DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.4975

ISSN No. 0976-5697

Volume 8, No. 9, November-December 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

STUDY OF CRYPTOLOGY AND ITS FORMS IN TODAY'S SECURE WORLD

D KALYANI
Information Technology
VNRVJIET
Hyderabad, India

P VIJAY
Computer Science Engineering
DRKIST
Hyderabad, India

Abstract: Nowadays every communication and data exchange has been digitized. So everyone thinks about privacy and security. In this paper, we are highlighting the need for security in daily data transmissions and the role of cryptography in order to handle demands of today's secure world. We study various cryptographic techniques that can be used and applied to our needs. This also initiates the comparison of security level with the other methodologies. There are different cryptographic methodologies available to perform uniquely specified tasks like- encryption, decryption, key agreement and digital signatures. In this paper, we review the study of different encryption schemes and its usage along with different key management techniques and the application of digital signature with its complete operational principle that is used in daily life as a part of secure communication.

Keywords: Cryptography, Digital signature, Encryption, Decryption, Key exchange.

I. INTRODUCTION

Cryptography is a branch of cryptology with abundant tricks for secure transmission over public channel even in the presence of unauthorized entities (adversaries) by encoding the clear content into an unreadable form. In today's computer-centric world, day to day activities from simple mail compose to business transactions and defense secret communications, from card payment to cloud storage the "cryptography" has been playing a critical role at the backend process. Cryptology also paved the platform to measure the level of security processes and to understand various attacks, this is called cryptanalysis. This cryptanalysis sometimes used to gauze the security of algorithms. Cryptography processes are like encryption- scrambling clear text into cipher text and decryption- decoding of ciphertext into clear text [1]. One of the earliest and easiest form of encoding uses various classical methods exist either as "transposition" type - in which each and every letter of clear text is rearranged to get encoded text(cipher) with pre-agreed secret code or "substitution" type -in this individual letters or groups of letters are replaced with another group of letters through some mapping mechanism. This kind of transmission demands super secure channel. As the cryptography is all about designing secure protocols for current needs and analyzing the security strengths with respect to the application demands, So modern cryptography techniques provide confidentiality, integrity, authentication and nonrepudiation to design fully secure information systems in the real world. Modern cryptosystem designs in a broad sense are symmetric-key cryptosystems and public key cryptosystems [1,2]. In addition to these, there are two more critical and important mechanisms of cryptology meeting the needs of today's world. They are - key exchange and digital signatures.

In this paper, we are going to give a study report about Symmetric key cryptosystem, Asymmetric key cryptosystem, Key Exchange and Digital Signatures.

II. RELATED WORKS

A. *Symmetric-key Cryptosystem*

In this process, the communicating entities should use only one key called secret key in encryption and decryption processes. Secret key must be communicated and commonly shared by the entities through some secure private courier or secret mail over a secure channel before the original communication has been taking place.

As shown in Fig. 1, the sender first chooses the clear plain text that he wants to communicate with the receiver and converts it into scrambled form by using some encryption method and shared secret key. The cipher text that is being generated after the encryption is sent via a public channel. Now the receiver applies some decryption method and the same shared secret key to transform the received cipher text into clear plain text form.

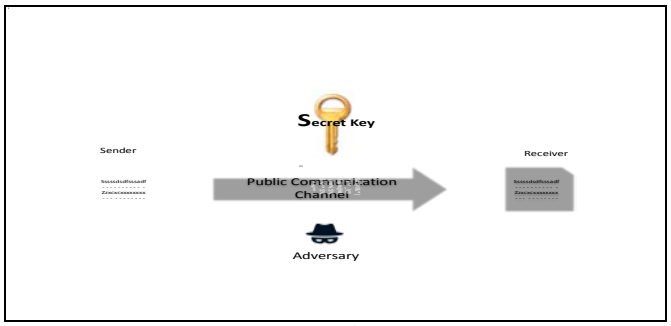

Fig1. Standard structure of secure communication

According to Kirchhoff's [1] principle data security lies with the key that is being used in the mapping but neither with the mapping method nor with the text message. Though symmetric encryption schemes use only one secret key to secrecy, these are simple, highly secure and fast when compared with other modern cryptographic schemes [3]. Also best suitable for repeated communications, But not fit for digital signatures. The Public key crypto system reduces the secret key exchanges to some extent.

B. Encryption & Decryption

Symmetric key encryption and decryption are implemented either as a stream or block ciphers. In symmetric stream ciphers encipherment is done on one bit at a time, whereas in block ciphers it is on a fixed length block of bits (generally block length is multiple of 8). Symmetric block ciphers mostly rely on Horst Feistel [1] cipher structure. Example stream constructions are RC4, CAST5. Most popular block constructions like – DES, 3DES, AES, Serpent, Twofish, Blowfish, Skipjack, IDEA.

Block cipher security further intensified by using different operating modes. They are simple Electronic Code Book mode but can't withstand for guessing attacks, deterministic Cipher Block Chaining mode but error propagation made it weak, interlinked plain text, cipher text based Cipher Feedback mode also has error propagation but has a strange feature that, works like block to stream cipher convertor, Output Feedback mode uses encryption scheme and acts like a key stream generator and Counter mode depend on synchronization of sender and receiver machines.

Symmetric ciphers are used to provide message authentication codes and hash codes but not for non-repudiation. Symmetric ciphers are not secure against Known-Plain text Attack (KPA), Chosen-Plain text Attack (CPA), differential and linear cryptanalysis. The Symmetric crypto system still has great demanded in government, defense and big financial corporation due to its high computational speed and efficient authentication feature than any other latest cryptographic schemes.

C. Asymmetric key Cryptosystem

The cost of hardware is becoming cheap, also the same with computational cryptographic devices which we use in numerous applications. This transformation leads to technologically new and cheap cryptosystems which minimize the key exchanges as that of a symmetric system and provably secure [3]. The public key or 2-key or asymmetric key crypto system is also known as "multiple access cipher". This completely eliminates the need for secret key exchange as in symmetric key crypto system before the actual communication. Asymmetric key schemes rely on hard problems like- considering discrete logarithm problem over finite fields.

Asymmetric key schemes are suitable for open environments i.e., mainly used for securing data in motion. As shown in the Fig. 2., the public key based scheme uses mathematically related and exist as a pair of keys, also known as

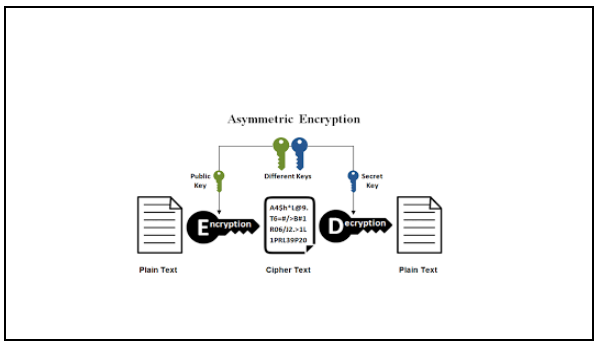

Fig2. Standard Public key based communication system

two keys called public and private keys. To provide security, the message is encrypted and decrypted with public and private keys respectively. Whereas to generate digital signatures, the signer and verifier have to use private and public keys respectively. If there are 'n' no. of entities in the group, then altogether there are n(n-1)/2 no. of keys to be shared over a channel, but it is tedious.

Asymmetric key crypto decryption schemes rely on trapdoor of one-way hash functions. One-way hash functions are feasible to make hash codes in one direction but are hard to invert. i.e., with the knowledge of additional information called trapdoor, the hash functions are inverted easily also well known asymmetric ciphers are – RSA [4], ElGamal [5], ECC [6].

A lot of research in the area of symmetric key cryptosystem has crossed many milestones- Diffie Hellmann [7, 8] public key based key exchange to identity-based public key encryption [9] schemes also in certificate less key issuing [10] and attribute-based encryption methods [11].

D. Key Management

Key management is the most typical and plays a vital role in computer security. Key management involves either manual key exchange or maintenance of the key server. This includes various secure design frameworks and maintenance of keying relationships as shown in the Fig. 3. Different phases of its life cycle include - key generation, key distribution, key storage, backup/recovery and use and key update, replacement, revocation, and destruction in the cryptosystem. The lifetime of a key is determined by data sensitivity, data frequency and key length (in bits). Building blocks for key management are the hash functions, but "Quantum key exchanges" address the problem of the man-in-the-middle attack.

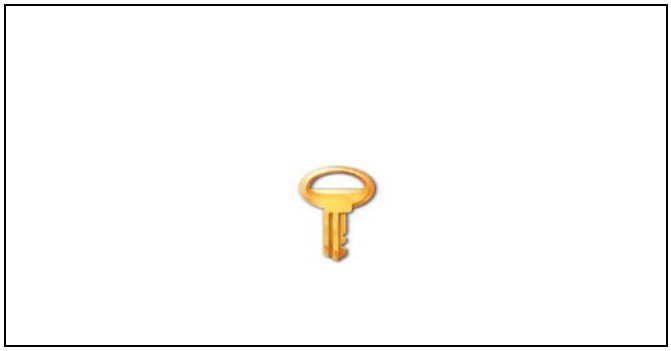

Fig3. Key management structure

Key generation- keys that are being generated by a random bit generator are encrypted with the master secret key and stored in a database with its attributes like key generation time, validity time, its public key, revocation time, key issuer id etc.,

Key storage – This is management of secure backup copy on traditional media –CD, USB. Key can be archived for a long time to stand in a court if necessary, but not for crypto requests. So there is a problem of Non-repudiation with key backup.

Key distribution – In case of symmetric keys, the traditional key distribution techniques, such as telephonic or meeting personally are allowed. With the advent of the public key crypto system this has been changed and today one can send a key over a secure channel by encrypting them with a public key.

Key use – allowing the activated key, accessed from an authorized party. Nowadays attacks are targeting for key

management in public key systems rather than cryptographic algorithms.

In general key exchanges, may takes place either at two users or one user and system. Manual exchange of key via non-electronic medium is very slow and inefficient. Alternatively, the symmetric key exchange can generate its own key and distribute it by a trusted party, called Key Distribution Center (KDC). Most generally used secure key exchange scheme is Diffie W., Hellman [7, 2] though there is a possible man-in-the-middle attack. Also, it doesn't provide authentication.

Public Key Infrastructure (PKI) holds the responsibility of identification of public keys and its distribution to the intended entities when they request for. But this demands a secure channel and an additional master key to encrypt session keys. The secret key that is shared or mutually pre-agreed upon should be sent beforehand through some other mechanisms, like public key cryptosystem. In public key system, key management is simpler with enhanced functionality and cease of KDC. Key exchange agreement protocols designs have been transformed from certificate based schemes to certificate-less authentication schemes [12] and identity-based key agreement protocols [13, 14, 15] to minimize the number of key exchanges.

There are few more proprietary key management schemes like- Thales Key Management, Oracle Key Manager, Bell ID Key Manager and many more; a few open source key management schemes like- Kee, Kmc-Subset137, KeyBox and more.

E. Digital Signatures

Now a day's document signature means either handwritten or image. In case of secure and efficient digital communications for the past handwritten signature or stamped seal practices, the digital signatures are best. A Digital signature is a numerical code based on some mathematical schemes intended to provide authenticity, integrity, and non-repudiation to address the problem of tampering and impersonation. In e-business, the validity of contracts is assured through digital signatures and also stands in a court as a proof of evidence in case of legal disputes. This signature directly connected with the message, so it gives assurance of evidence to origin, genuine identity and status of digital documents or digital transactions by acknowledging entity. This also assures regarding changes made to the document can't go undetected. These are used especially in the distribution of software, contract agreements and other financial transactions transmitted over the internet. Digital signatures are also used for validating public keys being used in public key cryptosystem [4].

Nowadays, with exceptional growth of e-commerce and digitization digital signatures give assurance to the origin as well as the acknowledgment of transactions by playing a vital role. Throughout the world in countries like the USA and the European Union, "Digital signatures" are considered to have much legal significance than the traditional one. According to the science of cryptology, authentication can be implemented with certificates, whereas certificates are implemented through digital signatures.

1) Operational Principle**:** Digital signatures are built with public key cryptography (asymmetric) [4]. Using any public key method, one can generate two keys. i.e., both public and private keys, but they are mathematically related to one another. As the public key schemes are slow and demand much computational power in terms of processor, a signature is generated on hash codes of the original message instead of a direct message. The complete standard structure for digital signature generation and verification is as shown in Fig. 4.

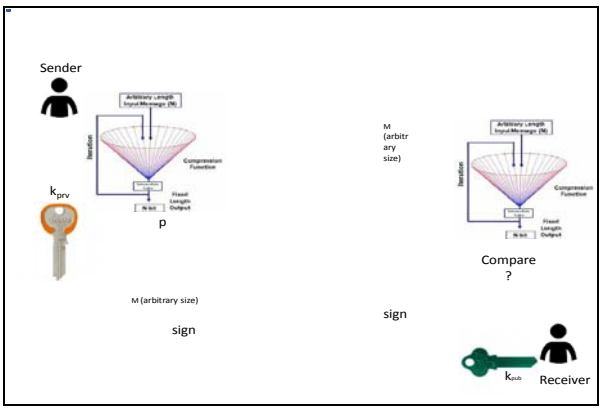

Fig4. Standard structure for Digital Signature

A signature scheme is defined as a set of following three probabilistic polynomial time algorithms, as follows:

Key-Generation (G): This generates a pair of public key and private keys ($\mathbf{k_{pub}}$, $\mathbf{k_{prv}}$) on input $\{0,1\}^*$.

Hashcode Generation: This is a probabilistic polynomial time map function from $\mathbf{\{0,1\}^* \rightarrow \{0,1\}^n}$ to improve the efficiency of the scheme. This converts a string, **p** of any size to a fixed size, **n**.

Signature Generation (S): Gives out a signature, **Sig** by encrypting an input string, **p** with the private key, $\mathbf{k_{prv}}$.

Verification(V): Anyone who knows the public key of the signer can check that the signature is accepted or rejected upon receiving the inputs- the $\mathbf{k_{pub}}$, a string, **p**. i.e., After hashing, the **p** must match with the decrypted hash code by k_{pub} received by the signer to prove that no tampering is done to the original content.

We say that this is secure if for every non-uniform probabilistic polynomial time adversary, *A* the following condition is get satisfied.

$$\Pr [(k_{pub}, k_{prv}) \leftarrow G(1^n), (p, t) \leftarrow A^{S(kprv, \cdot)}(k_{pub}, 1^n), x \notin Q, V(k_{pub}, p, t) = accepted] < \text{negl}(n),$$

where $A^{S(kprv, \cdot)}$ denotes that *A* has access to a signing oracle $S(k_{prv}, \cdot)$, and *Q*: set of the queries made by adversary, A for *S* which knows the public key, *pk*, and the security parameter, *n*.

There are various Certification Authority (CA) agencies to issue digital signature certificates to authorized registered entities. They can approach either e-mudrd, tcs-ca, idrbtca or nic certifying authorities to get digitized ones.

III. CONCLUSION

In this paper, we review main cryptographic branching schemes and protocols used in today's communication world for secure email transmissions with numerous encryption methods based on either symmetric key or public key while

completely eliminating the certification authorities and reducing the key pair generation and generation of signatures and verification methodologies for integrity during its transmission.

IV. REFERENCES

[1] D. Kahn, The Codebreakers, The Story of Secret Writing. Weidenfeld and Nicolson, London, New York: Macmillan, 1967.

[2] Diffie W., Hellman M. E.,"New directions in Cryptography" IEEE Transactions Information Theory,Vol. 22, no. 6 (1976), pp. 644-654.

[3] Yogesh Kumar, Rajiv Munjal, and Harsh, "Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures", Volume 1, Issue 6, June 2014, IJAFRC, ISSN 2348 – 4853.

[4] Rivest, R. L., Shamir, A., Adleman, L.,"A method for obtaining digital signatures and public-key cryptosystems" ACM Communications, Vol. 21, no. 2 1978, pp. 120-126.

[5] T ElGamal A public key cryptosystem and a signature scheme based on discrete logarithms IEEE Transactions on Information Theory, 31 (4) (1985), pp. 469-472.

[6] Koblitz, N.(1987), "Elliptic curve cryptosystems", Mathematics of computation, Vol.48, No.177, pp.203-209.

[7] W. Diffie and M. E. Hellman, "Multiuser cryptographic techniques," presented at National Computer Conference, New York, June 7-10, 1976.

[8] Daniel RL Brown, Robert P Gallant, "The static Diffie-Hellman problem", *IACR Cryptology ePrint Archive*, 2004/306.

[9] Kalyani, D, Sridevi. " Survey on identity-based and hierarchical identity based encryption schemes", Vol.134,No.14, January 2016, IJCA, pp 32-37.

[10] D. Catalano, D. Fiore, R. Gennaro Certificateless onion routing In Proceedings of the 16th ACM Conference on Computer and Communications Security (New York, NY, USA), CCS '09, ACM, pp. 151–160 (2009).

[11] V. Goyal, O. Pandey, A. Sahai, B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", *ACM conference on Computer and* CommunicationsSecurity, pp. 89-98, 2006.

[12] He Debiao, Padhye Sahadeo, and Chen Jianhua. An efficient certificate less two-party authenticated key agreement protocol"Computers & Mathematics with Applications, 4(6):1914–1926, Sep. 2012.

[13] D Kalyani, R Sridevi, "Robust distributed key issuing protocol for identity-based cryptography", ICACCI- 2016, pp. 821-825, IEEE conference publications.

[14] S. H. Islam and G. P. Biswas. A more efficient and secure id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Journal of Systems and Software, vol. 84, no. 11, pp. 1892–1898, 2011.

[15] Mohammad Sabzinejad Farash, Mahmoud Ahmadian Attari, "An ID-Based Key Agreement Protocol Based on ECC Among Users of Separate Networks", 2012 9th International ISC Conference on Information Security and Cryptology,978-1-4673-2386-4/12,2012 IEEE.

