Applications of Public Key Cryptography and Functioning Process

P.Kumaraswamy, C.V.Guru Rao, V.Janaki, Bhandi Bhaskar

Abstract—In cryptography, public key cryptography plays an important role to communicate sensitive information in online payment or any other electronic transactions securely. This paper illustrates the major applications of public key cryptography and their functioning process. The real time applications of public key cryptography are also included here.

Keywords: Public key cryptography, Encryption, Digital signature, Certificate, Authentication, Confidentiality, Non-repudiation.

I. INTRODUCTION

Information security is required in computer networks to maintain the trustworthy data. The major requirements of information security are, *integrity*,*availability and confidentiality*. The concepts relating to the communicate message are authorization,*authentication*and *non repudiation*. When the message is accessed by unauthorized person is known as loss of confidentiality. If the transmitted message is modified by any user is known as loss of integrity. If the network is not available to any legal user with the attack of denial of service then it isknown as loss of availability. To access the information in the network, every user should get the authorization by showing their authentication. Every user in the network should not deny the communication after delivering the message. It achieves the security service non-repudiation.

Information security uses cryptography to communicate data securely in the network with the help of encryption. Encryption is the process of converting data into another form, called as ciphertext. This cipher text not easily understood by any other user except the concerned authorized parties. Encrypted information can be changed back into its original form by only authorized users. Such information with the help of the authorized user can decrypt. Earlier, symmetric cryptosystem is used to perform encryption and decryption of messages [1]. In Symmetric cryptosystemonly one key is used for both encryption and decryption. If the key is maintained securely, the symmetric cryptosystem is safe otherwise the cryptosystem fails easily.In symmetric cryptosystem securely transferring the key is a difficult problem to the recipients. The invention of public key cryptography solves the problem of key distribution. In public key cryptography two keys such as public key and private key are used. The private key is maintained as secret at user side and the public key is publicly available to all the users in the network.

Publickey cryptography (Asymmetric key cryptography) is an important encryption and decryption scheme in online applications. It uses two different keys named as public key and private key [1]. In symmetric key algorithms only one key is used to perform encryption and decryption operations. But in public key cryptographytwo keys are used to perform encryption and decryption operations. If one key is used to perform encryption operation, second one is used to perform decryption operation vice versa.

In public key cryptography, it is not possible to calculate private key using the available public key in the network. Because of this reason public key can be freely available in the network. If a user encrypts a message with the public key of a target user, that message is decrypted only by the target user’s private key. Moreover, if a message is encrypted by a private key of a user, it is decrypted by the public key of that user. This process is also called as digital signature.

The keys generated in public key cryptography are too big such as 512, 1024, 2048 and so on bits. These keys are not easy to remember. Therefore, they are kept in the devices such as USB tokens or hardware security modules.

A major problem in public key cryptosystems is that an attacker can impersonate a legal user. He substitutes the public key with a fake key in the public directory. Further, he intercepts the communications or alters those keys. Public key cryptography plays an important role in online payment services and e-commerce etc. These online services be secure only when the authenticity of public key and signature of the user are secure.

The asymmetric cryptosystem should achieve the security services such as confidentiality, authentication, integrity and non-repudiation. The public key should maintain the security services such asnon-repudiation and authentication. The security services of confidentiality and integrity considered as a part of encryption process done by private key of the user.

The main applications of public key cryptography are considered are ***Digital Signature*** and ***Data Encryption***.

The encryption application provides the confidentiality and integrity security services for the data.The public key maintains the security services such as authentication and non-repudiation.

Revised Manuscript Received on April 12, 2019.

P.Kumaraswamy, Assistant Professor, Dept. of CSE, S R Engineeing College,Warangal, Telangana, India. (palleboina.kumar@gmail.com)

Dr.C.V.Guru Rao, Professor, Dept. of CSE, S R Engineeing College, Warangal. Telangana, India. (guru_cv_rao@hotmail.com)

Dr.V.Janaki, Professor, Dept. of CSE, Vaagdevi college of Engineering, Warangal. Telangana, India. (janakicse@yahoo.com)

Bhandi Bhaskar, Assistant Professor, Dept. of CSE, S R Engineeing College,Warangal. Telangana, India. (bhaskar_b@srecwarangal.ac.in@gmail.com)

Digital signatures are very useful in online applications. It provides the authentication and assurance of a user. The digital signatures are created by user's private key and also perform hashing on the encrypted data. The encrypted data means the digital signature is verified by the public key of the concerned user. The digital signatures will not be modified and tampered by any one. The major advantage is forging is not possible. But in conventional physical signatures forging is possible. Therefore, digital signatures provide the unique identity of a user or document.

Encryption is used to convert the plaintext message into unreadable format with the help of a key, again the message convert back to original message by using the decryption process.

The rest of the paper is organized as follows: Section 2 describes functioning of public key cryptography applicationsand real-time applications of public key cryptography are described in Section 3. The process of digital signingis discussed in section 4. Finally conclusion is given in section 5.

II. FUNCTIONING OF PUBLIC KEY CRYPTOGRAPHY APPLICATIONS

The functioning of public key cryptography major applications are described in the following sub sections [2]:

A. Encryption

In this process, each user encrypts the message with the receiver's public key. The encrypted message is decrypted by only the receiver's private key. Lets assume a user B's private key is Prv$_B$and public key is Pub $_B$. Asshown in figure1, If user A wants to send a message M to user B. First the message M is encrypted by the public key of user B and send it to user B. Then that encrypted message is decrypted by the private key Prv$_B$of user B.

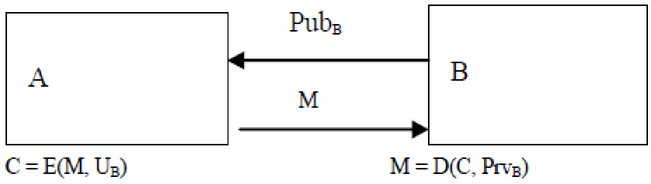

Figure1: Encryption functioning process

B. Digital Signature

Digital signature is used to sign the message to authenticate the message sender in the network. For example, If user A wants to send a message M with his digital signature to user B. First, user A signs the message with his/her private key Prv$_A$. The signed message sends to user B without performing any encryption on the message. After receiving the message, user B verifies the signature of user A with his/her public key Pub$_A$.

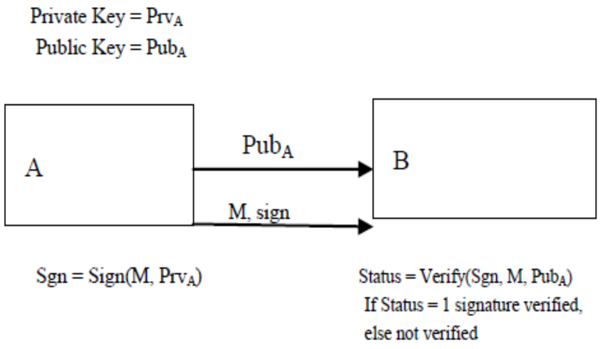

Figure2: Digital signature functioning process

C. Certificate

Digital certificates are used to authenticate the public key of a user. In public key cryptography, there is possibility that public key of a user can be modified by an attacker in the network. To avoid the authentication problem of public key digital certificates are developed. The digital certificates are issued by the certificate authority as shown in below figure1.

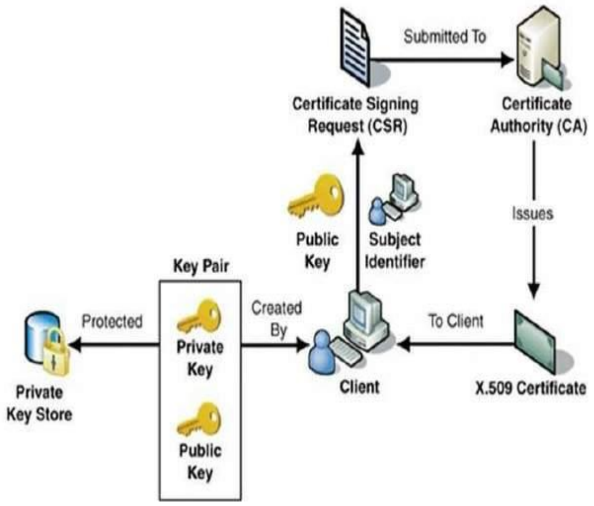

Figure1: Certificate generation process in public key cryptography.

In general, [11] digital certificates are computed in the format of x.509 format. It is the standard format accepted inthe Public-Key Infrastructure (X.509)has adapted the standard to the more flexible organization of the Internet. As shown in the above figure1, each user generates his/her public key and private key. The private key is maintained as secret at the user and public key is hosted in the network. Before host the public key in the network , each user requests a certificate authority (CA) to issue a digital certificate for his/her public key. Digital certificate consists information such as user's public key , user name, user signature, validity etc

III. REAL-TIME APPLICATIONS OF PUBLIC KEY CRYPTOGRAPHY

The main business applications for public-key cryptography are [3-10]:

- **Digital signatures** –It is a message created by user's private key used as authenticity of a user.
- **Encryption** –It converts the plaintext into unreadable format, used to communicate message securely to receiver.

➢ **Security Benefits of Digital Signatures**

The digital signature offers the following benefits.

- **Authentication** –It validates the message or user is legal or not.
- **Non-repudiation** –The message sender does not deny the signature after communication.
- **Integrity** – The signature assures the received message is not altered.

➢ **Security Benefits of Encryption**

The following security benefits are offered with encryption operation.

- **Confidentiality** –The communicated message is encrypted by the public key of receiver such that only the intended user's private key is used to decrypt the message.
- **Integrity** –The encryption process with secured public key assures the received message is not altered.

IV. THE PROCESS OF DIGITAL SIGNING& RESULTS

The following three algorithms are used to develop digital signature.

- ***Key generation*** – Each user generates two keys such as public key and private key. The private key kept at user side and public key is freely available in the network.
- ***Signing*** – Each user can perform signing operation using his/her private key.
- ***Verification*** – The signed signature is verified by the public key of concerned user.

The digital signature created by the private key of a user and hash algorithm. First the message is encrypted by the private key of the user. The encrypted message generates a signature for user after applying the hash algorithm on it.

The public key cryptography with its applications encryption and digital signature prevents the following attacks such as :

- ***Key-only*** – Attacker can easily access the public key of the user.
- ***Known message*** – Attacker can access the private key of the user with the signature.
- ***Adaptive chosen message*** – Attacker can choose the message for the available signature.

V. CONCLUSION

The public key cryptography is considered as the most secure cryptography to create digital signatures and to perform encryption process. The usage of digital signature will be considered as the most secured service in future for on-line communications. Hence, to perform secure online communications the public key cryptography plays an important role in cryptography.

REFERENCES

1. Bruce Schneier, "Applied Cryptography", second ed., John Wiley & Sons, New York, 1996.
2. Anoop MS, "Public key cryptography- Applications Algorithms and Mathematical Explanations", Tata Elxsi Ltd, India,.2008
3. https://searchsecurity.techtarget.com
4. https://www.cryptomathic.com/news-events/blog/what-is-a-digital-signature-what-it-does-how-it-works
5. https://www.securedsigning.com/why-secured-signing
6. https://www.signix.com/blog/bid/103216/top-5-benefits-of-electronic-signature-software
7. https://www.emptrust.com/blog/benefits-of-using-digital-signatures
8. https://en.wikipedia.org/wiki/Public-key_cryptography
9. https://www.globalsign.com/en-in/ssl-information-center/what-is-public-key-cryptography
10. https://www.webopedia.com/TERM/P/public_key_cryptography.html
11. https://tut4dl.com/public-key-infrastructure-pki-digital-certificates-2/