Extended Pretty Good Privacy

Kalpesh Khetade[1] Vikas Sable[2] Meghana Sail[3] Prof. Sandeep Chavan[4]
[1,2,3]Student [4]Assistant Professor
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]BharatiVidyapeeth College of Engineering, Navi Mumbai-400614

Abstract— Pretty Good Privacy (PGP) is a system which is used for the purpose of secure e-mails and messages communication over open network. PGP is important to implement secure and efficiency of e-mail messages, it is a security tool which enables the users to secure their damaging information, ands sensitive data by making their stored documents and e-mails safe and secured. Cryptography is used 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. Cryptography in digital world offers three core areas that protect data from attempt to be taken, taking or an unauthorized use of data. Cryptography covers these essential areas: Authentication, Confidentiality, integrity.

Key words: PGP, PEM, Cryptography

I. INTRODUCTION

Users who rely on electronic mail for business or personal communications should beware. Messages sent over a network are subject to eaves dropping. If the messages are stored in a file, they are subject to perusal months or even years later. There is also the threat of impersonation and that a message may not be from the party it claims to be from. Protection is available in the form of Pretty Good Privacy (PGP), an E-mail security package developed by Phil Zimmermann that combines confidentiality and digital signature capabilities to provide a powerful, virtually unbreakable, and easy-to-use package.

Personalization of the learning content, based on learners' preferences, educational background and experience

With the explosively growing reliance on electronic mail for every conceivable purpose, there grows a demand for authentication and confidentiality services. Two schemes stand out as approaches that enjoy widespread use: Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extension (S/MIME). The latter is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data Security. Although both PGP and S/MIME are on an IETF standards track, it appears likely that S/MIME will emerge as the industry standard for commercial and organizational use, while PGP will remain the choice for personal e-mail security for many users. In this course we will only be looking at PGP.

A. Overview:

Pretty Good Privacy (PGP) is a best program used to encrypt and decrypt e-mail securely and transmit over the Internet. It can also be used to generate and send a encrypted digital signature that used to receiver for verify the sender's identity and know that the message was not changed and send by the authenticated user or people. An PGP can be available freeware as well as low-cost commercial version, PGP is the most widely used for maintaining a privacy of our data by individuals and is also used by many corporations agency. In 1991 PGP was developed by Philip R. Zimmermann, PGP has become a genuine standard for e-mail security. PGP can also be used to encrypt files, data being stored in your system or drive so that they are unreadable by other users and provide the hidden security from unauthorized people.

B. Problem Statement:

When a person sends an email that email consist of plain text that is normal English language Sometimes it is so important to send valuable data through the email No one guarantees that it will land safely into the receivers inbox The email is in plain text so if hacker hacks the email account then he can able to read that email And attacker would be able to send email to people who is in the persons account and able to misuse the account If a client wants to send a confidential data and attachments to his boss, which is very important and crucial that has to send via an email because the boss is in other location ,then there is no guarantee of the data will land safely - certain situations can occur like:

- Hacker hacks the clients account
- Hacker modify the email message and send to boss
- The boss will not trust that the email has come from real client Or email consist of actual data

Another example: - A client wants to send crucial data about his case to the lawyer and client is in different country. Email is necessity of today's world. So we have to use email technology there is no other faster way to send or receive the data. So we will try to develop a software project that will reduce the hacking problems and guarantees the user that the data of email is trustworthy.

C. Objectives:

The main objective of this project work is to achieve

- Confidentiality refers to prohibiting the revelation of information to unauthorized people for individuals or systems.
- Data should reach the other end as it is. It should not be modified by attacker. But in case it is modified, receiver understands that it is modified. This means that data cannot be modified by unauthorised people in an unauthorized or undetected manner.

– Authentication it is necessary to ensure that the data are genuine. It is also important that both authorised party is validated who's claim to be.

II. REVIEW OF EXISTING SYSTEM

A. Privacy Enhanced Mail:

Privacy-Enhanced Mail (PEM) is an totally based on Internet standard that provides for securely exchange of e-mail between senders and the receivers. PEM used cryptographic techniques to allow for confidentiality, sender authentication, and message integrity. The integrity of message aspects allow the user to known that a message hasn't been modified during transmission time from the sender. The authentication of sender allows a user to verify that the Privacy-Enhanced Mail message received by us is send by the truly authenticate person who claims to have sent it. The features of confidentiality permit to a message to be preserved secret from the people whom they are not authenticate.

B. Drawbacks:

In existing System

- Encryption and decryption is possible.
- Data cannot be secure.
- Data can be altered
- Senders Authentication is not Achieves, receiver don't know whether message come from true sender

C. Pretty Good Privacy:

Pretty Good Privacy (PGP) is a technique that encryption and decryption data in computer program that provides cryptographic privacy and authentication security for data communication and sharing files. PGP is also used for signing, encrypting, and decrypting texts and image file, e-mails, files, directories, and whole disk partitions to provide the safety and growth the security of e-mail communications. It was developed by Phil Zimmermann in 1991. It is best opportunity to you that you can electronically sign your email: naturally or cardinally, PGP will calculate a complicated mathematical value called a hash value. That hash value exactly based on the actual data of your email message, and will then encrypt that value to your private key. The receiver of your email will use their PGP software to automatically make the same calculation - if the calculations match with the senders hash value, the receiver's software automatically will use your public key to decrypt your encrypted hash function, and that hash value is the proof for the message or file has not been change in any way.

III. PRESENT INVESTIGATION

A. Proposed System:

We develop software that will encrypt as well as decrypt data .In addition to provide Authenticity, Integrity and Non - repudiation to document, we will develop digital signature we will achieve

- Authentication
- Privacy/confidentiality
- Integrity

This project has proposed a PGP-based cyber-security for DNP3 to streng then power system computer network security. With increased network access due to modernization and automation of power systems, cyber-attackers have more avenues of attack available to assume control over power system operations, potentially causing serious wide-scale blackouts.

Security has become a critical issue for the commonly used DNP3 protocol for power system communications. The proposed PGP-based cyber-security provides authentication technique using public key cryptography, with better security performance using symmetric keys algorithm technique for most of the encryption technique.

This project has described a symmetric cipher key exchange mechanism to further enhance the efficiency of the proposed cyber-security. The proposed cyber-security based on PGP is implemented as an artificial layer on below the DNP3 data-link layer to use for minimizes any impact on the DNP3 specification and the operations of original DNP3 devices.

Otherwise, the power system communication network interoperability would be risked. Also the cyber-security must be interoperable with devices that do not use cyber-security. The PGP-based cyber-security implemented below the data link layer provides effective cyber-security through exchanging symmetric cipher keys for the symmetric-cipher only cyber-security.

The symmetric cipher keys are only valid until the PGP-based cyber-security replaces them, limiting the security risks involved with only using symmetric ciphers. The PGP-based cyber security replacement rate for the symmetric cipher keys is dependent on the parameter settings as determined by the control centres.

This PGP-based cyber security system provides to us, of a confidentiality, identity authentication, transmission content authentication, and non-repudiation.

B. How to PGP Encryption & Decryption Work:

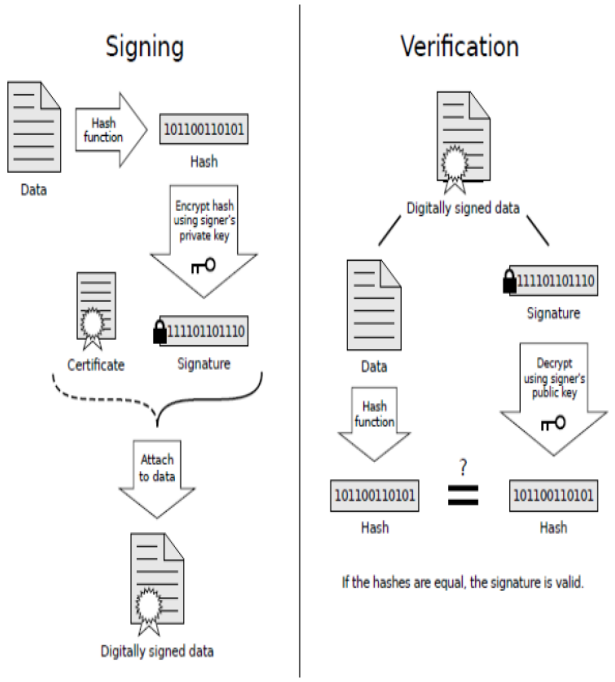

Fig. 1: PGP Encryption & Decryption Work

C. System Architecture:

1) At Sender Side:

a) Login:

– User enters username and password.
– If username and password match then user is valid, user can proceed further Otherwise user is not valid, user not allow to proceed further.

b) Encryption:

– Definition: Encryption is the process of encoding the message or file with the help of encryption mechanism or technique in such a way that only authorized party can read the message.
– That encrypted file can read only after the Decryption.
– Sender Encrypt the message

c) Digital Signature:

– Definition: A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message
– Hash value is generate

d) Digital Certificate:

– A Digital Certificate is like passport that allows user to exchange the information or file by electronically. It can bind the public key with identity information such name address, and all other information like serial number, subject, issuer, valid-form, valid-to, key-usage. etc which is cheque and generated by the Legal agency.

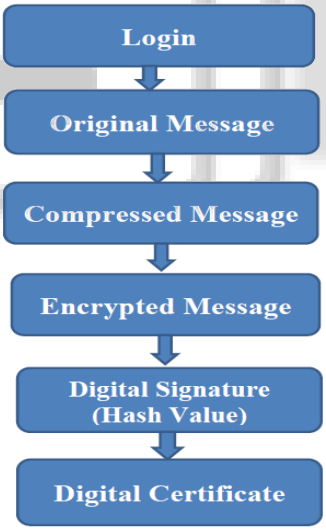

Fig. 2: System Architecture: At Sender Side

2) At Receiver Side:

a) Signature Authentication:

In that it check the hash value of signature of received Certificate, if hash value of signature is matches, then data is not modified, otherwise Data is Modified

b) Certificate Authentication:

In the (more recent) Open PGP specification, trusted user signatures can be used to prove certificate authorities. A trust signature can be indicates that the key belongs to its claimed (authorized) owner and also the owner of the key is reliable to another keys can sign at one level below their own. A level 0 sign is correspondent to a web of trust sign since only the keys validity is certified. A level 1 sign is similar to the legal one has in a certificate authority because a key signed to level 1 is able to issue an unlimited number of level 0 signatures. A level 2 sign is highly similar to the trust assumption users must have confidence on whenever they can use the certificate authority list which is can be default; it permit the owner of the key can be generate other keys certificate authorities.

c) Decryption:

Decryption is the Process of converting the encoded or encrypted text or other data which is send by sender in such way that it back into original text that you or the computer are able to read and understand. so that means it can be read only by authorized person who has the right encryption key to decrypt it.

Fig. 3: System Architecture: At Receiver Side

IV. SYSTEM DESIGN

A. PGP Set Up:

To set up PGP you need to download Gnu PG and install Enigmail, which is a plugin for Thunder bird. You then have to create keys and upload the public key to a key server. For Mac these operations can be done in GPG Keychain Access (which comes with GnuGP), while on Windows you have to do this through the command window (can also be done through the terminal on Mac if you prefer to do it that way). In our case we used the MIT key server. From this site you can also download public keys belonging to other users. You can then sign and encrypt email for sending. When you download a key, you have the ability to sign it. By doing so you verify that you trust the owner of the key, and that people who trust you also should trust this person. This is called the "Web of Trust". If you receive a message from an untrusted sender, you can choose to start trusting the sender by signing his key. If doing so, you should be sure that the sender is the one you think.

(a) Encryption and signing symbols (b) PGP security info

Fig. 4: PGP Set Up

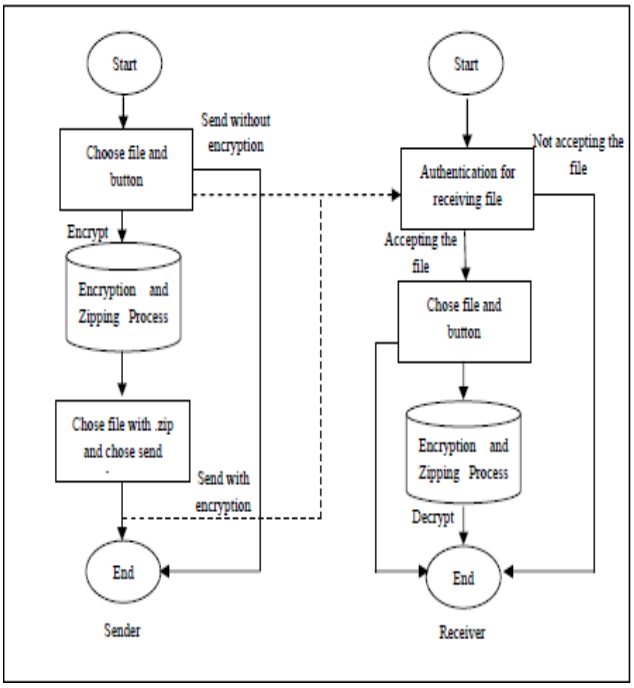

Fig. 5: Working of Sender & Receiver side PGP

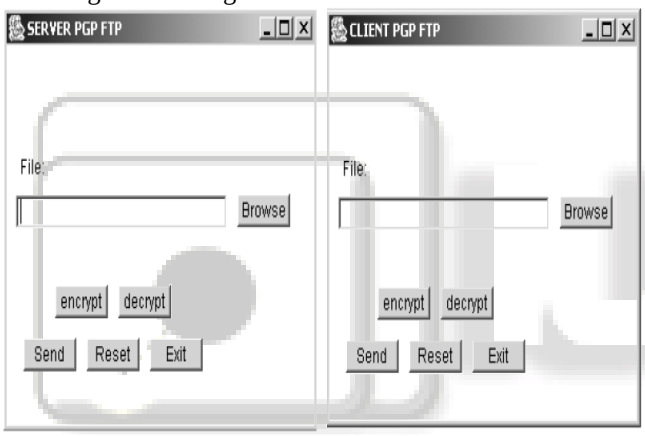

Fig. 6: The Interface for Client and Server

B. Keys and fingerprints:

PGP gives you a choice of creating RSA and DSA keys with the size ranging from 512 to 4096bits. In our case we mainly used keys of the length 2048 bits or 4096 bits. A reason for choosing the 2048 bits key over the4096 bits one is the running time of the program during the key generation. And the fact that the 2048 bits key is the recommended key length and is said to be secure enough.

Every time you run PGP a different session key is generated.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.0

mQENBFC8+DsBCADwwGGlvkJULcvzlVk5spYQiRiVerD0L+czJjF9WLrFTpNe+Tlyq+rh8zul
6a53nz5uWeiQ2v4fUFyJNPcUHOcZFtv5XiO4uzjJ1CLiUwWdNo8G1FMx+YTRizmwSteqGX91
wWTsWOSKh3DBv48L6LChw6AluzIc4uqkisMllx51rGPiSOWz6Bi4CxVYHPKt8F6HKJwipHgV
tdZ1CROt1h0DZe4xfFCBNhj+ZWGBwCZGK8Jkn2siYc/WfqPy8QkgwqROIpMREUksoOcQGQFj
Q/uwm8FpmrE5xtEmbDktLuQvePlgLy438VL+5g+kpynaJZYnSRFEhQmoRaHPE1HtbKgFABEB
AAG0Kkhhbm5lIFJpaXNlIE1hZWhsdW0gPGhhbm5lX3JtQGhvdG1haWwuY29tPokBOAQTAQIA
IgUCULz4OwIbDwYLCQgHAwIGFQgCCQoLBBYCAwECHgECF4AACgkQ3jtTlNdn7gi9bAf+PfjC
BDr9TXBuwAcfYC7XENpDJIOyR9PLHx3vmYoU4lyzwqUS8BZs8hx6owgmLhug4bJ2tPo+Ihlw
02bO7NJ0dj43yfSzXJfViLT5ItKSQmkiTEqw8U8bxvK+IT+VuJHKrAIULlCUUTyPOy7G6HhY
zdi9eCr8TlYFXuGEIhHJyByqYqnVM0Vz0STnsc4VrEv6bo6275nHJbYIe/4Ri4mFD2J+t6BW
zVudGKPHg42lEZyv4KqpPxCyEEGaP1/+qvPwUCqvaSXZ2LnnYpP+ku08TSKtdKMVBhOLks0O
BcRtVdzJehUejoksjnB0aezylI0bI9XBimVskysNxTdC2TKtMA==
=OC7w
-----END PGP PUBLIC KEY BLOCK-----
```

Fig. 7(a): A newly created Key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.0

mQENBFC8+DsBCADwwGGlvkJULcvzlVk5spYQiRiVerD0L+czJjF9WLrFTpNe+Tlyq+rh8zul
6a53nz5uWeiQ2v4fUFyJNPcUHOcZFtv5XiO4uzjJ1CLiUwWdNo8G1FMx+YTRizmwSteqGX91
wWTsWOSKh3DBv48L6LChw6AluzIc4uqkisMllx51rGPiSOWz6Bi4CxVYHPKt8F6HKJwipHgV
tdZ1CROt1h0DZe4xfFCBNhj+ZWGBwCZGK8Jkn2siYc/WfqPy8QkgwqROIpMREUksoOcQGQFj
Q/uwm8FpmrE5xtEmbDktLuQvePlgLy438VL+5g+kpynaJZYnSRFEhQmoRaHPE1HtbKgFABEB
AAG0Kkhhbm5lIFJpaXNlIE1hZWhsdW0gPGhhbm5lX3JtQGhvdG1haWwuY29tPokBOAQTAQIA
IgUCULz4OwIbDwYLCQgHAwIGFQgCCQoLBBYCAwECHgECF4AACgkQ3jtTlNdn7gi9bAf+PfjC
BDr9TXBuwAcfYC7XENpDJIOyR9PLHx3vmYoU4lyzwqUS8BZs8hx6owgmLhug4bJ2tPo+Ihlw
02bO7NJ0dj43yfSzXJfViLT5ItKSQmkiTEqw8U8bxvK+IT+VuJHKrAIULlCUUTyPOy7G6HhY
zdi9eCr8TlYFXuGEIhHJyByqYqnVM0Vz0STnsc4VrEv6bo6275nHJbYIe/4Ri4mFD2J+t6BW
zVudGKPHg42lEZyv4KqpPxCyEEGaP1/+qvPwUCqvaSXZ2LnnYpP+ku08TSKtdKMVBhOLks0O
BcRtVdzJehUejoksjnB0aezylI0bI9XBimVskysNxTdC2TKtMIkCHAQQAQIABgUCUL0HXwAK
CRA0ZsGJ50efo5iiEACPSUMgxSV14f40j8ehLMQQK3bV46yG6sEShXXtE8eiCEA1U96DPhJJ
zJ7Zd4fMqIO98o38YaN+DknQ9+qHlzKFztCh8eGeSroEE1yVAmjWjyZHopoPssrCCC0x+I7T
JGzR1dV1mDACQ2cJTrvMGvNfc+bgv49gkBo25IJK7MbDzp67HU6eZPTbK3j43HW83Gs6ECJa
2o+b8KInqEA/Eia9OpFWyT1OCsyFO8P8oHHPpdwLLY9tS8/2HYrQQdFnEpEQ6XUCTY9j67CK
GmzeQAygeQ5S3WeRwJEUeuzEwJnack+tyGA+CSCAGFxTW8LyQ6r48qkmSmqGEQIBAbH/IYbx
gBTJRqv0fz3E3cgsNWvCvR36O7okj77bDfONG+IPu59RrDgjpZft7qAMKK8nKhzt/yUd00xn
qUeuxgUpwQYC6og0cBblONFdKuwm+shJ11CcTcEst3S9afFwWFtSD6mBHmS0RKs+uw/RWpcF
98i1TSUJk4ZbZYxyEjP3ucbEb5ZhNFSgZJ9XRKdA7Ty0LJ9urVtlXYofVPeOeYnyvHqM44Ut
+Cs042RglWdibaDULFOv911Ong/HeKtShkJoQe0MwWLW95f9OqrV2AzYHbg+Q9qdUyTUYCYz
8dM1/mSh5MYiuXtoJ+T0FVCYHea1OJPs8n661xihEmjkWryvAWZBNQ==
=a0jE
-----END PGP PUBLIC KEY BLOCK-----
```

Fig. 7(b): Key signed once

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.0

mQENBFC85BQBCAC2bUVhc3HorzsqHdJb1/kbfFYPe6XpCkMskQu/GVnpI9HkSPsRJ/XeEAq2
M6QDaH04MNFKPC0+DP62kxUwcVov1tC3493ayWnLxgNxTVKzcus0TCzLlaGvq66qCF8x9rcN
3acGb8qAS1mHnDKTlzKqaXuQwokJDMHOgmmSM/AME6GoBPnG4Ki638SSePvLLdCIn0uWxRED
yFjWMLZCeFik6TlIaZLBvbP02JhUfmANNa+aY06m6G5cnY/nqi4HUI0gN5bwEHcYLRznlVBG
dnqSER4sFJaCsjsCc1G3CXIx9VnoKOEaYyazsi6M3ukGjoVXzr2KPqIwEFX2MdP6pIXnABEB
AAG0KkFubGF1zyBVbmRlcmRhbCA8YW5sYXVndW5kZXJkYWxAZ21haWwuY29tPokBPwQTAQIA
KQUCULzkFAIbLwUJB4YfgAcLCQgHAwIBBhUIAgkKCwQWAgMBAh4BAheAAAoJENtuIE3Z6MPI
Zf0H/0QEZWE+IMDN9/pSPQQtdU/R+Wklcu+WfkqBbKvEI/GKndwk3JWKwySpL5yA3jJJUogq
CPAiczrlD9juVgxoF0OHUWUNH9k5CnpKS6W8smA8ejfPl5bm+5wJkBPvKLva7y6I/Nf6snoE
3pgQQeDB2gf4CkQWF4cvRkftAWcPyVp0nJrYRjTt15/I3zISy6UGVUDb9xWLbSc5nHZ9LFPo
eKz/Gzol0IV7sO6ZCji1Og/JNJBBhaexLKy75k4KzJJuH5otfQp25hbqDsWrBLDhRJEE83Hq
ODacac+H1J4AVaYQdYjEBg0O9TX3aka4DUF7TXjUqwlZmuP6wk/PlnFNIna5AQ0EULzkFAEI
ANJzqr4P5bFDdeRqTjy+YxEA/DPi4UY5X3KT4KeyW671gLGof1KoOsJ2YwWYBCgYDKNGvXjn
C6rn1Qbg2yEWcyFcB7gwG2WbkAIx+8Qr9p4kH1vW74l0V9NvVR6GLXLNv6Lgv2LnFk9FTO2C
Jjw5tlQdz36Y9euRsTzGQSHcot+FPC5xJCCjXBQ59vkejYybnOVm0YZzrsk0isBCluCr4QZG
9LwHMChlkRJYGMMqqPqYQWcjZSMTqDR+cOWF0X/PjItgS0uhrJsZ+XhD4FJKT8LlDxJFRTrE
TnhWphoMPwcu2Jb7iNztiDeEwKCY9YDLWyy6lvnAXUaWzxZVG52vxxcAEQEAAYkCRAQYAQIA
DwUCULzkFAIbLgUJB4YfgAEpCRDbbiBN2ejDyMBdIAQZAQIABgUCULzkFAAKCRDSHGN+t+bf
iRumB/98XrMSjBvprs7FsHaSIK3Q5Udozvj85Zd+FK/TlCBaOPXwZDoaYlqjX++WJRv4BYfn
S5tNUqWokHW4f9CGAPPXHHfaC5aOhA14NVxFRqeBo1SRp5Qi/9OKP82UOM1SpXnEaFwggb/A
jBi7wEXFkBtURyUi4YuHmsk21jRAYg7ocFNowbzq43jobYMMR+u5hydsGKCXhNECoLQ/zVhg
tBvMiNkW9cWiJEjYb5FbdWYH7j+oSf9aHIaW9z5umqnVusupNaHbOIfiS87hcAypSdD3iIR8
Hx1rBU9xE3Ac93LyEJ0TeMT1NUMuwK4zQyrHavy2qIChv+ts4ZqbjCrRy0Zl1l8IAKnsw899
QTeZRli1kZch074qqPaWOpLnwP1ZwQ2TIGdf5eiBA+EqGO5Pz5CnuLudXhozKEHB3Xp5O3sP
QUD4J1S3v60puCXivrtC3+jljGpHYz7nKv2pgHrkkUZZ1t8O4dgOg5sBz4Yeh+p7zLe9VRhX
migDv6ytGtscQwoiA7C3WpEykgc5OYgWagSTZbxmzWV8fTCPXjJWTOmf0jC3vLR0UVAFQ/gG
awpaDGAbW1iE8c8rDWY3O1BOhSUqUGF9dz5SSx0jqwXNadHxg9B8yZQ1QwNDk6dLiwK0MBO4
vCBmvHa+LCACc1vUx919568tCUo2Oh8jyO1meLO+fZ4p/+g=
=RVXs
-----END PGP PUBLIC KEY BLOCK-----
```

Fig. 7(c): Key signed twice

In figure a,b,c you can see three different examples of the same key block. In figure (a) the key is newly created and not signed by anyone. In (b) the key has been signed once and in (c) the key has been signed twice. As you can see, the key block is expanding with the number of signatures. This is due to the fact that information about the signers of the key are stored with the key block. Fingerprinting is deployed to verify the ownership of a key. You can distribute your key through different channels. You can post your fingerprint on your web page, in person or other channels you consider secure. This makes it easier for other to authenticate you.

V. FEATURES

- The combination of these two encryption methods combines the convenience of publickey encryption with the speed of conventional encryption.
- Using Conventional encryption is about 100 to 1,000 times faster than public-key encryption, which solves

the problem of slow encryption with asymmetric algorithms.

- Public-key encryption technique provides a proper solution to key sorting and data transmission issues when using symmetric key encryption.
- When used together, performance and key sorting are improved without any loss in security.
- PGP is good hybrid solution; it ties together the advantages of public key and symmetric cryptography, while also providing a feasible solution to the disadvantages of both. .

VI. CONCLUSION

Pretty Good Privacy is a much closure to public key encryption program. In fact, it is the genuine standard among public key encryption schemes for both services like microcomputers and mainframes. It provides confidentiality for e-mail and stored files, using a private/public key pair, along with sender authentication and data integrity, using digital signatures and digital certificate .It is used provide a privacy to the people, for protect our file and data .

VII. ACKNOWLEDGMENT

No project is ever complete without the guidance of those expert how have already traded this past before and hence become master of it and as a result, our leader. So we would like to take this opportunity to take all those individuals how have helped us in visualizing this project.

We express our deep gratitude to our project guide Prof. Sandeep Chavan for providing timely assistant to our query and guidance that she gave owing to her experience in this field for past many year. She had indeed been a lighthouse for us in this journey.

We would also take this opportunity to thank our project co-ordinate Mr. Rahul Patil for his guidance in selecting this project and also for providing us all this details on proper presentation of this project.

We extend our sincerity appreciation to all our Professor form Collage of Engineering for their valuable inside and tip during the designing of the project. Their contributions have been valuable in so many ways that we find it difficult to acknowledge of them individual.

We also great full to our HOD Mr. Ingle for extending her help directly and indirectly through various channel in our project work.

REFERENCES

[1] "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendation," U.S.-Canada Power System Outage Task Force, April 2004.
[2] "The World Market for Substation Automation and Integration Programs in Electric Utilities: 2005-2007 Executive Summary North American Market," Newton-Evans Research Company, September 2005.
[3] RFC 4346: The TLS Protocol Version 1.1, Internet Engineering Task Force (IETF), April 2004.
[4] DNP3 Specification Volume 7: IP Networking, DNP User's Group, December 2004.
[5] DNP3 Specification Volume 2: Application Layer, DNP User's Group, October 2005.
[6] RFC 1991: PGP Message Exchange Formats, Internet Engineering Task Force (IETF), August 1996.
[7] P. R. Zimmermann, The Official PGP User's Guide, Cambridge: The MIT Press, 1997.
[8] F. Cleveland, "IEC TC57 Security Standards for the Power System's Information Infrastructure-Beyond Simple Encryption", IEC TC57 WG15 Security Standard, October 2005.
[9] DNP3 Specification Volume 3: Transport Function, DNP User's Group, November 2002.

