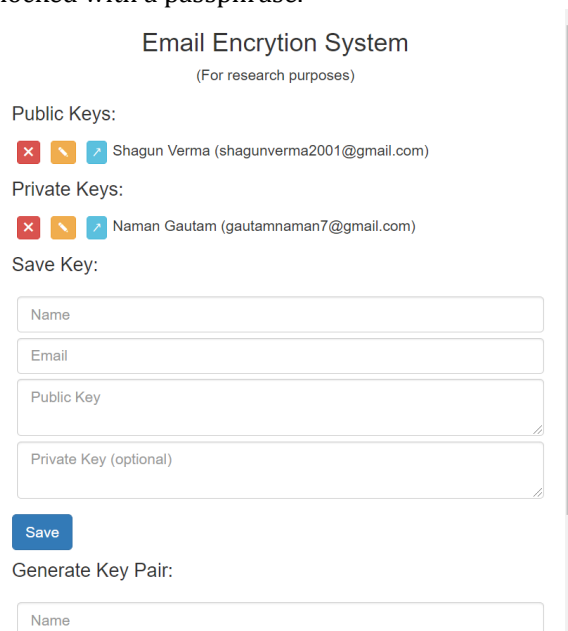


Fig 6. UPDATED PGP KEY CAROUSEL

- 4. A key pair can be generated in the extension using the Generate Key Pair section after entering the necessary details. As soon as the details are entered like in Fig.5, the key pair is generated and is displayed in the Key Carousel now. This has been illustrated in Fig 6.

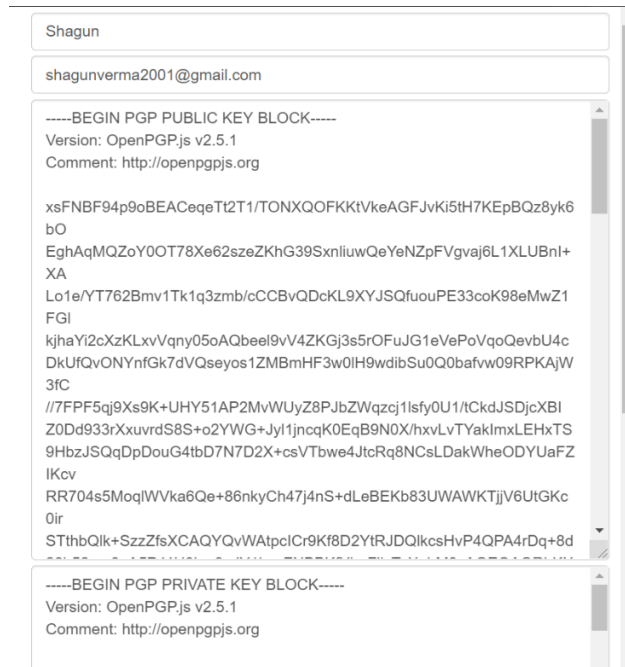


Fig 7. KEY EDITOR

- 5. On clicking the edit button against the name in the keys list, the recipient's details can be viewed, and both the keys can be seen and stored in a file for transferring.

### 5.3. Extension Working:

- 1. Now we will send the mail to the desired recipient, titled "Test Encryption Email". Normal text is entered into the mail. A new button appears beside the Send button known as the Secure Send button. As soon as this is clicked, it asks for a passphrase and when the right passphrase is entered into the field, the email is sent to the recipient.

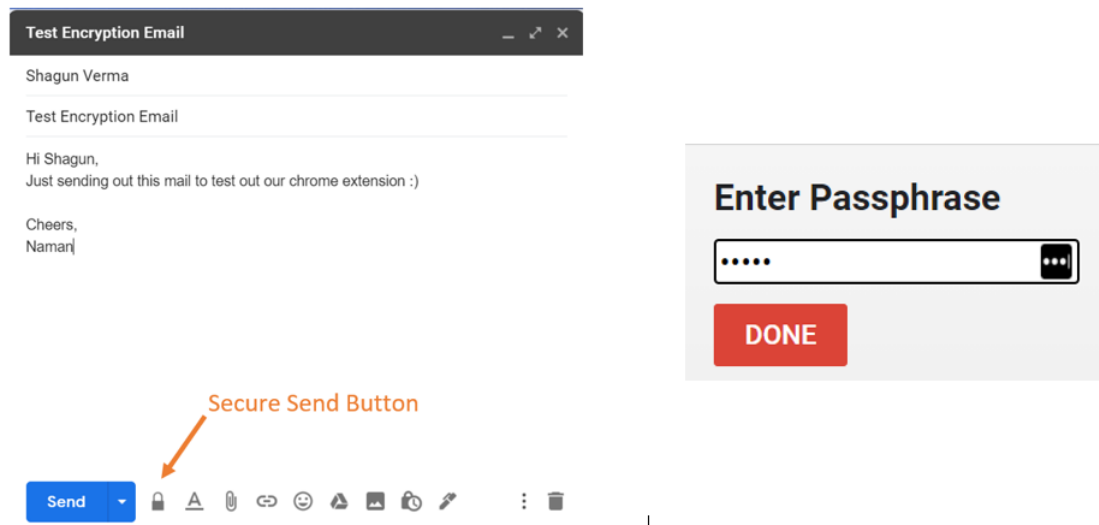


Fig 8. ENCRYPTING

- At the recipient's end, it can be concluded that the email did not go as is. The text was converted to an encrypted text using the PGP software on which the extension is based.

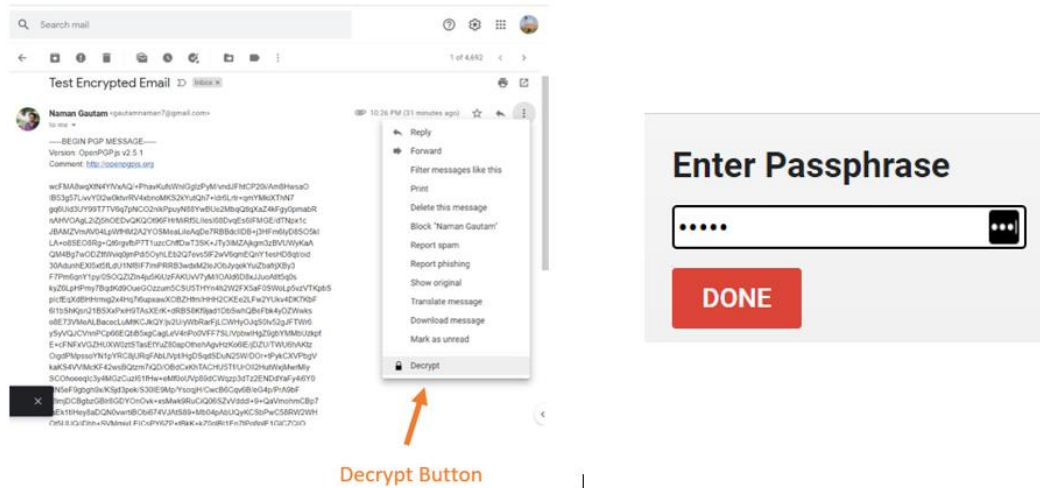


Fig 9. DECRYPTING

- A decrypt button appears in the options of the email. As soon as the receiver clicks Decrypt, they have to enter the same passcode which was used to create the key pair.



Fig 10. NORMAL TEXT AFTER DECRYPTION

- The recipient receives the mail like any other email and can see the original text which was sent.

## 6. CONCLUSIONS

This paper altogether with some crucial aspects of security. We studied the basic mechanism of cryptography and the two types of encryption algorithms. Over the past years, the number of email users has increased, and email has become a means of communication among thousands of users across continents.

In this paper, we presented a comprehensive review of the email architecture, components, and security protocols used for encryption and authentication processes. We discuss Pretty Good Privacy (PGP) and presented our extension implemented on Google Chrome. PGP is the most widely standards protocol to protect email messages, and how they can be used to enhance the security of Gmail service providers.

## 7. FUTURE SCOPE

If the extensions for sending mails are widely used or automated while sending emails, the scope of cyber-attacks like phishing and other fraudulent attacks can be avoided since one more layer of security is added that would take more than a decade to crack. Such extensions with a stronger update can work well for the defense departments in the country and ensure information security.

In the future, this work can be extended and evaluated for application-specific software codes written in other programming languages with different sets and numbers of keywords. The functionality of the extension can be extended to support the encryption of the attachments in further updates.

## REFERENCES

- 1) Vert, G. and Alfize, M., 2006. An Enhanced Pretty Good Privacy (EPGP) System with Mutual Non-Repudiation. In Security and Management (pp. 364-370).
- 2) Koch, A., 2019. Cryptographic protocols from physical assumptions (Doctoral dissertation, Karlsruhe Institute of Technology, Germany).
- 3) Qashqari, A., Alhbshi, D., Alzahrani, F., Ghwati, H. and Aljahdali, A., 2020. Electronic Mail Security. International Journal of Computer Science and Information Security (IJCSIS), 18(5).
- 4) Garfinkel, S., 1995. PGP: pretty good privacy. " O'Reilly Media, Inc."
- 5) Zimmermann, P.R. and Zimmermann, P.R., 1995. The official PGP user's guide (Vol. 5). Cambridge: MIT Press.
- 6) Fibíková, L. and Vyskoc, J., 2001, December. Practical cryptography-the key size problem: PGP after years. In Proceedings in Workshop "Santa's Get Together (pp. 10-11).
- 7) Lucas, M., 2006. PGP & GPG: Email for the practical paranoid. No Starch Press.
- 8) Shukla, R., Prakash, H.O. and Phanibhusan, R., 2016, March. Open PGP-based secure web email. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 735-738). IEEE.
- 9) Reuter, A., Boudaoud, K., Winckler, M., Abdelmaksoud, A., and Lemrazzeq, W., 2020, February. Secure Email-A Usability Study. In International Conference on Financial Cryptography and Data Security (pp. 36-46). Springer, Cham.
- 10) Callas, J., Donnerhacke, L., Finney, H. and Thayer, R., 1998. OpenPGP message format. RFC 2440, November.
- 11) DENG, H.J. and JIANG, M.F., 2010. Analysis of Encryption Theory and Security of E-mail System PGP [J]. Modern Computer, 14.
- 12) Kurniawan, Y., Albone, A. and Rahyuwibowo, H., 2011, July. The design of mini-PGP security. In Proceedings of the 2011 International Conference on Electrical Engineering and Informatics (pp. 1-4). IEEE.
- 13) McLaughlin, L., 2006. Philip Zimmermann on What's Next after PGP. IEEE Security & Privacy, 4(1), pp.10-13.
- 14) McMurdo, G., 1996. Pretty good encryption. Journal of information science, 22(2), pp.133-146.
- 15) Wueppelmann, D., 2015. PGP Auth: Using Public Key Encryption for Authentication on the Web (Doctoral dissertation, Carleton University).