ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

Cryptographic process for Cyber Safeguard by using PGP

Bharatratna P. Gaikwad[1]

Department of Computer Science and IT, Dr. Babasaheb Ambedkar Marathwada University Aurangabad, India[1]

ABSTRACT: Data security is crucial for all businesses as payment, personal files, bank account details all of this information is often impossible replace if lost and dangerous in the hands of criminals. Data lost due to disasters such as a flood or fire is devastating, but losing it to hackers or a malware infection can have far greater consequences. Encryption process are handle and protect your data is control to the security of our business and the privacy expectations of customers, employees and partner. Encryption is a powerful defensive weapon for free people. It offers a technical guarantee of privacy, regardless of who is running the government. It's hard to think of a more powerful, less dangerous tool for liberty. Cyber security is not a single problem, but rather a group of very different problems involving various sets of threats, targets and costs. As a result, legal policy analysis must begin by identifying the particular problem to be considered. It is clear that cyber attacks impose heavy costs and that the rate of attack is increasing. Security vulnerabilities continue to be discovered and disclosed in widely-deployed software at a great rate. Internet-connected computer users generally fail to take basic steps to patch the vulnerabilities in their software and to safeguard their systems from malicious code. Despite the large accumulated losses and warnings of more serious dangers, the internet remains a place of cyber insecurity. Pretty Good Privacy (PGP) is data encryption and decryption software that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions to increase the security of e-mail communications.

KEYWORDS: PGP, Encryption, Decryption, Cyber Security, Public Key, Private Key.

I. INTRODUCTION

In computer networks, the sensitive data are encrypted on the sender side in order to have them hidden and protected from unauthorized access and then sent via the network. When the data are received they are decrypted depending on an algorithm and zero or more encryption keys. The existence of many applications on the Internet, for example e-commerce (selling and buying through the Internet) is based on network security [1]. In a developing country such as India, a majority of its local organizations remain using firewall alone as a method of protecting their server from the intrusion issues. However, it can be outline that being dependent via this method alone for enhancing the security level without having other additional protection might not be adequate enough to protect the server from being accessed by intruders; the concept of Pretty Good Privacy (PGP) is associated with issues of computer security. While there have been numerous developments to ensure computer security such as Intrusion Prevention, network device hardening, router based firewalls and etc., the PGP concept may also partially aid in providing valuable improvements to issues concerning computer security [2].

Cryptosystem consists of cryptographic algorithm, keys and protocols that make it work. A cryptographic algorithm is a mathematical function used for the encryption and decryption process. This algorithm works in combination with a key, which can be a word, number or phrase, used for encryption of plaintext into ciphertext. The size of keys is measured in bits. The bigger the key, the more secure the ciphertext. There are two types of encryption: symmetric and asymmetric. In symmetric (also called secret key encryption) one key is used for encryption and decryption. This key is shared secret between communicating parties. Usually the size of key is up to 128 bits. One example of this type is Data Encryption Standard (DES). It is very fast, but it can be very expensive due to difficulty of secure key distribution. This problem is solved by asymmetric encryption (also called public-key encryption). It uses the pair of keys, one for encryption and one for decryption. One is published and called the public key; the other is kept secret and called the private key. It is computationally infeasible to deduce the private key from the public key. The size of keys is up to 1024 bits [3].

II. ENCRYPTION AND DECRYPTION

Encryption is a technique for transforming information in such a way that it becomes unreadable. This means that even if a hacker is able to gain access to a computer that contains protected information system, anyone will not able to read or interpret that information.

Data that can be read and understood without any special measures is called plaintext or clear text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext. You use encryption to make sure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption [4].

Encryption algorithms that use the same key for encrypting and for decrypting information are called symmetric-key algorithms. The symmetric key is also called a secret key because it is kept as a shared secret between the sender and receiver of information. Symmetric key encryption is much faster than public key encryption, often by 100 to 1,000 times. Encryption algorithms that use different keys for encrypting and decrypting information are most often called public-key algorithms but are sometimes also called asymmetric key algorithms. Public key encryption requires the use of both a private key (a key that is known only to its owner) and a public key (a key that is available to and known to other entities on the network).

Cryptography in relation of protecting the information and keep it safe and secret. The cryptography is the practice and study of hiding specific information; it is used to keep the information secret and safe. When a message is sent using cryptography, it is changed (or encrypted) before it is sent. The change makes the message hard to read. If someone wants to read it, they need to change it back (or decrypt it).How to change it back is a secret. Both the person that sends the message and the one that gets it should know the secret way to change it, but other people should not be able to. There are steps to do that when the message is decoded and sent by the sender choosing appropriate method and after that when it is received decoded by the recipient [5].

As per the Figure 1 input the plain text as “India” and apply the Encryption key algorithm on plain text as a India, after encryption of data is secure by unreadable format of data is called as Cipher text, this text can’t be recognized by human mind.

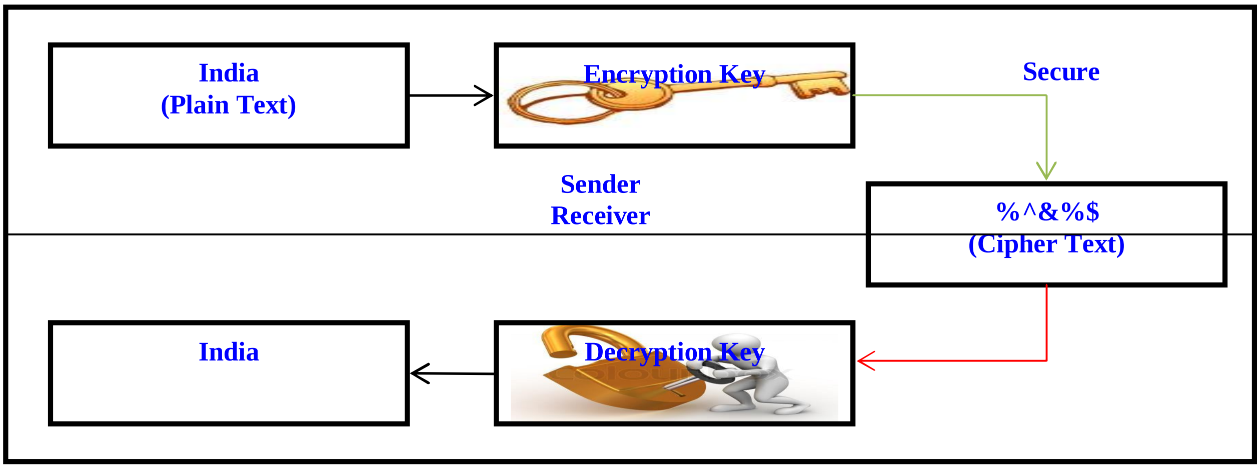


Fig.1. Encryption and Decryption methods with a secure channel for key exchange

Through the internet our data is send to destination person via email and receiver person get the data in the format of cipher text; there is need to decrypt by using decryption algorithm using decryption key. After successfully decryption it will generate the original message as same as sender person.

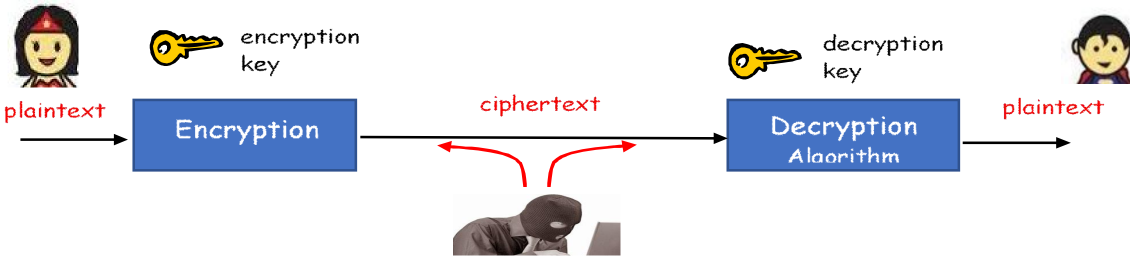


Fig.2.Cryptographic illustration

The main components of the symmetric encryption include - plaintext, encryption algorithm, secret key, cipher text and decryption algorithm. The plaintext is the text before applying the encryption algorithm. It is one of the inputs to the encryption algorithm. The encryption algorithm is the algorithm used to transfer the data from plaintext to cipher text. The secret key is a value independent of the encryption algorithm and of the plaintext and it is one of the inputs of the encryption algorithm. The cipher text is the scrambled text produced as output. The decryption algorithm is the encryption algorithm run in reverse [6][10].

III. PGP EXPLORATION

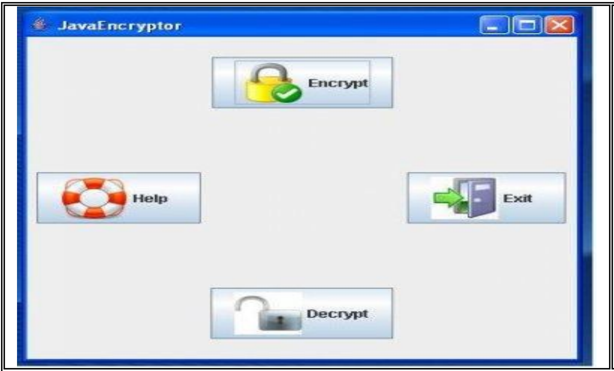
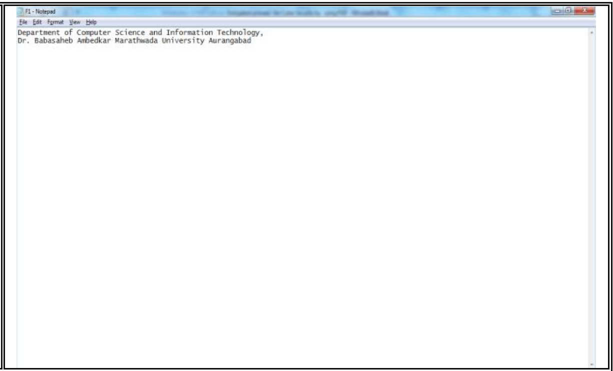
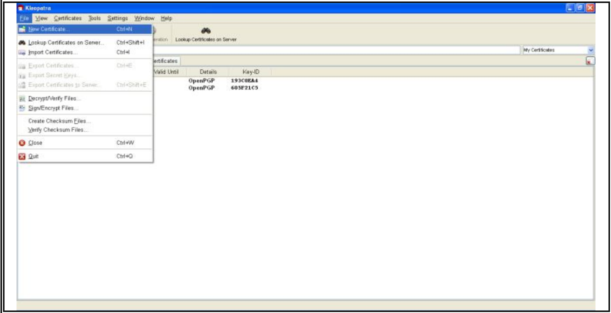
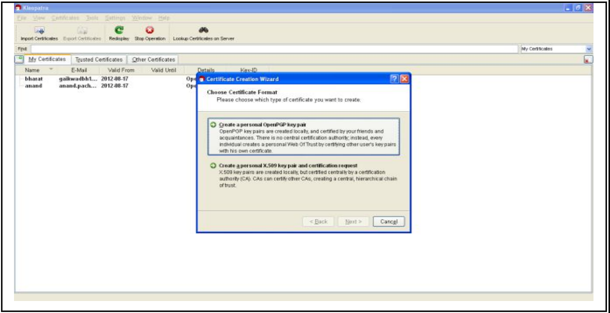
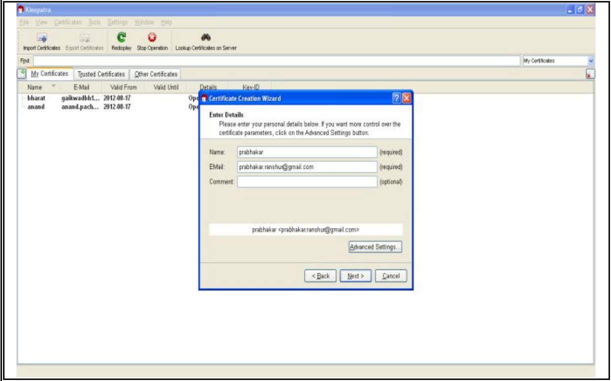
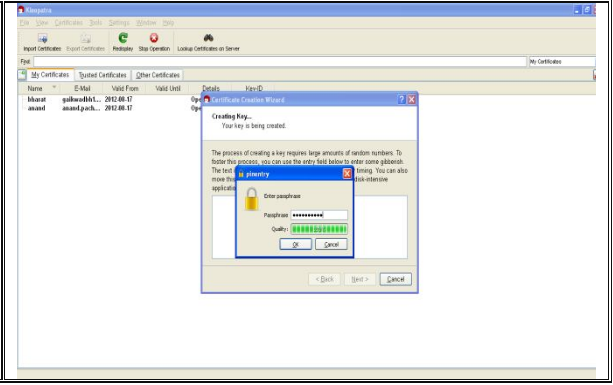
Development of tool for security this idea was given by Phil Zimmermann in 1991 Senate Bill 266 (a sweeping anti crime bill), some common of encryption methods to produce the software he named Pretty Good Privacy or PGP. The ideas behind (PGP) were known and understood by computer scientist and mathematicians for certain years, which means that the main concepts were not exactly innovation. The real innovation of Zimmermann was making these tools usable by anyone with a home computer. Even early version of (PGP) gave users with standard operating system based home computers access to military grade encryption in the USA [5].

Pretty Good Privacy is a computer program that provides cryptographic privacy and authentication. (PGP) is software which is used often for signing, encrypting and decrypting e-mails to increase the security of e-mail communication. To more specific it is a program that gives electronic mail something that does not have. It provides this by encrypting the mail so it cannot be readable by any other user, when the message is encrypted it is made to look like meaningless, and that the idea of (PGP) works. It has been proven that (PGP) is a very capable of resisting even the most sophisticated forms of analysis aimed at reading the encrypted text. (PGP) can be used to apply a digital signature to a message without encrypting. This is used in public posting where the message not needed to be hidden, but rather is needed to be allowed to the other users [9]. Once a digital signature is created, it is impossible for any to modify either the message or signature without the modification being detected by (PGP).

IV. EXPERIMENTAL ANALYSIS OF CRYPTOGRAPHIC PROCESS USING PGP

Experimental Analysis of Encryption-Decryption Process PGP users generate a key pair consisting of a private key and a public key; only you have access to your private key, but in order to correspond with other PGP users you need a copy of their public key and they need a copy of your private key to sign the email messages and file attachments you send to others and to decrypt the messages and files they send to you. The first thing you need to do before sending or receiving encrypted and signed email or files is create a new key pair. You generate a new key pair from PGP keys using the PGP Key Generation. The PGP keys window (Table No.I) displays the private and public key pairs you have created for yourself, as well as any public keys of other users that you have added to your public key ring. It is from this window that you will perform all future key management functions. The PGP Key Generation Wizard provides some introductory information on the screen. You can choose the type of key to generate, specify a key size, set an Enter your name in the Name box and your email address in the Email box. It is not absolutely necessary to enter your real name or even your email address. However, using your real name makes it easier for others to identify you as the owner of your public key. Also, by using your correct email address, you and others can take advantage of the plug-in feature that automatically looks up the appropriate key on your current keyring when you address mail to a particular recipient[8]. The PGP Key Generation Wizard asks you to enter a passphrase. In the Passphrase dialog box, enter the string of characters or words you want to use to maintain exclusive access to your private key. To confirm your entry, press the TAB key to advance to the next line, and then enter the same passphrase again. Even though your private key is protected by a passphrase that only you should know, it is possible that someone could discover your passphrase and then use your private key to decipher your email and files.

TABLE I. FLOW OF ENCRYPTION DECRYPTION USING PGP

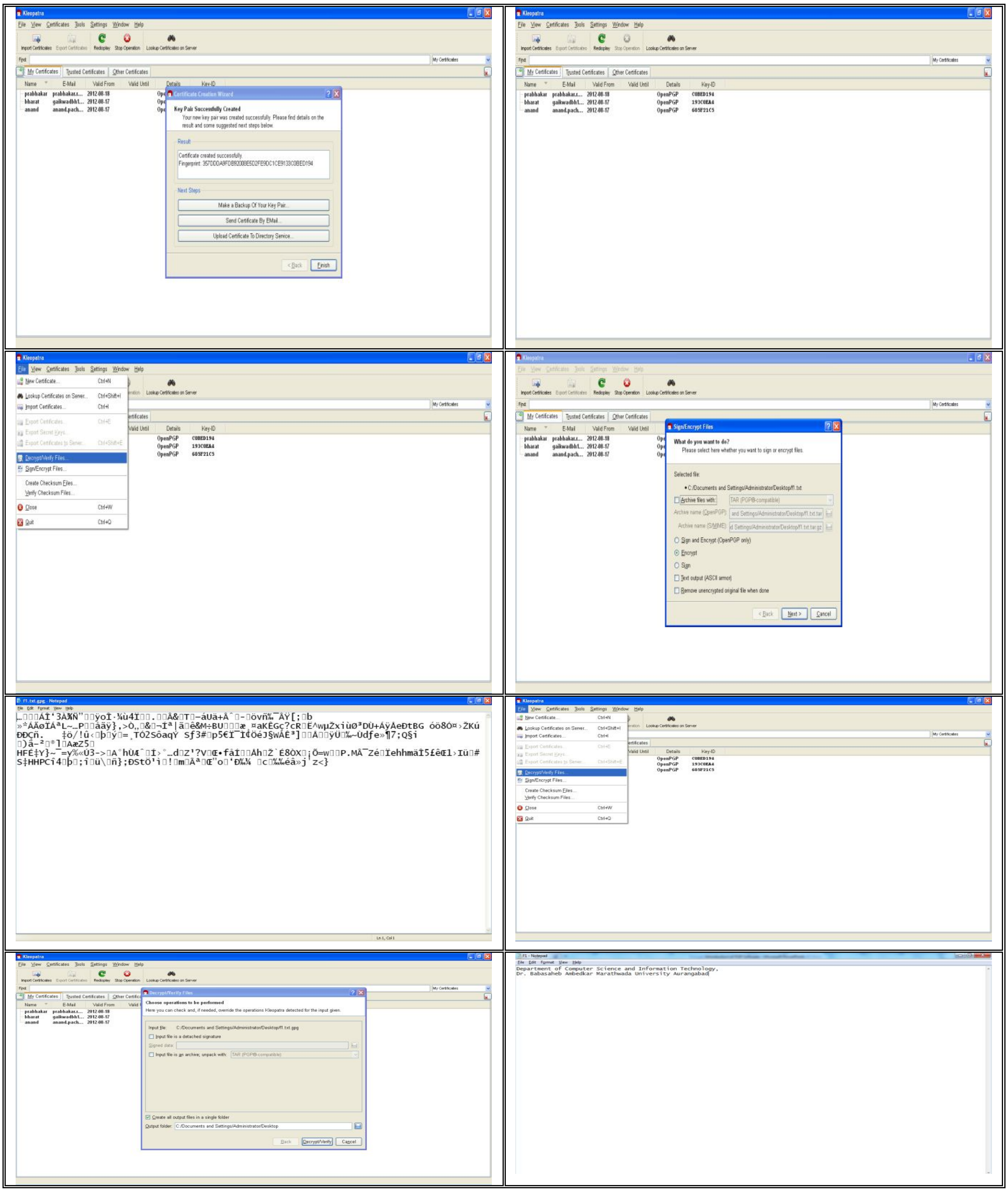
	 Department of Computer Science and Information Technology, Dr. Babasaheb Ambedkar Marathwada University Aurangabad
 Kleopatra File View Certificates Tools Settings Window Help New Certificate... Ctrl+N Lookup Certificates on Server... Ctrl+Shift+I Import Certificates... Ctrl+I Export Certificates... Ctrl+E Export Secret Keys... Export Certificates to Server... Ctrl+Shift+E Decrypt/Verify Files... Sign/Encrypt Files... Create Checksum Files... Verify Checksum Files... Close Ctrl+W Quit Ctrl+Q Lookup Certificates on Server My Certificates Valid Until Details Key-ID OpenPGP 193C0EA4 OpenPGP 605F21C3	 Kleopatra Import Certificates Export Certificates Redisplay Stop Operation Lookup Certificates on Server My Certificates Trusted Certificates Other Certificates Name E-Mail Valid From Valid Until Details Key-ID Certificate Creation Wizard &lt; Back Next &gt; Cancel bharat gaikwadbh1... 2012-08-17 anand anand.pach... 2012-08-17 **Choose Certificate Format** Please choose which type of certificate you want to create. ○ **Create a personal OpenPGP key pair** OpenPGP key pairs are created locally, and certified by your friends and acquaintances. There is no central certification authority; instead, every individual creates a personal Web Of Trust by certifying other user's key pairs with his own certificate. ○ **Create a personal X.509 key pair and certification request** X.509 key pairs are created locally, but certified centrally by a certification authority (CA). CAs can certify other CAs, creating a central, hierarchical chain of trust.
 Kleopatra Import Certificates Export Certificates Redisplay Stop Operation Lookup Certificates on Server My Certificates Trusted Certificates Other Certificates Name E-Mail Valid From Valid Until Details Key-ID Certificate Creation Wizard Advanced Settings... &lt; Back Next &gt; Cancel bharat gaikwadbh1... 2012-08-17 anand anand.pach... 2012-08-17 **Enter Details** Please enter your personal details below. If you want more control over the certificate parameters, click on the Advanced Settings button. Name: prabhakar (required) EMail: prabhakar.ranshur@gmail.com (required) Comment: (optional) prabhakar <prabhakar.ranshur@gmail.com>	 Kleopatra Import Certificates Export Certificates Redisplay Stop Operation Lookup Certificates on Server My Certificates Trusted Certificates Other Certificates Name E-Mail Valid From Valid Until Details Key-ID Certificate Creation Wizard pinentry OK Cancel &lt; Back Next &gt; Cancel bharat gaikwadbh1... 2012-08-17 anand anand.pach... 2012-08-17 **Creating Key...** Your key is being created. The process of creating a key requires large amounts of random numbers. To foster this process, you can use the entry field below to enter some gibberish. The text ... timing. You can also move this ... disk-intensive applicatio... Enter passphrase Passphrase •••••••••• Quality:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014



Name	E-Mail	Valid From	Valid Until	Details	Key-ID
prabhakar	prabhakar.r...	2012-08-18		OpenPGP	C0BED194
bharat	gaikwadbh1...	2012-08-17		OpenPGP	193C0EA4
anand	anand.pach...	2012-08-17		OpenPGP	605F21C5

Key Pair Successfully Created
Your new key pair was created successfully. Please find details on the result and some suggested next steps below.

Result
Certificate created successfully.
Fingerprint: 357DDDA9FDB92008E5D2FE9DC1CE9133C0BED194

Next Steps
Make a Backup Of Your Key Pair...
Send Certificate By EMail...
Upload Certificate To Directory Service...

< Back | Finish

Sign/Encrypt Files

What do you want to do?
Please select here whether you want to sign or encrypt files.

Selected file:
- C:/Documents and Settings/Administrator/Desktop/f1.txt

□ Archive files with: TAR (PGP®-compatible)
Archive name (OpenPGP): and Settings/Administrator/Desktop/f1.txt.tar
Archive name (S/MIME): d Settings/Administrator/Desktop/f1.txt.tar.gz
○ Sign and Encrypt (OpenPGP only)
● Encrypt
○ Sign
□ Text output (ASCII armor)
□ Remove unencrypted original file when done

< Back | Next > | Cancel

```
…□□□ÁÎ'3À¾Ñ"□□ÿoÎ·¼ù4Ï□□.□□Â&□T□–áUä+Âˆ□-□övñ‰¯ÂŸ[;□b
»*ÁÃøÏÁªL~…P□□åãÿ},>Ò„□&□¬Íª|ã□ê&M÷BU□□□æ¸¤aKÊGç?cR□Ë^wµŽxiùØ³DÙ+ÁÿÅeÐtBG óö8Ó¤›ŽKú
ÐÐÇñ.    ‡ö/!û‹□þ□ý□=¸TÓ2SôaqŸ Sƒ3#□p5€Ï¯Ì¢ÖéJ§WÅÊ³]□□Â□□ÿÜ□‰~Ùdƒe»¶7;Q§i
□)ã–²□®]□AæZ5□
HFÉ‡Y}~¯=y%«Ú3->□A˚hÙÆˆ□Í›˚…d□Z'?V□Œ•fåÏ□□Âh□Ž`É8ÒX□¡Õ=w□□P.MÂ¯Zé□Ïehhmäî5£êŒ1›Ïü□#
S‡HHPCî4□þ□;î□ü\□ñ};ÐStÖ'ì□!□m□Âª□Œ"o□'Ð‰¼ □c□‰‰éâ»j'z<}
```

Decrypt/Verify Files

Choose operations to be performed
Here you can check and, if needed, override the operations Kleopatra detected for the input given.

Input file: C:/Documents and Settings/Administrator/Desktop/f1.txt.gpg
□ Input file is a detached signature
Signed data:
□ Input file is an archive; unpack with: TAR (PGP®-compatible)

☑ Create all output files in a single folder
Output folder: C:/Documents and Settings/Administrator/Desktop

Back | Decrypt/Verify | Cancel

```
Department of Computer Science and Information Technology,
Dr. Babasaheb Ambedkar Marathwada University Aurangabad
```

V. CONCLUSION

In this paper, it is practical implementation of cryptographic techniques have been presented and analyzed in order to make encryption algorithms used in PGP .Pretty Good Privacy (PGP) is data encryption and decryption software that provides cryptographic privacy and authentication for data communication and also used for signing, encrypting and decrypting texts, e-mails, files. Pretty Good Privacy (PGP) perception can be applied to increase the level of security for a digital file. With the security enhancement, intruders will have to deal with more obstacles in order to obtain the files content. The security program does not set up an exact port number between client and server due to the reason that this action can also be an additional obstruction for intruders when trying to gain access with the communication.

REFERENCES

1. Ramaraj, E., and Karthikeyan, S.: A New Type of Network Security Protocol Using Hybrid Encryption in Virtual Private Networking. Journal of Computer Science 2(9) (2006)
2. Kamarudin Shafinah, Mohammad Mohd Ikram, “File Security based on Pretty Good Privacy (PGP) Concept”, Computer and Information Science, Vol. 4, No. 4; July 2011
3. Natasa Prohic, “Public Key Infrastructures – PGP vs. X.509”, INFOTECH Seminar Advanced Communication Services (ACS), 2005
4. “An Introduction to Cryptography”, PGP*, Version 7.0, United States of America.
5. http://cgi.csc.liv.ac.uk/~dominik/teaching/comp516/_downloads/PGP_essay_3.pdf.
6. Ahmad Abusukhon, Mohamad Talib , Issa Ottoum , “Secure Network Communication Based on Text-to-Image Encryption”, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(4): 263-271
7. PGP Freeware for Windows 95, Windows 98, Windows NT, Windows 2000 & Windows Millennium, “User’s Guide Version 7.0”, Copyright © 1990-2001 Network Associates.
8. http://GPG4win.com.
9. National Bureau of Standards, “Data Encryption Standard,” FIPS Publication 46, 1977.
10. Gurjeevan Singh, Ashwani Kumar Singla,K.S. Sandha, ”Through Put Analysis Of Various Encryption Algorithms”, IJCST Vol. 2, Issue 3, September 2011.

BIOGRAPHY

Mr. Bharatratna Pralhadrao Gaikwad

Completed M.Sc., Pursuing Ph. D. in Computer Science from University Department of Computer Science and Information Technology, Dr. Babasaheb Ambedkar Marathwada University Aurangabad. Paper published in IEEE Xplore, Springer, IJCA, CIIT and Area of specialization in Network Security, Video Processing, Cyber Law, E- Commerce, and Pattern Recognition. Member of IEEE, Life Member of ISCA, ICSA, IAENG, IACSIT