

PGP Encryption Software

Shuhan Wang

Technology, Communication and Transport
Degree Programme in Information Technology

2014

Technology, Communication and
Transport
Degree Programme in Information
Technology

Author	Shuhan Wang	Year	2014
Supervisor	Jouko Teeriaho		
Commissioned by			
Title of thesis	PGP Encryption Software		
No. of pages + app.	53		

The PGP encryption software is considered as the most powerful and effective software to protect the confidentiality of the email. The goal of this thesis was to render the reader an overview of what the PGP software is, what cryptographic there are behind the PGP software, how the PGP software works and how it can be installed.

In the theoretical part, the basic cryptographic terminologies and concepts were explained to help the understanding of the PGP working principles. In the middle part the PGP's functions were explained in detail. They included how the authentication of the communicating parties is implemented, how the keys are managed and delivered, how the messages and the data are encrypted. The last section included the installation instructions with the screenshots and the user guide about the main icons in the user interface.

Today, even the company such as Google has to provide the back door for the government, the PGP software is still unreachable for the government to monitor the citizens' communication. Thus, having a strong understanding of PGP is useful for the users to protect personal privacy.

Key words cryptography, encryption, decryption, security

CONTENTS

1	INTRODUCTION	7
2	DEVELOPMENT OF PGP	8
3	BASIC TERMINOLOGY	10
3.1	Key.....	10
3.2	Plaintext and Ciphertext.....	10
3.3	Cryptanalysis	11
4	BASIC THEORY OF CRYPTOGRAPHY	12
4.1	Encryption and Decryption.....	12
4.2	Symmetric Encryption	12
4.3	Asymmetric Encryption	13
4.4	Key Space	14
5	HYBRID ENCRYPTION SYSTEM.....	16
5.1	Authentication of Hybrid Encryption System	16
5.2	Encryption and Decryption of Message	16
6	BLOCK CIPHER	18
6.1	Definition of Block Cipher.....	18
6.2	How Does Block Cipher Work.....	18
7	HASH FUNCTION	20
7.1	Definition.....	20
7.2	Hash Function in PGP	21
8	DIGITAL SIGNATURE	22
8.1	Digital Signature	22
8.2	Digital Signature in PGP	23
9	KEY DISTRIBUTION	25
9.1	Keyserver.....	25
10	CERTIFICATE	27
10.1	Digital Certificate	27
10.2	Certificate Authority and Revocation Certificate	29
11	CERTIFICATE FORMAT	31
11.1	PGP Certificates	31
11.2	X.509 Certificates	32
12	WEB OF TRUST.....	35

12.1	Origin of Web of Trust	35
12.2	Application of Web of Trust.....	35
12.3	Weakness of Web of Trust	36
13	CONFIDENTIALITY OF PGP	38
13.1	Encryption and Decryption of PGP	39
14	SIGN A KEY	41
14.1	Prerequisites for Signing Other's Key.....	41
14.2	Sign for Familiar People and Strangers.....	42
15	INSTALLATION	43
15.1	System Requirement for Installation.....	43
15.2	Download Archive Package.....	44
15.3	User Guide	46
16	CONCLUSIONS	50
	BIBLIOGRAPHY	51

LIST OF FIGURES

Figure 1. Key, Plaintext and Ciphertext (Heitmeyer 2011)	11
Figure 2. Encryption and Decryption (Keyoung Information Ltd. 2014).....	12
Figure 3. Symmetric Encryption (Thakor 2013).....	13
Figure 4. Asymmetric Encryption (Blurrent 2014)	14
Figure 5. Block Cipher Encryption (McCombe 2007)	19
Figure 6. Hash Function (Wikimedia Foundation, Inc. 2014c)	20
Figure 7. Digital Signature in PGP (PGPi 1999).....	21
Figure 8. Digital Signature (Kelly & McKenzie 2002)	22
Figure 9. Digital Signature in PGP (PGPi 1999).....	24
Figure 10. PGP Keyserver (Symantec Desktop Email Encryption, 2014)	26
Figure 11. Digital Certificate (PGPi 1999)	29
Figure 12. PGP Certificate (PGPi 1999)	32
Figure 13. X.509 Certificate (PGPi 1999).....	34
Figure 14. Encryption and Decryption of PGP (Wikimedia Foundation, Inc. 2014a)	40
Figure 15. Symantec Desktop Email Encryption Trialware (Symantec Desktop Email Encryption, 2014).....	44
Figure 16. Register for SymAccount (Symantec Desktop Email Encryption, 2014)	45
Figure 17. Available Versions of Symantec Encryption Desktop (Symantec Desktop Email Encryption, 2014).....	45
Figure 18. Acquire the Activation Code (Symantec Desktop Email Encryption, 2014).....	46
Figure 19. PGP Desktop Interface (Symantec Desktop Email Encryption, 2014)	48

SYMBOLS AND ABBREVIATIONS

AES	Advanced Encryption Standard
CA	Certificate Authority
HD Space	Hard Disk Space
PGP	Pretty Good Privacy
RAM	Random Access Memory

1 INTRODUCTION

In the information and networking era the Internet plays an increasingly important role at work and in the daily life. More and more users acquire and process information via the Internet. However, as an open system for the general public the Internet results in the security problems. While being transmitted, the information in emails may be accessed by the outsiders and lose confidentiality. In consequence, the issue how to protect the confidentiality of email has become vitally important.

In the past, people considered to use the scanning of the handwritten signature into the email to prove its authenticity. Email was readable for all who could capture the message. One tool to solve the email security problem is PGP, an email encryption software, which can provide confidentiality of the email by preventing unauthorized persons from reading it. Furthermore, PGP uses a digital signature at the end of the message so that the recipient can confirm the identity of the sender of the message, and to ensure that the message is not changed.

In this thesis, the theory and the technology behind this encryption tool are explored to help the reader to understand the functions of PGP. In the beginning of the thesis the basic concepts of cryptography are explained. After that a specific description of the PGP encryption system and the features are provided to deepen the understanding. The last part of the thesis describes the detailed steps of installing the PGP desktop software, and it contains some instructions to the new users.

2 DEVELOPMENT OF PGP

Dating back to 1991, for controlling the potential criminals, the American government tended to set up a Senate Bill 266, in which the communication companies were coerced to provide the government with an accessible back door to monitor the citizen's communication. Due to the unfair bill, Phil Zimmermann was promoted to produce the encryption software called Pretty Good Privacy or PGP, which integrated various encryption methods. Ultimately, the bill was rejected, but the PGP Encryption Software was auspiciously released. (Lucas 2006, 3.)

In fact, the encryption methods of the early PGP software have existed for a long period of time. The uniqueness of the PGP software is that it is available to anyone who owns a computer. At that time, PGP was in the same level of the military encryption software. The major difference between the military encryption software and PGP was that PGP was accessible for civilians, while the military encryption software is only available for the military. (Lucas 2006, 3.)

In addition, for PGP in the early time, there are no authorization and fees required for non-commercial purposes. In the early released versions, the source code is completely free of charge. The first version of the PGP software contained a symmetric key algorithm designed by Phil Zimmermann. The second version, that gradually replaced the first version, became the stand version in early 90's. (Wikimedia Foundation, Inc. 2014a.)

However, because people were worldwide using PGP, the American government treated the wide exported encryption software as a national security issues, and the American government defined PGP as a "weapon". Finally, the American government accused Zimmermann for "exporting weapons". In fact, the charge was merely an excuse for the American government to control civil communication. Fortunately, from the aspect of law, there are no restrictions on exporting papers or files, which means it is legal to export the code of PGP in handwriting. Ultimately, the accusation on Zimmermann was withdrawn and he published his

code in book. In the following years, the PGP version 5 was released as well.
(Lucas 2006, 3.)

3 BASIC TERMINOLOGY

3.1 Key

The key is a sort of parameter applied into an algorithm to transform a plaintext into a cipher text, or a cipher text into a plaintext inversely. The keys are divided into encryption keys and decryption keys. The length of the key decides how difficult it is to decrypt a ciphertext. In cryptography, the keys are widely used in various functions and features, i.e. in a digital signature and a digital certificate. (Janssen, 2010.)

In comparison with the algorithm, it is more convenient to change the key instead of changing the whole algorithms. The key is only a parameter, but the algorithm refers to a serious of mathematical issues. Thus, the user is more inclined to modify the key for strengthen the security of a message under the normal conditions. (Janssen, 2010.)

3.2 Plaintext and Ciphertext

The plaintext is the text that directly represents the original information without any modification before encryption. It is readable for the readers even without any assistance from tools or software. For the experts and the amateurs, a plaintext is completely understandable.

After the plaintext is encrypted, the encrypted text is called ciphertext. In a ciphertext, all the original information is transferred into pieces of unreadable codes which shadow the original information. As a result, the readers can not directly read the original information in the ciphertext.

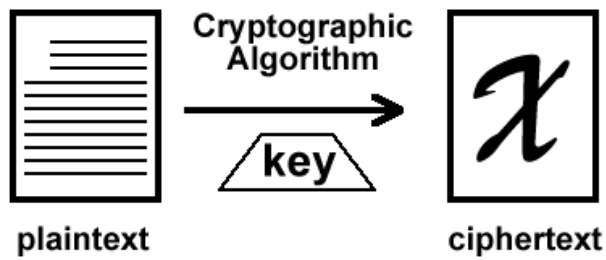


Figure 1. Key, Plaintext and Ciphertext (Heitmeyer 2011)

3.3 Cryptanalysis

The cryptanalysis refers to a technique, by which a cracker attempts to crack the ciphertext without knowing about the key. It is similar to decryption, in which the key has been known. Thus, in order to create a secure key, it is indispensable to consider about the possibility of the cryptanalysis that a cracker may use to break the cryptosystem. (Rouse 2014.)

In the modern cryptanalysis, Frequency Analysis is an old method for cracking the classical ciphers according to the daily methods. In English, for instance, the letter E is likely to have the highest frequency to be used in the text. According to this method, when using frequency analysis to decipher the text, it is concluded that the letter with highest frequency appearing in the ciphertext is E as well. However, because a plaintext is encrypted in the blocks instead of the characters, frequency analysis is not as effective as it used to be. (Lucas 2006, 17.)

4 BASIC THEORY OF CRYPTOGRAPHY

4.1 Encryption and Decryption

Encryption is a method that transforms the original information from a clear text into pieces of unreadable cipher texts according to a particular algorithm. The purpose of encryption is for assuring the confidentiality of the original information. By utilizing encryption, even if an unauthorized user intercepts the encrypted text, the unauthorized user cannot understand the contents of the original information, because the unauthorized user lacks the key to decrypt the text into the clear text. (Rouse 2014.)

After encrypting information, decryption is a method that restores the original information from the unreadable cipher text by entering a corresponding key. It is an inverse process of encryption. The primary procedures in the decryption process are the same as the procedures in the encryption process. (MSDN 2014.)

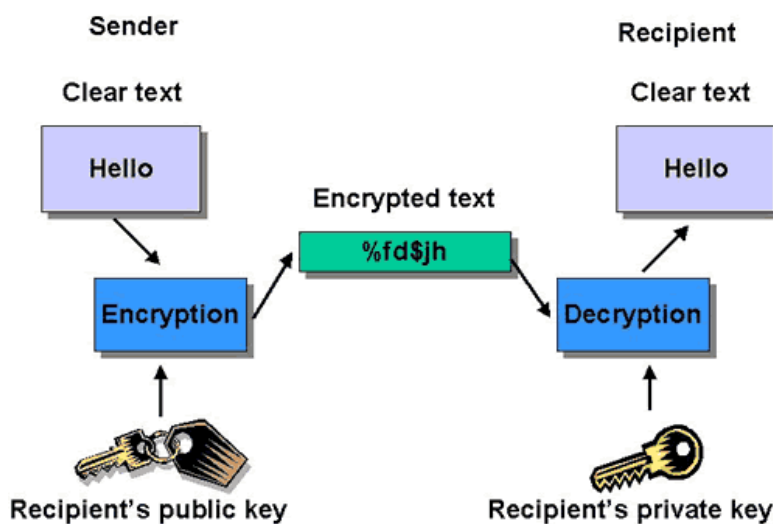


Figure 2. Encryption and Decryption (Keyyoung Information Ltd. 2014)

4.2 Symmetric Encryption

Symmetric encryption is an encryption method that uses a single key for both information encryption and information decryption. Meanwhile, the symmetric encryption method is also called as Single-Key encryption (Wikimedia Foundation,

Inc. 2014b). However, using a single key for both encryption and decryption potentially increases the risk of being cracked as well.

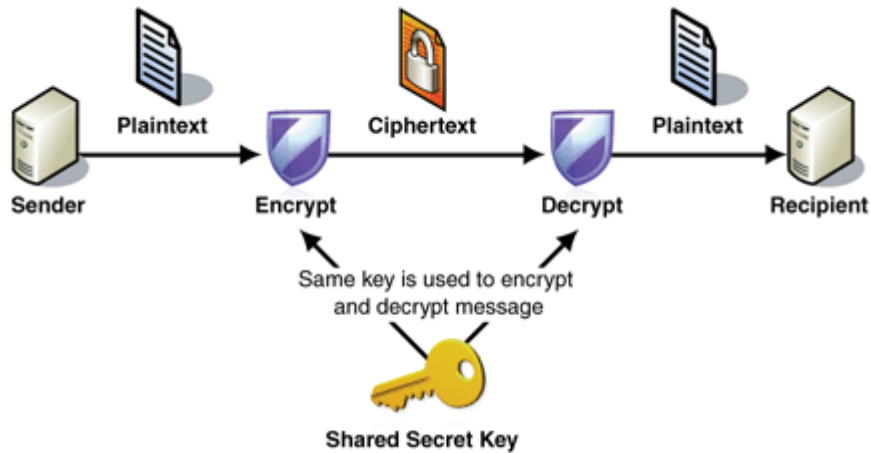


Figure 3. Symmetric Encryption (Thakor 2013)

In the symmetric encryption process, once the single key is changed, the corresponding encrypted message changes as well. And the decrypted message is completely disparate too. Thus, if the receiver finds that the key is changed, the user is supposed to decrypt the message again.

Although using a single key is able to simplify process and accelerate processing efficiency, it also becomes a weakness on security. Due to the Internet is not absolutely secure, the key may be intercepted by a malicious person when transmitting the key via the Internet. Once the key is intercepted and captured, the malicious person can use the captured key to decrypt the encrypted message and steal the confidential information in the message.

4.3 Asymmetric Encryption

In comparison with symmetric encryption which uses a single key for both the encryption process and the decryption process, the asymmetric encryption process is more difficult to attack, resulting from separate keys. In the asymmetric encryption process, a private key for decryption and a public key for encryption are required. More importantly, for the purpose of security, the private key and

the public key must be totally disparate. In this way, the possibility for the crackers to crack the message is dramatically decreased. (Hitachi ID Systems, Inc. 2014.)

Within a key pair which consists of a public key and a private key, the algorithm for creating a public key involves in the extremely complex mathematical formulas. Therefore, it is extremely difficult to calculate the corresponding private key according to the algorithms of a public key. Through this method, the security of the key has been remarkably surged. Normally, the public key is outward, whereas the private key is personally possessed. Consequently, Asymmetric Encryption is called Public-Key Encryption as well. (Wikimedia Foundation, Inc. 2014b.)

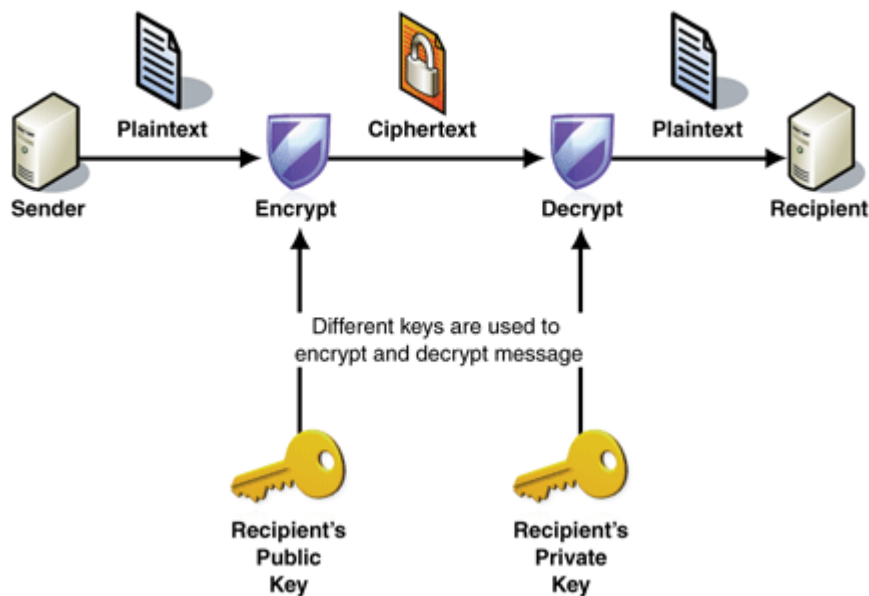


Figure 4. Asymmetric Encryption (Blurrent 2014)

4.4 Key Space

The key space refers to the whole possible encryption keys of an algorithm. If a malicious person searches for a key by exhaustively search throughout the whole key space, it is possible for the malicious person to find the key and crack the cryptographic system. Thus, a secure key space plays a vitally important role in enhancing the security of a cryptosystem. (Teeriaho 2006.)

In term of the attribute, normally over a half of the keys in the key space must be searched to find the right key. Thus, the secure key space should be over 80 bits. Through this standard, the block cipher DES in which the key space is only 64 bits is insecure. However, the key size is not equal to effective key space, unless the encryption algorithm is well planned. (Teeriaho 2006.)

The other attribute of the key space is that all the keys in the key space should be set absolutely randomly. If violates this attribute, the nonrandom keys in the key space will probably display certain clues about the right key for the cracker. Then, the time to search the right key through the key space can be dramatically reduced according to the clues. As a result, the insecurity of the algorithms is begot.

Besides, the key space plays an important role in resisting the attacks. The size of key space is positively linked with the difficulty to crack an encrypted message. Therefore, the difficulty for a malicious person to crack the cryptosystem is raised when the key space is prolonged. (Kessler 2014.)

In cryptography, the most effective attack is the Brute Force attack. In this attack, an attacker performs a complete search within the key space of all the possible keys to find the exact key. In order to prevent the Brute Force attack from locating the exact key, it is necessary to prolong the key space size so that the searching time will increase. When the key space size is large enough, the searching time will be too long to locate the key. By this method, it effectively ensures the search from attackers to be ineffective. (Janssen 2014.)

5 HYBRID ENCRYPTION SYSTEM

5.1 Authentication of Hybrid Encryption System

The hybrid encryption system is a system that congregates multiple and different types of the ciphers. Meanwhile, the hybrid encryption system also takes all advantages of them. Thus, the hybrid encryption system possesses the convenience of a public-key cryptosystem and the efficiency of a symmetric-key cryptosystem. (Janssen 2014.)

The hybrid encryption system provides effective solutions to the problems related to the key encryption management, the computing time, the integrity, the authentication and the confidentiality. Moreover, the hybrid encryption system protects the data integrity by using the hash function, improves the authentication by using the digital signature and enhances the data confidentiality by using the AES.

Through the hybrid encryption system, the receiver will receive an encrypted message with a digital signature. Utilizing the digital signature to confirm the receiver that the message from the sender is incapable of being viewed or modified by the unauthorized people. Moreover, the digital signature also plays the role to verify the identity of the sender. That utilize the digital signature in the hybrid encryption system convinces the receiver that the message is sent from the appointed sender, instead of the unauthorized people.

5.2 Encryption and Decryption of Message

The encryption process of a message in the hybrid encryption system is accomplished by Rijndael AES (Advanced Encryption Standard) algorithm which is secure and efficient. Meanwhile, Rijndael, on which AES is based is designed to resist against the known attacks. More importantly, it is capable of adapting to disparate platforms. (Mateescu & Vladescu 2013, 661.)

The decryption process of a message in the hybrid encryption system is accomplished by the receiver with a secret key. And this secret key is the same key used by the sender. In the process of key transmission, the secret key is encrypted by RSA private key and the encrypted secret key is sent along with the message. (Mateescu & Vladescu 2013, 661.)

6 BLOCK CIPHER

6.1 Definition of Block Cipher

In cryptography, a fixed-length group of bits are defined as a block. Based on the block definition, the block cipher is an algorithm to encrypt the plaintext into the ciphertext with the same key, and it is a symmetric cipher. And the encryption key and the algorithms in the block cipher are applied into a block of data at one time, instead of into a bit each time.

An alternative method for the block cipher is the stream cipher, which is used less frequent than the block cipher. The stream cipher is a sort of the symmetric ciphers, as well as block cipher. When implement the stream cipher in the plaintext, the transformation between bits varies as time progresses. The stream cipher encrypts bits separately while the block cipher encrypt in a block of the plaintext. (Canteaut 2014.)

6.2 How Does Block Cipher Work

The block cipher divides the message into separate blocks, each of which the input length in binary is exactly same as other blocks. In most cases, the length of the input plaintext is not an exact multiple of the block size. Then, the encryption algorithm will pad some exact bytes to fill in the last block to ensure the whole text length is an exact multiple of the block size.

In the encryption process, the principle is using a block of the input plaintext and a block of the key to create a block of the output ciphertext. There is a row of all the blocks of the input plaintext, the block cipher will add the corresponding blocks of the keys into these input plaintext and encrypt them. Finally, the equal blocks of the output ciphertext are created. (Allen 2006.)

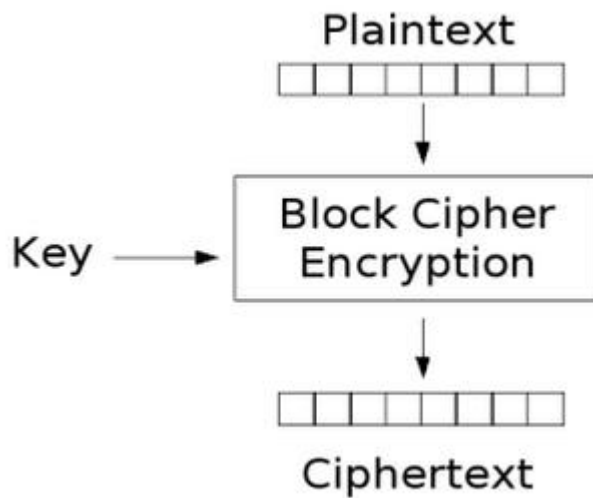


Figure 5. Block Cipher Encryption (McCombe 2007)

In the decryption process, it is declared as an inverse process of encryption. The decryption algorithm deletes the pad bytes, which is added during the encryption process. After this procedure, the output plaintext is returned. The same principle in the encryption process also applied into the decryption process. With the certain blocks of the ciphertext being provided, the block cipher will add the certain blocks of keys into the ciphertext and decrypt them. After this step, the certain blocks of plaintext are generated as an outcome. (Allen 2006.)

7 HASH FUNCTION

7.1 Definition

A hash function is defined as a particular mathematical calculation according to the algorithms. After the user inputs the message, the output is produced based on the algorithm. No matter how many bits being input, only a fixed size output will be produced. The value produced by the hash function is called hash value or message digest. And the input data is called message. For a hash function, once the original message changes, the corresponding message processed by a hash function changes accordingly. Even if only one bit changed in the input, the hash enables the output to be completely different. (Lucas 2006, 43.)

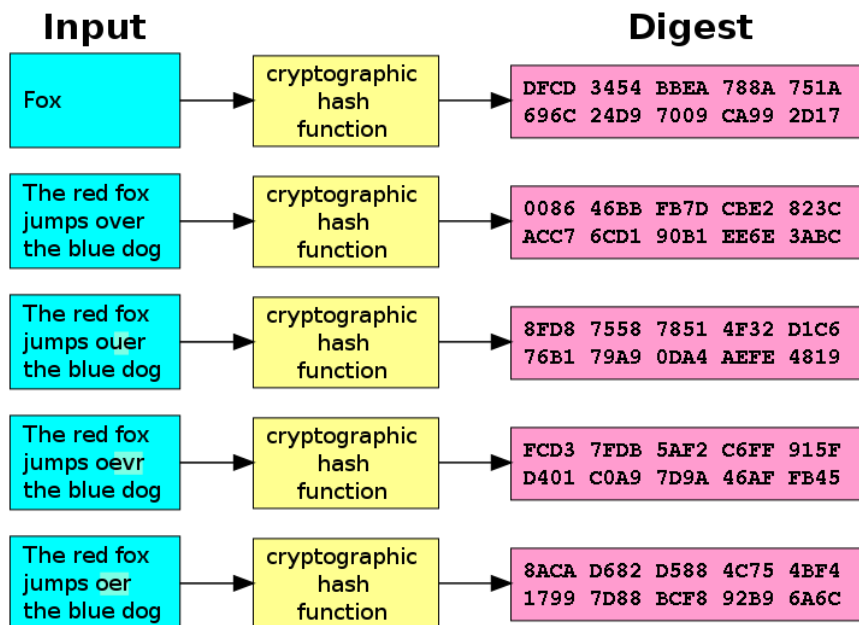


Figure 6. Hash Function (Wikimedia Foundation, Inc. 2014c)

In cryptography, a hash function has four properties. Firstly, the hash function cannot be inverted, which means it is impossible to produce the input based on the given hash value. This is called the one-way hash function. Secondly, if any message is given, it is easy compute the hash value through the hash function. Thirdly, there is no possibility to change the message without changing the hash value. Finally, each message has its unique hash value. Based on this property,

even if nuance exists on the input data, the output is completely different. Therefore, these properties of hash value have remarkably enhanced the confidentiality and security of information.

7.2 Hash Function in PGP

In PGP, a cryptographically strong hash function is applied into the plaintext. Then, a message digest is created by the hash function. With the help of the message digest and the private key used for signing, PGP successfully creates a signature. Afterward, PGP transmits the signature and the plaintext together. When receives the message, the receiver uses PGP to compute the message digest again, by which verifying the authenticity of the signature received. (PGPi 1999.)

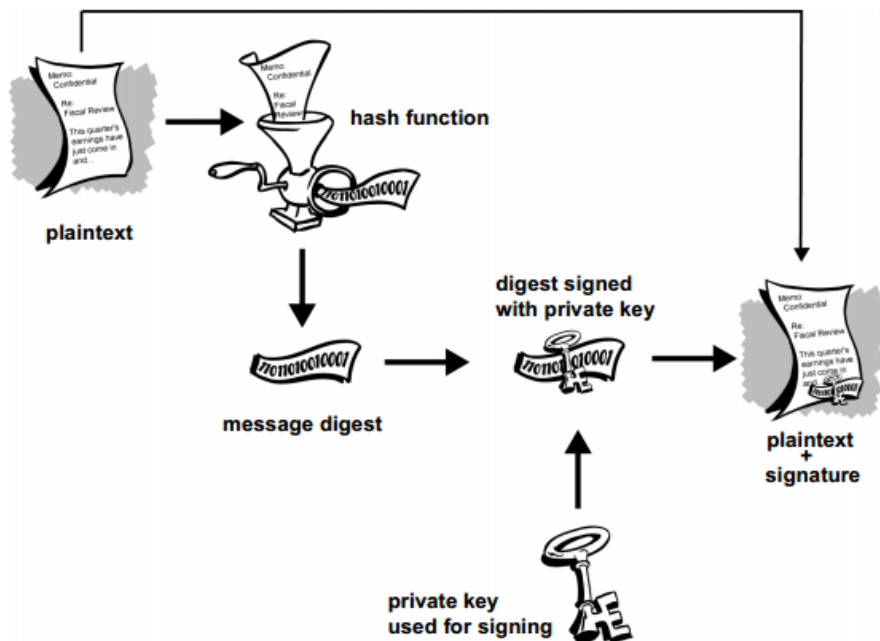


Figure 7. Digital Signature in PGP (PGPi 1999)

Undoubtedly, the hash function is highly secured. Even if a slightly change happens in the signed message, the final verification on the digital signature will fail. Therefore, it is impossible to modify the signed message or remove the signature from the signed message for any malicious purposes.

8 DIGITAL SIGNATURE

8.1 Digital Signature

A digital signature refers to a mathematical mechanism to verify the authenticity of the identity of the sender. The purpose of the digital signature is to convince the receiver that the message is sent from an authenticated sender. Creating a valid digital signature is mainly using the asymmetric encryption, which is also known as the public encryption. (Lucas 2006, 22.)

To create a digital signature, using the public key algorithm such as RSA or DSA to generate a key pair in which contains a public key and a private key, is the prerequisite. The public key can be obtained by anyone, but the private key is only reachable by the sender. If the sender wants to digitally sign the message, the sender need to encrypt the message by sender's private key. Then, the sender sends the message which contains the sender's public key to the receiver. Due to the message can be decrypted only by the sender's public key, a successful decrypted message with a digital signature verifies the authenticity of the identity of the sender.

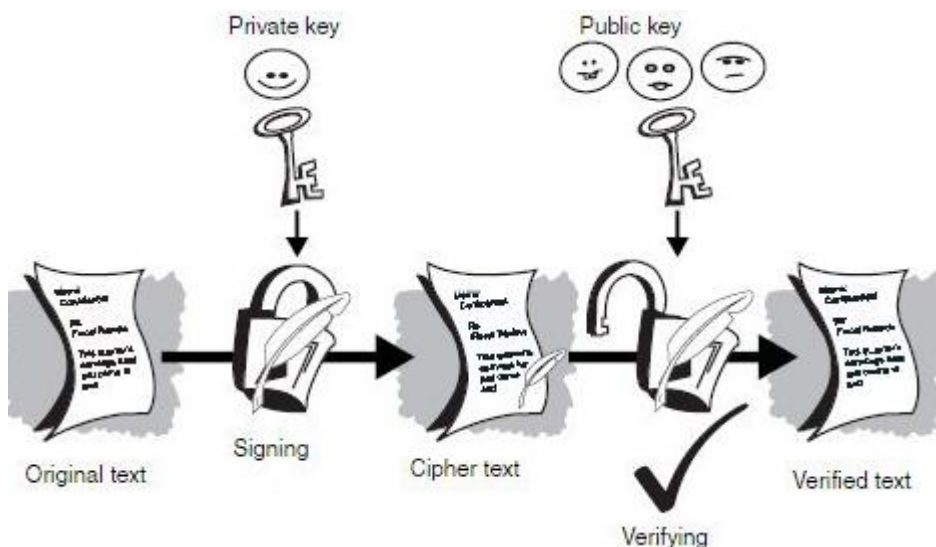


Figure 8. Digital Signature (Kelly & McKenzie 2002)

8.2 Digital Signature in PGP

In PGP, it used the public-key encryption to digitally sign the message for protecting the hash value from being stolen. First, when the users input the plaintext, PGP will create a hash value for the plaintext through the hash function and encrypt the hash value by the private key. Then, a digital signature is generated. Next, PGP will transmit the encrypted hash value to the input text, through which the message has been digitally signed. Finally, PGP sends both the message and the encrypted hash value to the receiver. (PGPi 1999.)

After operating the steps mentioned above, the receiver will receive a message with the plaintext and the encrypted hash value. If the receiver has downloaded the PGP software beforehand, the hash along with the messages will be decrypted by the sender's public key. Due to private key for the message is only reachable by the sender, the hash value with the message can only be created by the sender as well. Meanwhile, on the side of the receiver, PGP will independently generate a hash value. If the hash value created by receiver's side matches the hash value created by the sender, it is certain that the message is sent by the specific sender. (PGPi 1999.)

Furthermore, if someone tries to change the message, the system will display an error when it confirms the hash value. Then the sender's public key may not decrypt the hash value. Instead, it will show that the message is coming from other's private key. Even if the sender's public key still decrypts the hash value, this hash value can't match the hash value from sender. The receiver will be informed about the modification on the message.

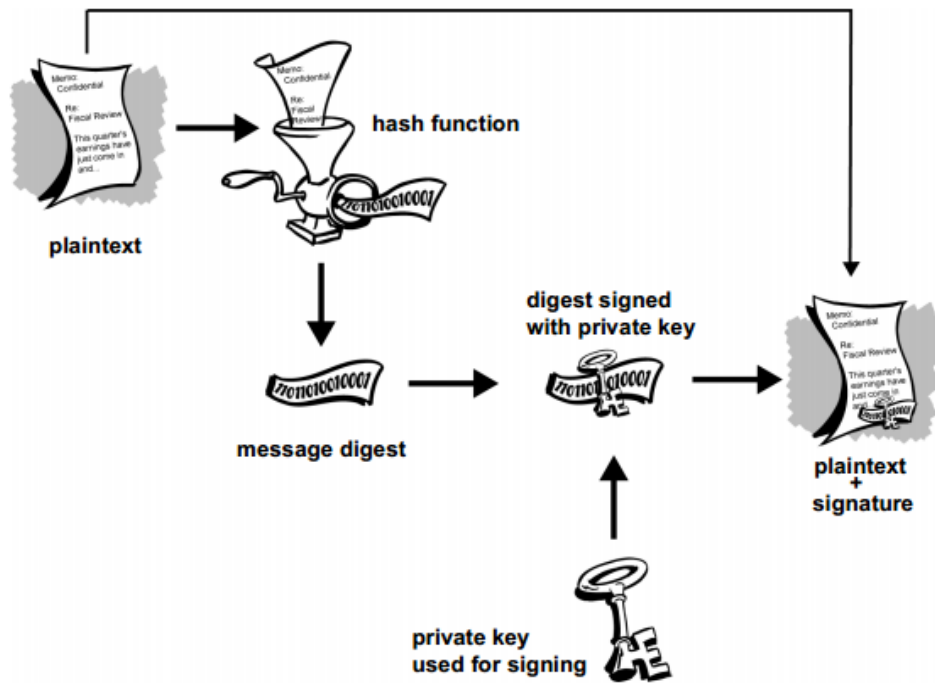


Figure 9. Digital Signature in PGP (PGPi 1999)

9 KEY DISTRIBUTION

For the symmetric key encryption, there are three prime ways to distribute the keys. Firstly, sending the key via an encrypted path is feasible. Secondly, authorizing a trustworthy organization to deliver the key is viable. Thirdly, the safest way is to privately meet and transfer the key. However, the three ways do exist uncertainty which reduces the security of the key.

For the asymmetric key encryption, it is common to use the public keyserver for distributing the public keys. Through this method, the public key is uploaded to a specific server which is accessible to anyone. At the same time, the private key is maintained privately and safely.

9.1 Keyserver

In PGP, it uses the keyserver which is able to worldwide distribute its key. PGP has established a special Internet server to enable the users to upload or remove the PGP keys. By clicking the bottom “Uploading Your Key”, the users can upload the public keys and enable the public keys to be searchable for other users. By clicking the bottom “Removing Your Key”, the users can remove the keys from the searchable directory. (Lucas 2006, 37.)

Moreover, PGP has set up a large amount of alike keyserver around the world and all the keyserver contain the same database which maximizes the users' options and improves the utility of the PGP keyserver. In this way, even the people come from the different countries can share the same key resource. And the PGP software is automatically connected with the PGP keyserver, which greatly improves users' efficiency to distribute the public keys.

Compared with the former PGP servers which permits everyone to upload the public key, the latest PGP server sets up some restrictions on the authority. On the webpage of the PGP Global Directory, a new service named Verified Key Service is promulgated. Being confined by this Verified Key Service, only the key

owner deserves the right to publicize the key in the directory. If the user wants to upload a key, the user will be required to send an email to the email address in the key and to ask for the permission from the owner of the key. Meanwhile, if a person has access to the email account of the key owner, the person can upload the key to the PGP server without any obstruction from the PGP group. (Lucas 2006, 38.)

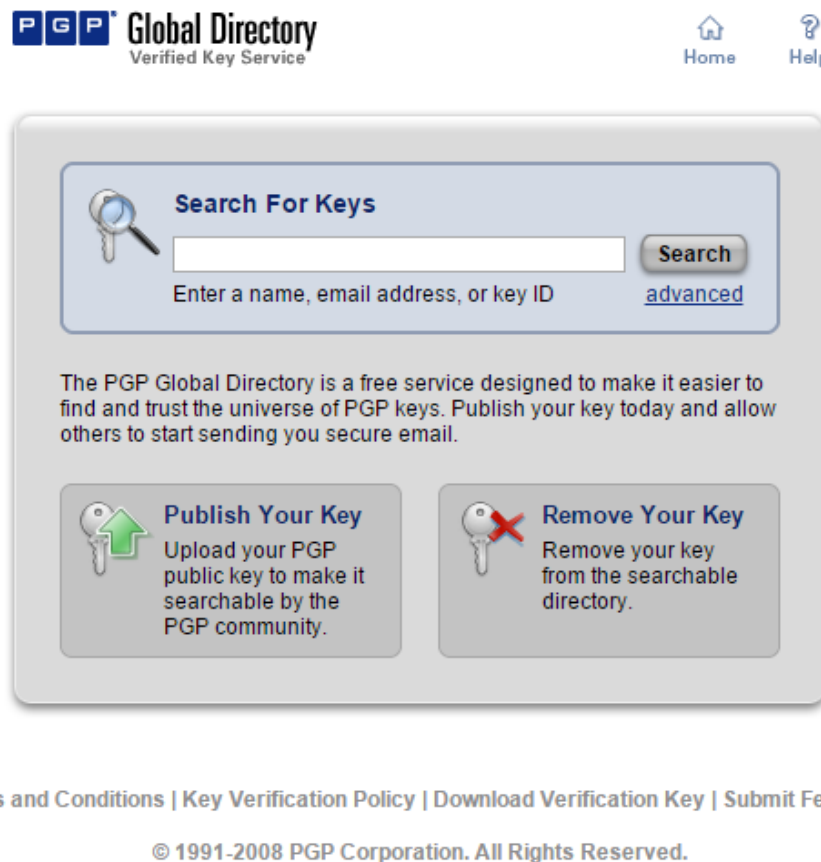


Figure 10. PGP Keyserver (Symantec Desktop Email Encryption, 2014)

Similar to the keyserver, the certificate server also contains a database that allows the users to upload digital certificates and search for the corresponding digital certificates. To enhance the security of the certificate server, some administrative organizations are entrusted to manage the server in various aspects. For example, the administrative organization manages the verification of the key service. Regulated by the organization, only the verified key is allowed to be uploaded to the server.

10 CERTIFICATE

10.1 Digital Certificate

In cryptography, the digital certificate is vitally important. Because of it, the user can ensure that the key is from the correct person, instead of unauthorized person. Meanwhile, there still exists some potential risks and threats from the other attacks. For example, man – in – middle attack. In this attack, the malicious people pretend to be the person that the user want to message to. The malicious people impose a counterfeit key in the public server and attach the name of the person that the user wants to send message to. In this way, the user might mistake the public key from the malicious people for the public key from the correct receiver. After encrypting the message with the counterfeit key, the encrypted message will be sent to the malicious people. (PGPi 1999.)

Theoretically, there three methods available, sending the key via an encrypted path, authorizing a trustworthy organization to deliver the key and private meeting to transfer the key. However, in practical application, all of the three methods have certain weakness and restriction. Firstly, the private meeting and authorizing a trustworthy organization are strictly restricted by some objective conditions. For instance, two parties are in the opposed areas on earth, there is no opportunity for them to meet in person, and there is no fully trusted organization for transmitting the extremely important key. Thus, these two means are defectively and limited. As for sending key in an encrypted path is entirely effected by the security level of the path. Such a man – in – middle threat can occur in the encrypted path. Hence, the potential risks and the potential threats are able to degrade the security level of the encrypted path, which led to the insecurity. (PGPi 1999.)

As a result, the digital certificate is created for protecting the public keys. By using the digital certificate, it is ensured that the public keys using by the users are the correct public keys of the intended receivers. For the physical certificate, it com-

monly shows the name, the birth date and the gender for the purpose of the identity authentication, such as the passport and the residence permit. The same function also applied into the digital certificate, which is a form of the electronic passport. The main purpose of the digital certificate is to verify the ownership of the public key by the electronic documents.

For a valid digital certificate, it is supposed to contain at least a public key, the sufficient identity information and the several digital certifications. The public key in the digital certificate is used to assist the user in testing the validity of the key. The identity information such as the name in the digital certificate is used for the identity authentication. And the digital signature in the digital certificate is to claim that the information on the certificate has been testified by the person who signs it. However, the digital signature cannot warrant the authenticity of the whole certificate. The only part that it can assure is the identity information such as the name and the ID on the signed certification. (PGPi 1999.)

Based on these features, using a digital signature provides the identifying information. Because a digital signature is the forgery resistant, and it can be verified to guarantee the authenticity. This property has effectively prevented the other malicious people from replacing the original public key by the forged public key.

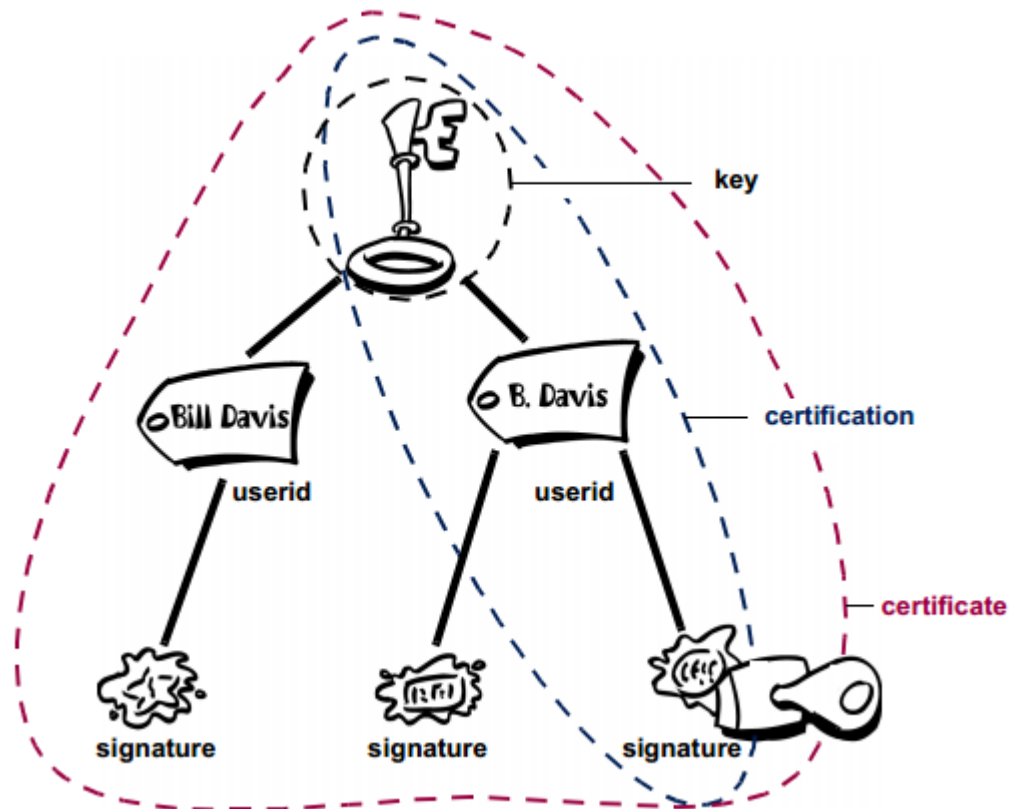


Figure 11. Digital Certificate (PGPi 1999)

10.2 Certificate Authority and Revocation Certificate

The certificate authority is an authorization in the Internet that issues the digital certificate containing the public key, the identifying information and several digital signatures for the message encryption. The CA's responsibility is to certify the owner's credentials and convince the users that the information on the certificate is reliable. It is a third party which is trustworthy for both the owners of the public key and the users of the public key. (Rouse 2007.)

Furthermore, if the user loses his/her private key, it is urgently necessary to proclaim this situation. This is the function of the Revocation Certificate. It enables the users to announce that the user's key pair is invalid. Once a key is produced, the revocation certificate will be generated instantly. (Lucas 2006, 35.)

In the aspect of storing the revocation certificate, the users should bear in mind that never store personal revocation certificate publically, such as the public computer. It is insecure to deal with the revocation certification in the mentioned way. If the others gain the user's revocation certificate, he/she can intentionally disable the user's private key around the world, which is unquestionably inconvenient for the user. (Lucas 2006, 35.)

11 CERTIFICATE FORMAT

11.1 PGP Certificates

The PGP certification is a commonly recognized certificate format in PGP. In the PGP certificate, it should at least but not most contain the PGP version numbers, the public key, the identity information, and the valid period, the digital signature and the preferred key encryption algorithm. Each of these contents results in the corresponding functions. (PGPi 1999.)

To begin with, the PGP version numbers in the PGP certificates claim the current exact version, in which the key related to the specific certificate is created. Next, the certificate owner's public key reveals the algorithms, such as RSA applied into the key. Afterward, the identity information about the certificate owner, which contains the owner's name, the owner's ID and so on, is used for the identity verification. Then, it is undisputed that the certification owner's digital signature is an essential part of the whole certificate. Because it indicates whether the signed information in the certificate has been testified. (PGPi 1999.)

Besides, the valid period of the certificate should be attached as well. The particular period shows when the certificate becomes valid and when the certificate turns to be invalid. The last component of the PGP certificate is the certificate owner's preferred symmetric encryption algorithm for the key. It demonstrates the symmetric encryption algorithms which the certificate users incline to use for the key. (PGPi 1999.)

For every PGP certificate, it possesses a self-signature. In the self-signature, the users will discover that the owner of the key signed his/her own key. And the personal identifying information is along with the personal signature. In addition to the signature from the owner of the key, each PGP certificates is able to be signed by several different people, which means that the signed PGP certificates is certified by these specific people. Thus, it is common to find that in a separate

digital certificate, there exists the signatures from the owner of the key and from the other people. This is a particular characteristic of the PGP certificate.

Lastly, a valid certificate requires the public key and the information about the owner of the key to be transmitted together. In the PGP certificate, it allows anyone to validate a certificate based on the particular characteristic. Meanwhile, the PGP certificate bears out the hierarchical structure which uses a certificate authority to validate a certificate.

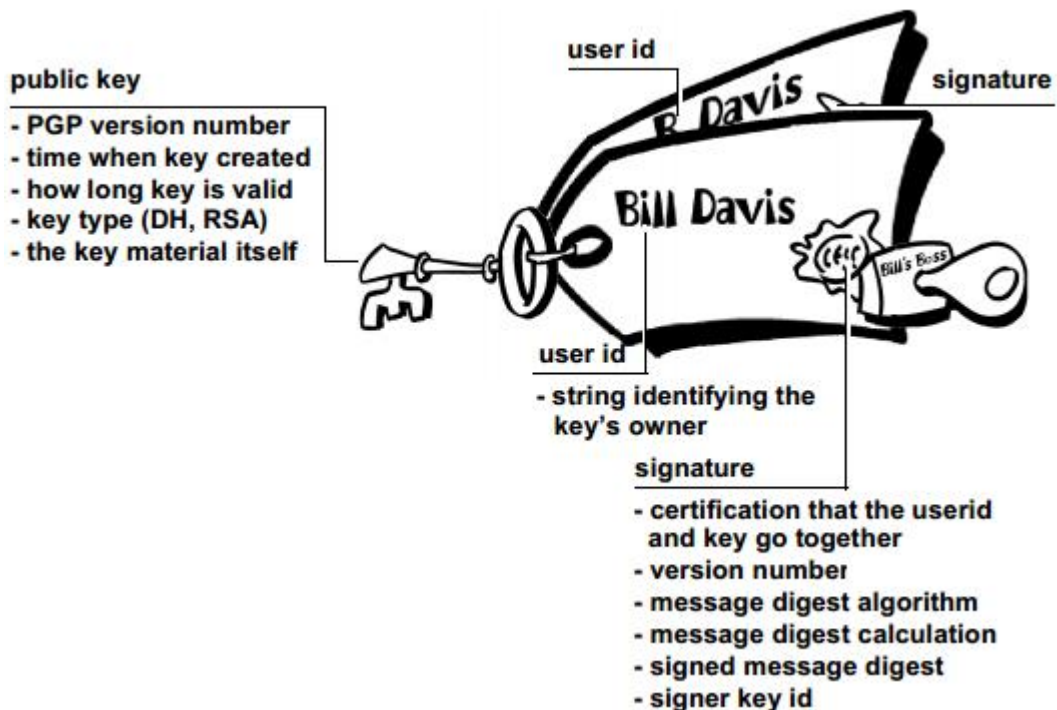


Figure 1. PGP Certificate (PGPi 1999)

11.2 X.509 Certificates

The other commonly recognized certificate format in PGP is X.509 Certificate, which should include the X.509 version number, the public key, the certificate issuer's and certificate owner's name, the valid period, the issuer's digital signature, the serial number of certificate and the algorithm identifier at lowest. Each of these contents corresponds to the specific functions. (PGPi 1999.)

Primarily, the function of the X.509 version number is to determine the exact version current in use. Different versions contain different information. Then, a public key from the owner of the certificate is required to identify the key parameters and point out the cryptography system. The next parts are the certification issuer's and owner's names. But the two names serve as the disparate purposes. The certificate issuer's name and the digital signature are for enhancing the reliability and the authentication for the users. On the contrary, the certificate owner's name is for the identity verification, the same purpose as it is in the PGP certification. (PGPi 1999.)

Moreover, the serial number of the certification is for differentiate the specific certificate from the others. As for the valid period of the certificate, it serves as the same purpose as it is in the PGP certificate. It reveals the exact time for the certificate to be valid and invalid. In the last, the algorithm identifier for the signature shows the detail algorithm used for the digital signature. (PGPi 1999.)

Furthermore, in the X.509 certificate, it requires a certain person to perform the validator role. In the most cases, the certificate authority is chosen as the validator. Therefore, in order to acquire a X.509 certificate, the users need to submit the application to the certificate Authority. (PGPi 1999.)

Meanwhile, according to the procedure to acquire a X.509 certificate, the applicants will be required to provide the public key, the personal identifying information such as the name and the ID. Meanwhile, the applicants should prove the holding of the private keys. Once the submitting documents and the keys are attested by the certificate authority, the certificate authority will offer the X.509 certificate to the applicants. (PGPi 1999.)

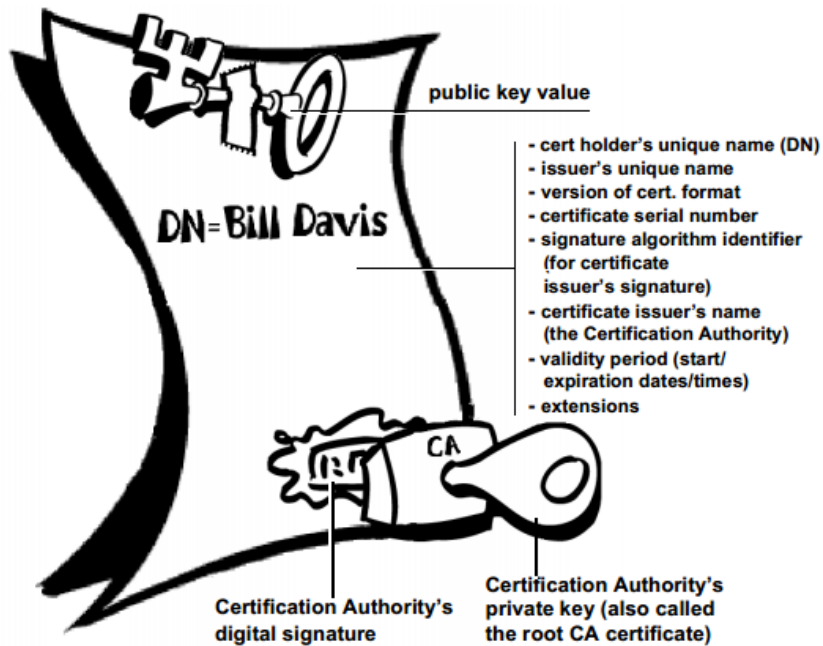


Figure 13. X.509 Certificate (PGPi 1999)

There are several fundamental differences between the PGP certificate and the X.509 certificate. First of all, in the PGP certificate, it is viable for anyone to become the validator and to create the personal certificate. In contrast, the X.509 certificate only allows the certificate authority to be the validator and issue the certificate upon the request. Secondly, in the PGP certificate, it supports one or several signatures. However, in the X.509 certificate, only one signature is permitted.

12 WEB OF TRUST

12.1 Origin of Web of Trust

The core principle for the PGP implementation is about the identity verification. Normally, the only way to recognize the identity of the sender is to view the email address showing in the FROM column. More deeply, the user can identify the sender by matching the private keys. However, how to authentically connect the real word identity with the key pairs has become a problem.

In the business fields, the certificate authority has become a general method to authentically connect the identity with the key. Most people pay the certificate authority for its digital certificate to verify the identity. But this approach consumes quite much time and costs much money. And there is no technological superiority on the certificate authority. More terribly, there is no absolutely warranty about the validity of the digital certificate that the certificate authority has signed. Thus, PGP originates Web of Trust, which enables the users to generate the digital signature by themselves. Meanwhile, it transfers the responsibility to verify the identities into the users. (PGPi 1999.)

12.2 Application of Web of Trust

Web of Trust is a network that connects the individuals around the world together. There is a central storage within this network, in which people can identify and digitally sign the key mutually. The idea of the Web of Trust completely discards the principle of the certificate authority. The resource and the effectiveness of this network is positively linked with the number of the users. The more users use this network, the more effective this network will be. (PGPi 1999.)

In the Web of Trust, if a user received a digitally signed message from a stranger, the user can identify the sender's identity by inspect the sender's public key from the central storage. If that public key has been verified by the others, it is of great possibility that the sender's identity is authentic. Especially when the public key

in the central storage has been signed by the trustworthy people, or by some people that the user trusts, there is no doubt that the identity of the sender is authentic. In addition, the more people sign a key, the shorter a key will be.

However, being a part of the Web of Trust cannot refer to the reliability of a person. A negative situation might occur in the Web of Trust either. If a person that signs anyone's key that he or she encounters in a casual manner, the key signed by this sort of people is of no reliability. In this case, the users deserve the rights to choose which key and signing person they trusts. At the same time, the users will undertake the consequence resulting from their choices. All in all, the responsibility to verify the identity is on users' owns.

12.3 Weakness of Web of Trust

Being a unique feature of PGP, however, the Web of Trust is not compulsory for running PGP. On the contrary, the uniqueness of the Web of Trust causes some resistances from a part of users toward itself. Based on the global network of the Web of Trust that interconnects the individuals, the platform of the Web of Trust is relatively public. No matter the user signs the other people's keys or the others sign the users' keys, these interrelated people as defined as the associating people. The activities within the associating people are tractable under the particular techniques. This is the similar principle as the police track the suspects. (PGPi 1999.)

If a person A intentionally investigates a person B's activity and the person B once signed the user's key, the person A can easily track from person B to the user. As a result, the activity of the user will be investigated as well. For the user who pays much attention on the personal privacy, the Web of Trust is the one that this kind of users want to escape from.

An alternative solution for this problem is to verify the key locally and personally, which mean the signature cannot be exported to the public server. And it is safer if the user only verify the key when the user must do verification. By using the

personal verification, the users are capable of taking full advantages of PGP as well.

13 CONFIDENTIALITY OF PGP

In cryptography, the confidentiality is the feature that enables the message to be invisible for the unauthorized people. When transmit the clear text through the Internet, there exists many potential security threats. In term of the ciphertext, only the person who holds the appropriate key can read the ciphertext. Based on its confidentiality, the ciphertext is a suitable solution to solve the secure risk threats.

PGP is described as a hybrid cryptosystem that combines convenience of a public-key cryptosystem and the efficiency of a symmetric-key cryptosystem. Meanwhile, it possesses high level of the confidentiality to remain the message private. There are six main actions that PGP has accomplished to protect the confidentiality of the emails, each of which has the specific meaning.

To start with, PGP can digitally signs the message with the sender's private key to convince the receivers about the sender's identity. Secondly, PGP is capable of testing the authenticity of the digital signature by using the sender's public key. In this way, this function enables the receivers to verify the identity of the senders to improve confidentiality of the message.

Besides, PGP can encrypt the message with the receiver's public key to enable the sender to specify the receiver. Meanwhile, PGP can decrypt the message with the private key if the user intents to. After that, PGP is able to encrypt the message with the receiver's public key and meanwhile digitally sign the message with the sender's private key. Through this function, PGP enables the sender to limit the specific receiver and enable the receiver to be informed about the identity of the sender. Lastly, PGP is capable of decrypting the message with the receiver's private key and verify the signature with the sender's public key at the same time. By this function, PGP enables the users to accomplish decryption and verification. (Lucas 2006, 14.)

13.1 Encryption and Decryption of PGP

The first step in the encryption process of PGP is the data compression, which greatly compressed the clear text into the small size text. It is similar to the Zip file format which has been widely used in the daily life for the data compression. After the data compression, the size of the original clear text has been greatly reduced. As a result, the transmission time and the space are also dramatically reduced. Meanwhile, compressing data also decreases the pattern in the clear text. Due to some malicious people who try to crack the text by exploring the pattern in it, the pattern decreasing undoubtedly reduces the risks from the cryptanalysis.

After the data compression, PGP will randomly generate a session key, which is a one-time key. With the random key and the symmetric algorithms, PGP encrypted the clear text into the ciphertext. After this step, the one-time session key will be encrypted with the public key for the secure purpose, and will be sent to the receiver along with the ciphertext.

Compared with the encryption process in PGP, decryption is an inverse process. The receiver uses the private key to recover the session key, after which the decrypted session key decrypts the message. The basic procedures of the encryption process and the decryption process are almost the same.

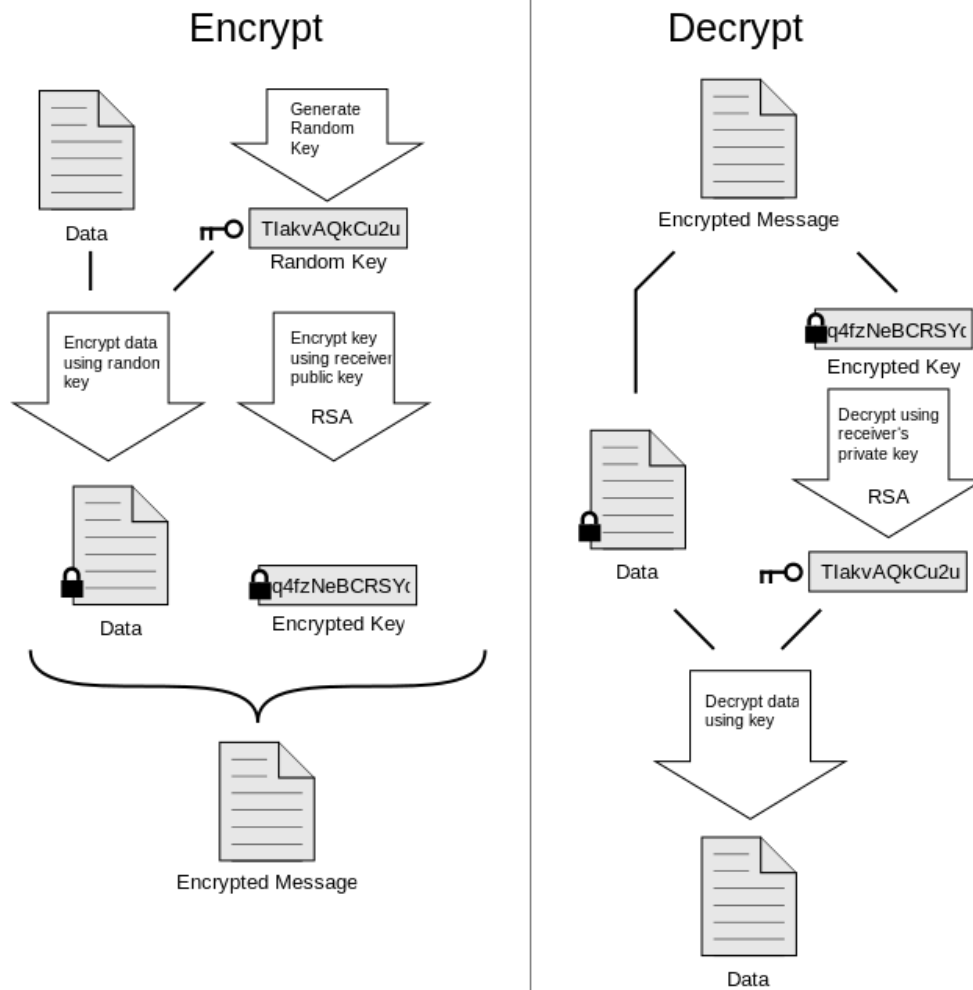


Figure 14. Encryption and Decryption of PGP (Wikimedia Foundation, Inc. 2014a)

14 SIGN A KEY

In cryptography, a person A signs a key of a person B means the person A has verified the identity of the person B. In PGP, signing a key not only means the confirmation of the identity, but also means trusting the identity. More importantly, the trust in PGP is specialized in trusting the identity of a person, instead of the trust on a person's other features. Meanwhile, signing the key will enhance the key holder's Web of Trust as well.

In PGP, the format of the key signing can be both formal and informal. When sign for a close friend, the key signing can be informal. And when sign for a strangers, the key signing is always formal. There is no absolute restriction on the key signing format.

14.1 Prerequisites for Signing Other's Key.

Firstly, signing a key requires the user to obtain the key holder's exclusive public key fingerprint and the unique key id integrated with the user ID. PGP will display the fingerprint and the key id upon the request. Within a key pair, the key id and the fingerprint are similar in their appearance. To guarantee the safety on transmitting the key id and the fingerprint, the offline mechanism is the first choice. Because it avoids the key id and the fingerprint from being attacked through the internet. (Lucas 2006.83.)

The second prerequisite for signing other's key is acquiring the key holder's public key, which can be easily discovered on the key server. The following prerequisites are the key holder's email address, the key holder's full name and the key holder's identity proof. Besides, the detail requirement for identity proof varies from the familiar people to the strangers. (Lucas 2006.83.)

14.2 Sign for Familiar People and Strangers

Signing for the familiar people in PGP is easiest. Initially, the user should acquire the key holder's key id and the fingerprint. Then check the key holder's legal ID and the user ID. Once the name and the email address on the legal ID match the name and the email address on the key, and the key id as well as the fingerprint match the corresponding information showed in the user's legal ID, the user is able to sign for the key holder. (Lucas 2006, 84.)

As for signing for the strangers, firstly, the user is supposed to check the stranger's ID for insuring the legality of the ID. Then, the user can ask the key holder for the key id, the fingerprint, the key server and the email address. The following step is for downloading the key from the informed key server, and for checking if the name, the email address and the fingerprint on the key match the legal ID and the asserted key. Only when all of these information matches perfectly, the user should sign the key. If any of the above information differs from the information in the legal ID and the asserted key, it is more advisable for the user to stop signing any key. The user should follow the rule that never signs a key from a person the user never meets beforehand. (Lucas 2006, 85.)

15 INSTALLATION

15.1 System Requirement for Installation

To successfully install the PGP software, it is vitally important to ensure the operating system is one of the following systems. Both the client side and the server side are supposed to meet the requirement for the installation process. The requirements below are the minimum requirements. If the version number of the device is above the following indication, it is capable of installing the PGP software as well.

Table 1. System Requirement

Client Side	Server Side
Microsoft Windows 2000	Microsoft Server 2003 Service Pack 2 32bit and 64-bit
Microsoft Windows Server 2003	Microsoft Server 2008 Service Pack 1 and Service Pack 2 32-bit and 64-bit
Microsoft Windows XP Professional and Home Edition 32-bit and 64-bit,	Microsoft Server 2008 R2 32-bit and 64-bit
Microsoft Windows Vista 32-bit and 64-bit,	512 MB of RAM
Microsoft Windows 7 32-bit and 64-bit,	64MB HD Space

15.2 Download Archive Package

The previous name of the PGP software has been changed to Desktop Email in the Symantec official website. The formal Desktop software charges fee from the users. However, a 30-days free trial is available for the users to evaluate the software. To download the trial ware, it is required to acquire a Symantec account.

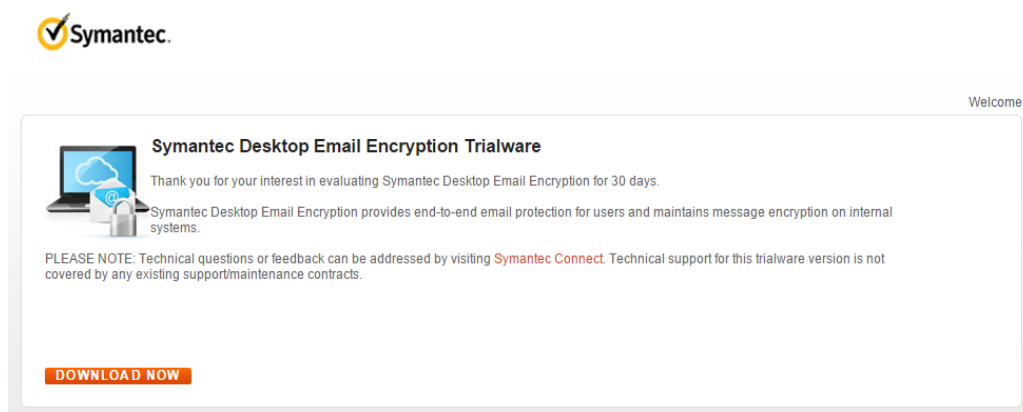


Figure 15. Symantec Desktop Email Encryption Trialware (Symantec Desktop Email Encryption, 2014)

The personal contact information and the operating system will be required to fulfill. Once finish the form, the user needs to select the correct version according to the user's operating system. In the webpage, it contains Windows, Linux and Mac versions. Meanwhile, the users can select the single file for the individual encryption management server and the evaluation guide. Multiple choices are provided for the users.



Welcome

SymAccount Login

SymAccount is Symantec's user account management application for Business customers. With a SymAccount, you have unlimited access to Symantec trialware, white papers, and other collateral.

Existing Users

Email/Username

Password

Forgot your Password?

LOGIN

Sign up Now : Create a new account

Email Address

Password

(Password must be 6 to 12 characters.)

Re-enter Password

CREATE ACCOUNT

Figure 16. Register for SymAccount (Symantec Desktop Email Encryption, 2014)

SOFTWARE DOWNLOAD

Symantec Encryption Desktop Corporate

Single File Download

File	Size	
Symantec Encryption Desktop Corporate 10.3.2 MP6 (Windows)	84 MB	DOWNLOAD NOW
Symantec Encryption Desktop Corporate 10.3.2 MP6 (Linux)	72 MB	DOWNLOAD NOW
Symantec Encryption Desktop Corporate 10.3.2 MP6 (MAC OSX)	29 MB	DOWNLOAD NOW
Symantec Encryption Management Server 3.3.2 MP6 (PUP)	1.03 GB	DOWNLOAD NOW
Symantec Encryption Management Server 3.3.2 MP6 (Full Zip)	1.72 GB	DOWNLOAD NOW
Symantec Drive Encryption Evaluation Guide (PDF)	929 KB	DOWNLOAD NOW
Symantec File Share Encryption Evaluation Guide (PDF)	1.05 MB	DOWNLOAD NOW
Symantec Desktop Client Email Encryption Evaluation Guide (PDF)	1.63 MB	DOWNLOAD NOW

Note: Using "Save Target As" may result in an access denied on the download
 Problem downloading or need more information? Go to [Download Instruction](#)>>

[Other trialware products](#)

Figure 17. Available Versions of Symantec Encryption Desktop (Symantec Desktop Email Encryption, 2014)

Once click the bottom "Download", the system will provide an archive package. In the archive package, there will be two EXE files for the 32-bit operating system

and the 64-bit operating system, and a folder contains the maintenance instruction. At the same time, the activation code will be sent to the email address that the user fulfills in the registration form.

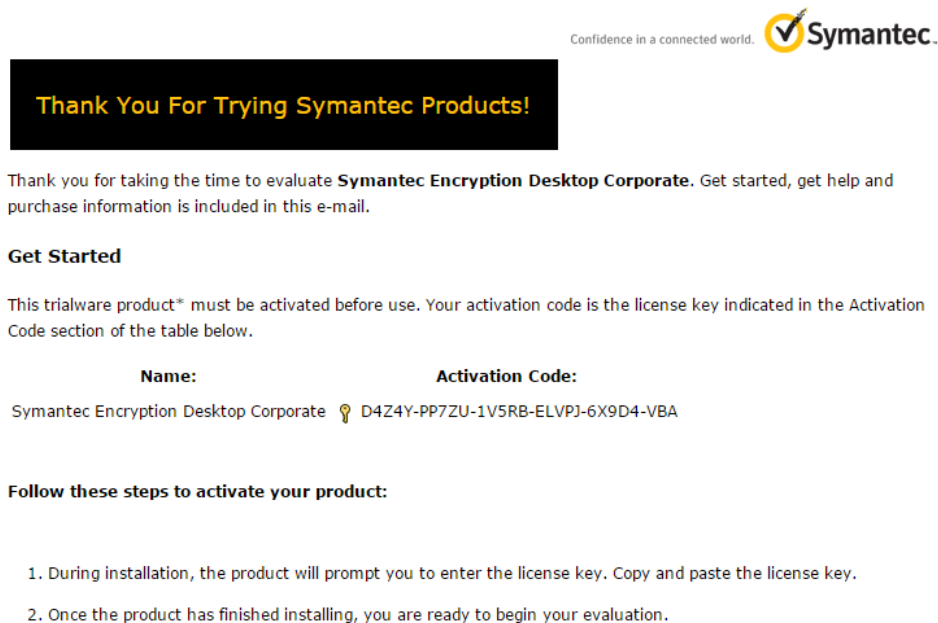






Figure 18. Acquire the Activation Code (Symantec Desktop Email Encryption, 2014)

After downloading the archive package, it is advisable to use administrative rights to decompressing the files into the designated locations. In the first step of the installation process, the user will be required to provide the activation code to activate the license, so that the user could move on the further steps of the installation process. Then, the user is capable of installing and setting up the software according to its instruction.

15.3 User Guide

On the right bottom of the desktop, there is an icon to display the state of the PGP software. There are totally four disparate icons to show the state of Normal Operation, Cached passphrase, Message proxying disabled and Busy. Each of these icons represents the situation that the PGP software is working in.

Table 2. Four Icons for Four disparate states

Icon	State	Explanation
	Normal Operation	1) Running normally and no other operations 2) No cached passphrase 3) Message proxying disabled
	Cached passphrase	Running normally with several cached passphrase.
	Message proxying disabled	Both sending message and receiving message will not be encrypted or decrypted.
	Busy	A specific operation is in use. Once the specific operation is accomplished, the state will return to Normal Operation.

When selects Programs PGP > PGP Whole Disk Encryption, the user has entered the Start Menu with the PGP desktop interface. In the PGP desktop interface, there are nine primary icons to perform various functions.

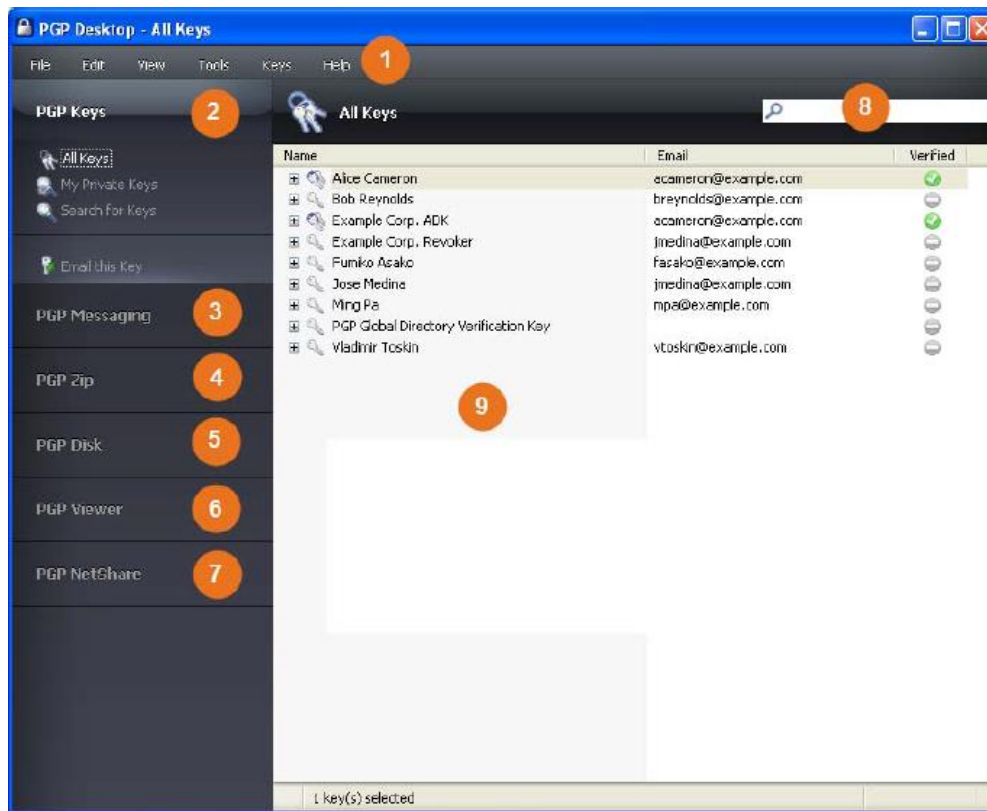


Figure 19. PGP Desktop Interface (Symantec Desktop Email Encryption, 2014)

For Icon 1, Menu Bar, It provide the user with the access to the PGP desktop command. Meanwhile, diverse control boxes possess various functional contents. According to the control box that the user selects, the available contents in Menu Bar change as well.

For Icon 2 to Icon 7, these icons are mainly used for the purpose of controlling. Icon 2, the PGP Key Control Box, enables the user to control the PGP keys. Icon 3, the PGP Messaging Control Box, enables the user to control the PGP messaging. Icon 4, the PGP Zip Control Box, enables user to control the PGP Zip and the PGP Zip Assistant, for the purpose of creating the PGP Zip archives. Icon 5, the PGP Disk Control Box, enables the user to control the PGP disk. Icon 6, the PGP Viewer Control Box enables the user to decrypt and verify the receiving message out of the mail stream. Icon 7, the PGP NetShare Control Box enables the user to control the PGP NetShare.

Within the last two icons, Icon 8, the PGP Desktop Work Area, it aims to provide the user with the information and the actions, so that the user can apply into the selection of the Control Box. For Icon 9, the PGP Key Find Box is designed to provide the user with the ability to search for the keys.

16 CONCLUSIONS

The original goal of the PGP software is to provide confidentiality against the government so that the government is unable to obtain the user's private message. After all these years, even if the potent company such as Google cannot avoid from rendering the user's private message to the government, the PGP software is competent to protect confidentiality of the user's message.

The reason why the PGP software is capable of maintaining confidentiality is that the PGP software utilizes end-to-end encryptions in which the message is encrypted at the sender's end and decrypted at the receiver's end. By end-to-end encryption, the intermediary through which the user sends the message, can only view the encrypted message as well.

Presently, the PGP software is not free of charge anymore, because the company which presently maintains the PGP software is Symantec. It charges 148.93 US dollars per license with the one-year essential support. Meanwhile, to assist the user in evaluating the software, Symantec provides a 30-day free trial.

BIBLIOGRAPHY

- Allen, N. 2006. How Block Ciphers Work. Referenced 26.11.2014
<http://blogs.msdn.com/b/drnick/archive/2006/07/20/how-block-ciphers-work.aspx>.
- Canteaut, A. 2014. Stream Cipher. Referenced 1.11.2014
<https://www.rocq.inria.fr/secret/Anne.Canteaut/encyclopedia.pdf>.
- Czagon, D. 2013. Symmetric and Asymmetric Encryption.
Referenced 12.10.2014
<http://resources.infosecinstitute.com/symmetric-asymmetric-encryption/>.
- Giry, D. 2014. Cryptographic Key Length Recommendation.
Referenced 02.12.2014
<http://www.keylength.com/>.
- Heitmeyer, D.P. 2011. Encryption Basics. Referenced 10.10.2014
http://cscie12.dce.harvard.edu/lecture_notes/2011/20110504/slide53.html.
- Hitachi ID Systems, Inc. Definition of Asymmetric Encryption.
Referenced 28.11.2014
http://hitachi-id.com/concepts/asymmetric_encryption.html.
- Janssen, C. 2014. Brute Force Attack. Referenced 17.01.2015
<http://www.techopedia.com/definition/18091/brute-force-attack>.
- Janssen, C. 2010. Cryptographic Key. Referenced 31.10.2014
<http://www.techopedia.com/definition/24749/cryptographic-key>.
- Jenkins, B. 2002. Hash Functions and Block Ciphers. Referenced 15.12.2014
<http://www.burtleburtle.net/bob/hash/#block>.

- Kelly, G & McKenzie, B. 2002. Security, privacy, and confidentiality issues on the Internet. Referenced 8.12.2014
<https://tspace.library.utoronto.ca/html/1807/4637/jmir.html>.
- Kessler, G. 2014. An Overview of Cryptography. Referenced 5.10.2014
<http://www.garykessler.net/library/crypto.html#keylen>.
- Keyoung Information Ltd. 2014. Encryption. Referenced 18.10.2014
<http://www.data-processing.hk/encryption>.
- Lucas, M. 2006. PGP and GPG: Email for the Practical Paranoid. San Francisco: William Pollock
- Mateescu, G & Vladescu, M. 2013. A Hybrid Approach of System Security for Small and Medium Enterprises: combining different Cryptography techniques. Referenced 4.12.2014
<https://fedcsis.org/proceedings/2013/pliks/193.pdf>.
- McCombe, I. 2007. Block Cipher. Referenced 23.11.2014
<http://imps.mcmaster.ca/courses/SE-4C03-07/wiki/mccombi/blockciphers.html>.
- Microsoft. 2014 Data Confidentiality. Referenced 30.11.2014
<http://msdn.microsoft.com/en-us/library/ff650720.aspx>.
- Newtechie. 2014 Types of encryption [What is]. Referenced 15.10.2014
<http://www.newtechie.com/2011/09/types-of-encryption-what-is.html>.
- PGPi. 1999. How PGP works. Referenced 23.12.2014
<http://www.pgpi.org/doc/pgpintro/#p13>.

- Rouse, M. 2005. Stream Cipher. Referenced 18.11.2014
<http://searchsecurity.techtarget.com/definition/stream-cipher>.
- SANA Institute. 2001. InfoSec Reading Room. Referenced 17.11.2014
<http://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730>.
- Symantec Corporation. 2014. Symantec Desktop Email Encryption (powered by PGP Technology). Referenced 28.01.2015
http://buy.symantec.com/estore/categoryDetailPage/productCode/PGP-DEE-EXP-LEM_Vx_12MO_PC/skuType/Product.
- Teeriaho, J. 2006. Cryptography. Referenced 3.10.2014
<http://ta.ramk.fi/~jouko.teeriaho/cry2.pdf>.
- Wikimedia Foundation, Inc. 2014a. Pretty Good Privacy.
Referenced 04.11.2014
http://en.wikipedia.org/wiki/Pretty_Good_Privacy.
- Wikimedia Foundation, Inc. 2014b. Symmetric-key algorithm.
Referenced 25.10.2014
http://en.wikipedia.org/wiki/Symmetric-key_algorithm.
- Wikimedia Foundation, Inc. 2014c. Cryptographic hash function.
Referenced 28.01.2015
http://en.wikipedia.org/wiki/Cryptographic_hash_function.
- Youd, D. 1996. What is a Digital Signature?. Referenced 5.11.2014
<http://www.youdzone.com/signature.html>.