E-Mail Security through Pretty Good Privacy Algorithm

C.Suriya,
Department of Electronics & Communication Engineering
Nandha College of Engineering, Erode, India.

1. ABSTRACT

This paper aims to address the ever increasing problem of privacy and security while communication through the internet. By making use of an algorithm known as Pretty Good Privacy **(PGP)** we achieve high amount of security and privacy compared to other algorithms. This is a protocol which was introduced by Phil Zimmerman. It performs encryption and integrity protection on files. Using this algorithm the file is first converted into cipher text and then transmitted using the traditional mailer. Each user has a private key and a public key. The private key is used for encrypting the file and it is kept as a secret. The public key is known to everyone and is used for decrypting the file which was encrypted by that user. Although this process may seem long and tedious, this process works faster than described above.

2. INTRODUCTION

Security is an important issue today that many users need to look into. Because the number of people using the interne is growing day by day the chances that our information is being read by someone are very high. There are many different protocols that are existent. Each differs in their algorithms and by the way they handle the data. This was first named as *Guerilla Freeware* by its author Phil Zimmerman. The main work done by this algorithm is encryption and decryption. Encryption is the process done at the sender’s end

The problem is that since anyone can issue certificates, there can be many long certificate chains leading from one person to another person. In the end, to believe that the first person in the chain is dependable. If one person gives a certificate wrongly to a person then the whole chain collapses.

3.HASHES

A Hash is also known as a Message digest. It is a one way program which does the work of encryption. It takes the Encryption is the process done at the sender’s end. He (the sender) gives his original message as input to the PGP software. This uses its own techniques and converts this into some text which will look like pure rubbish. This is known as the Hash text or cipher text. To do this, the user has to use a code which is known as his public key. Then it is this cipher text which is transmitted through the traditional medium. Anyone who intercepts this message will not be able to understand anything.

3.1 KEYS

The key of every user is certified that it is original by means of a certificate known as a key certificate. This is a very important feature in PGP. And another special feature is that the user need not do much of work to obtain this certificate from any server or something like that. Any user can give a certificate to anyone. This makes PGP a very much use friendly protocol. On he other hand, these certificate are not an absolute necessity. To send a user a message a just need to use the receiver’s public key for encoding. The public key need not be kept secret. Because with this key, anyone can send me an encrypted message but no one can read my messages. But there is also a disadvantage in this method of certification.

4.CERTIFICATE REVOCATION

When a person knows that he has authenticated a certificate to a wrong person, he/she has the rights to revoke the certificate. This means that the whole chain which was dependent on this certificate is no longer valid. The chain collapses.

In the same way, keys can also be revoked. If a user’s private key has been lost or stolen, then he can immediately revoke his/her private key. This is how PGP works:

message as the input and gives out a random cipher text as output. The very special property of this is that it is practically impossible to find which input has given a specific output. There is no specific mathematical definition for the work done by it. This involves some amount of randomness. Also the hash text need not be of the same length as that of the message itself. It is generally of some fixed length say 128 bits or 256 bits. The more we need a message to be secure, the more we can increase the length of its hash text. The various techniques that are used for encryption are :

- MD2 (Message digest 2)
- MD4 (Message digest 4)
- MD5 (Message digest 5)
- SHA-1 (Secure Hash algorithm)

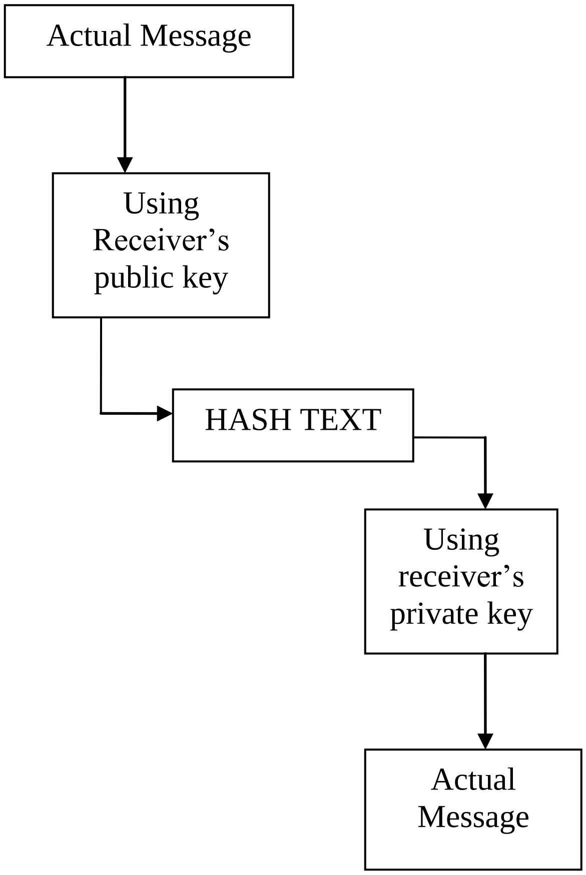
Also another feature which makes PGP a versatile program is that after creating the hash text, PGP compresses this file to half of its original size. So the transmission is much faster.

5. SIGNATURES

In PGP, every user can also attach his/her digital signature in the message which they transmit. It further strengthens the security and privacy of the data. Generally in PGP the signature field is only 8 bits long. There is also a provision by which the program itself will generate the private key for the user. All the user has to do is to specify the size of the private key. Then by giving a password the private key is generated by using MD 5 algorithm.

6. KEY RINGS

A key ring is a data structure that contains some public keys, some information about the users and the certificates. Generally, this is stored in the local computer but it can be uploaded on to the internet. Also in PGP there are three levels of trust that a user can have on his contacts. They are: Complete, Partial and None. Depending upon the amount of trust placed by the user on any person the certificates signed by that person are trusted or



7.1 ENCRPYTED MESSAGE

The encryption process is done by **IDEA (INTERNATIONAL DATA ENCRYPTION ALGORITHM).**
The sending PGP program chooses the IDEA key for encryption and then encrypts the IDEA key with the public key of the recipient. This is placed at the header of the message.

7.2 SIGNED MESSAGE

This is message in which the user uses his digital signature to confirm the identity of the sender to the receiver. The rest if the procedure remains unchanged.

8.CONCLUSION

Thus we conclude that this particular algorithm provides a very simple and secure way for private communication. As the transmitted message is in compressed form there is no chance for congestion in the channel or slowing down of transmission process.

ignored. The decision of trusting purely lies in the user's hands.

7. MESSAGE FORMATS

Any message in PGP algorithm does not look like a normal message. It consists of a sequence of primitive objects. They are:

- Encrypted message
- Signed message
- Encrypted signed message
- Signed human readable message

This being freely available on the internet, makes it a very useful tool for safe and secure transmission of data.

9.REFERENCES

1. Cryptography and network security, William Stallings, Pearson education.
2. Network security, Charlie Kaufmann, Radia Pearlman and Mike Spencer, Pearson Education.