I J C T A, 10(8), 2017, pp. 559-565 ISSN: 0974-5572
© International Science Press

Comparative Study of Cryptography and Secret Sharing

Priya Potnis* **and Sonali Patil***

ABSTRACT

Today everything in the world is becoming digital. We are dependent on the Internet for various activities like shopping, banking and transferring information as well as funds etc. Information has become an important asset in the digital world. With such an enormous usage of the Internet for sharing information and making monetary transactions, there is a need for safe and secure environment. Cryptography is an ancient and a well-known technique that provides secure communication over the network. It provides privacy and authenticity to the information exchanged over the Internet. Secret sharing is another cryptographic technique used in the recent years which encodes secret information into a group of users. Each user will receive a single share from the secret message. The complete secret can be regenerated only when some specific shares are combined together. A single share is of no use. This paper presents a comparative study of Cryptography and Secret Sharing methodologies and techniques which will help to understand the utilities of both approaches for specific applications.

Index Terms: cryptography, secret sharing, symmetric key, asymmetric key, threshold, proactive, verifiable, access structure.

1. INTRODUCTION

A lot of information is exchanged over the internet today. We use the internet for personal as well as business needs. Internet has become an essential part of our daily routine. Everything is becoming available to everyone as the Internet is open and accessible to all. Hence, it is very important to protect sensitive data or information communicated over the internet. There are numerous attacks that can be performed to retrieve secret information communicated over the internet. Suppose you make some online shopping and choose to make the payment online, you would need to provide the details of the debit/credit card while making the transaction. If unfortunately this information is hacked, then it wouldn't be good news to hear. Hence, it is very important to secure such critical and sensitive information.

If two users want to exchange a secret message over the internet, care should be taken that this message should not be leaked to the third party. The study and practise of different techniques for hiding the sensitive information from third party is called as Cryptography. Cryptography is used to provide security to a wide range of applications where the data is to be exchanged securely and kept hidden from any third party users. The examples include securing computer passwords, ATM card details, electronic transactions and many more day-to-day examples. Cryptography is a simple process where the secret message or the sensitive information (plain text) to be transferred between two users is encrypted into unintelligible message (cipher text). On the receiver side a decryption method is to be applied that converts the unintelligible message to the original intelligible plain text. There are numerous well-known algorithms for converting the plain text to cipher text.

Secret sharing is another methodology used for securing the data that is to be communicated between different users over the internet. The secret message to be exchanged between the users securely is split

* Department of Computer Engineering, PCCOE, Pune University, *Emails: priyapotnis322@gmail.com, sonalimpatil@gmail.com*

into a number of shares. These shares are transferred individually over the internet. At the receiver end, the secret message can be reconstructed by combining a few shares out of the total shares. Individual share is of no use to the receiver.

The cryptography approach is very popular among the researchers and developers. Along with the cryptography, secret sharing also plays a vital role in providing high security to the confidential data. This leads to the need of understanding the difference between the different techniques and applications of Cryptography and secret sharing. This paper presents a clear understanding of these two methodologies, cryptography and secret sharing. This study helps to understand various pros as well as cons of the techniques used and decide which method will be more appropriate to provide security for any given application.

The rest of the paper is arranged as follows: Section II briefly presents the literature survey on cryptography and secret sharing and different techniques under these methods. Section III discusses and compares both the methodologies on various parameters. Section IV summarizes the paper.

2. LITERATURE SURVEY

This section discusses the techniques of securing critical information and sensitive data with Cryptography and secret sharing.

2.1. Cryptography

The process of scrambling the contents of a secret message to keep it secure from the outside world is called the process of Cryptography. It consists of two parts: Encryption and Decryption. Encryption is the process where the secret message is scrambled in such a way that it is difficult for an adversary to understand. Decryption is the process where the scrambled message is reconstructed to retrieve the original message. The encryption process and the decryption process is done with a parameter called “key”. Depending on the key, the cryptographic techniques are divided into two classes: symmetric key cryptography (SKC) and asymmetric key cryptography (AKC). For the symmetric key cryptography, the same key is commonly used for both the encryption (by the sender) and the decryption (by the receiver) process. In the asymmetric key cryptography, one key is used for the encryption process and another mathematically related key is used for the decryption process. Hash function is also a technique of cryptanalysis. [3]

2.1.1. Symmetric Key cryptography

Symmetric key cryptography (SKC) sometimes called as shared or secret key cryptography (as the same key is commonly used by both the users) is very simple and easy method for securing the information to be communicated, but managing the key is tedious task. For secret-key cryptography technique, the same key is used for encrypting and decrypting the sensitive information. If the key is lost or compromised to an adversary, the information would be easily retrieved from the encoded text. The key is required to be securely communicated to both the sender and receiver. There are a list of algorithms for symmetric key cryptography like AES, DES, 3DES etc. With the passing years, a lot of improvements were made to the traditional method of symmetrics key cryptography to provide more security to the critical information. [3][4]

An enhancement to the traditional symmetric key cryptography can be used by taking the plain text at bit-level which will provide more security than individual characters. A pattern is decided and the key is also generated by the bits generated from the plain text. The binary text and the key are XORed to form the cipher text. The cipher text is then converted to characters and sent to the receiver. At the receiver end, the cipher text is converted into binary format. The key is extracted according to the decided pattern. The encrypted bits are XORed with the key to retrieve binary bits. These binary bits are then converted to characters to read the original plain text message. [1]

Another algorithm of symmetric key cryptography that works with ASCII characters for encryption and decryption. For encryption, it is a three level process: first convert all characters to upper case letters and then convert the even blanks to $ and odd blanks to #, in the next step switch alphabets to its complementary alphabets (A ->Z and B ->Y and so on) and in the last step for each second alphabet which is not blank the value n is calculated with the given formula:

$$n = ASCII\left(char\right) \text{ and } n = n + \left(key\right)^{L}$$

and then append the original character to the encoded text. For the decryption process, the receiver will first convert the cipher text to upper case characters to extract each character. For the odd characters, replace it with its complementary alphabets. For even characters and if the character is not '$' or '#', subtract a value of $(key)^{L}$ from the number obtained and then typecast the received value into character and append the decoded text sequence. Lastly, if the character is a '$' or '#' then append a blank space to the decoded message. [2]

Securing the key is a very important factor. Symmetric key cryptography assumes that the keys are prior distributed to the users through secure communication channels. If the key is lost, it is very easy for an adversary to get the original message from the decoded text. There are different key-management techniques that help to protect the key from an attacker. Asymmetric key cryptography is an extension to the symmetric-key cryptography.

2.1.2. Asymmetric key cryptography

For this technique i.e. asymmetric-key cryptography (AKC), two keys are available for the encryption and the decryption process instead of an single key that was shared previously between the sender party and the receiver. Both the parties that mean the sender and the receiver possess a pair of keys – a private or the secret key and the public key. The public key is used for encryption and the secret key will be used to decrypt the scrambled text. It allows a secure communication between the users as the secret key is never shared and retained at the sender side. There are different algorithms for asymmetric or public key cryptography like the Diffie Hellman, RSA and many more. [3][4]

In the recent years, there is much advancement to the traditional asymmetric key cryptography. The RSA algorithm is likely to have an attack on the mathematical factorization. The enhanced RSA algorithm can be explained as follows:

1) Key generation:

- take two randomly generated prime numbers α and β and calculate the value of n as:

$$n = \alpha \times \beta$$

- Next calculate the value of $\phi(n)$ as:

$$\phi\left(n\right) = \left(\alpha - 1\right) \times \left(\beta - 1\right)$$

where ϕ is the Euler's function.

- calculate the value of $k1$ such that:

$$\sqrt{n} < k1 < \phi\left(n\right) \text{ and gcd } \left(k1, \phi\left(n\right)\right) = 1$$

i.e. $k1$ and $\varphi(n)$ are co-prime.

$k1$ must be short and have a negligible hamming weight.

- compute X to replace n in the following way:

i) if $\alpha > \beta$, consider X as:

$$n - \alpha < X < n, \quad gcd(X, n) = 1$$

ii) if $\alpha < \beta$, consider X as:

$$n - \beta < X < n, \quad gcd(X, n) = 1$$

Find $k2$ such that $k1 \times k2\ Mod(X) = 1$

- The public key now *is* ($k1$, X) and the private key is ($k2$, X).

2) Encryption Process:

- Now encrypt the plaintext message *PM* to cipher message *CM* as:

$$CM = PM^{k1}\ mod(X)$$

3) Decryption Process:

- For decryption, get the plaintext message *PM* from cipher message *CM* by applying the formula:

$$PM = \sqrt{}\ (CM^{k2}\ Mod(X))$$

This process gives better security by eliminating the value n from the original RSA algorithm. [5]

2.1.3. Hash Functions

Using hash functions is also one way of cryptanalysis. There are many algorithms that use hash function to provide security to the critical messages like the SHA, MAC etc. The hash functions take variable size input and convert it to a fixed size output. The keccak SHA-3 algorithm implements basics of hash function to provide security. It includes padding and permutation. Padding is done to make the input of a fixed size and then permutation is applied on a single block of input. The process is reworked for full set of input blocks. Permutation involves XORing of the input block with the output of the padding module. Permutation process is replicated for all input blocks. This method requires less memory and provides better security when compared to the original hash algorithms. [6]

2.3. Secret Sharing:

Secret Sharing (SS) is a technique in which secret information, which can be in the form of data, image or an audio file is transferred in the form of shares. The individual share itself does not disclose any information about the secret message. For the reconstruction of original secret a threshold number of shares are needed. The shares are then mingled and connected together to form the original secret. This method helps in addressing the problem of reduced trust. Visual cryptography is also a kind of secret sharing in which the secret message can be reconstructed by stacking the shadows. These techniques are having very low computational complexity. Secret sharing techniques can be used in variety of ways as per the need of the application. The various types of secret sharing schemes are: threshold SS, proactive SS, verifiable SS and access structure SS. [7][8]

2.3.1. Threshold Secret Sharing

In the threshold SS method, threshold is a parameter which decides the minimum number of shares needed for the reconstruction of original secret. This technique is used in situations where a group of participants which rely on each other but cannot trust the other individual completely. They are commonly called as (t, n) secret sharing techniques, where $2 <= t <= n$, where at least t or more participants out of total n participants must cooperate to get the original secret. Less than t participants cannot regain the original message. This is very useful in terms of reliability as though any t number of shares is available the original secret can be reconstructed. [9]

2.3.2. Proactive Secret Sharing

Proactive secret sharing are useful where the participants involved in keeping the shares may get added or removed from the participants group. Also the shares need to be refreshed without changing the original secret after some time duration. This technique can be used for applications that need to maintain data for an elongated time period. This provides the security from the threats of an adversary trying to get shares one by one. [10] [11]

2.3.3. Verifiable Secret Sharing

While receiving share of the secret information, participant may need to verify the accuracy of the provided share. And also, among the group of participants dishonest participants can provide fake shares at the time of reconstruction of the secret. Verifiable secret sharing techniques are very important in identifying such dishonest participants or cheaters. [12][13]

2.3.4. Access structure

This type of secret sharing is also known as general access structure secret sharing. It is useful in providing flexibility in terms of deciding specific participants to reconstruct the secret. It gives a subset for the authorized users to access the required capabilities. For getting the original secret the reverse method is applied on the qualified subset of shares. The shares that did not qualify will not reveal any part of the information. [14][15]

Thus a lot of study has been there by the researchers in the field of secret sharing and cryptography. The next section provides the comparative analysis of these two techniques with respect to the parameters like security, reliability, bandwidth requirement etc.

3. COMPARATIVE ANALYSIS

The following section compares both the techniques on various parameters to ensure the usability of the techniques.

Cryptography methods require an extra parameter as key for the encryption and the decryption process. Without the key, the data cannot be encrypted or decrypted. Hence, the key plays a very essential aspect in Cryptography. But in the case of Secret Sharing, there is no requirement of keys for creating shares from the secret. Also in case of symmetric key cryptography, if the key is lost, the message can be decrypted easily. For this reason it is very important to protect the key from the malicious attackers. It must be ensured that the keys are always communicated through secure channels. The asymmetric key cryptography makes use of a key-pair: the public key and the private key, if the private key is stolen then the secret message can be easily compromised. This will not happen in case of secret sharing as they do not use keys. Due to this, secret sharing is more flexible than cryptography. Secret sharing technique can sustain attacks up to their threshold value of $(n - k)$ where n is the number of participants and k is the threshold value whereas cryptography has a single point failure i.e. the keys. If the key is attacked, the secret message is compromised to the attacker. As cryptography has a single point failure, its reliability is less as compared to the SS scheme. But in the SS technique, the secret message is divided into a number of shares. This leads to increased bandwidth for communication compared to cryptographic techniques. Also, the space complexity is more in secret sharing. Cryptography involves a lot of computations like permutations, transpositions and mathematical and logical operations to be performed on the original text message which increases the computational complexity of the algorithms as compared to the secret sharing methods. The following table gives a systematic representation of the comparison of different parameters with respect to Cryptography and Secret Sharing.

Table 1
Comparison of Cryptography and Secret Sharing techniques.

Parameters	*Cryptography*	*Secret Sharing*
Key Required	Yes	No
Single Point Failure	Yes	No
Security	Yes	Yes
Flexibility	No	More
Accuracy	More	More
Effect of Attack	Single Point Failure	Can be sustained up to $(n - k)$ attacks
Reliability	Less	More
Threshold	No	Yes
Techniques	Symmetric, Asymmetric, Hash Function	Threshold, Proactive, Access Structure, Verifiable
Entropy	More	Less
Bandwidth	Less	More
Space Complexity	Less	More
Computational Complexity	High	Comparatively Less

4. CONCLUSION

Cryptography and secret sharing are playing very vital role in providing the security to the important information. This paper elaborates on both approaches in detail. It is very useful in making the understanding of cryptography and secret sharing in more clear way. Also, the paper presents a relative comparison of Cryptography and Secret Sharing techniques with respect to the concerned parameters, which is helpful to understand the utilities of both approaches for specific applications.

REFERENCES

[1] Omkar Kassem Khalil, Aissa Boudjella, “An Enhanced Cryptographic Technique for Messages Traveling between Computers”, Sixth International Conference on Developments in eSystems Engineering, pp. 239-242, (2013).

[2] Abhishek Anand, Abhishek Raj, Rashi Kohli, Dr. Vimal Bibhu, “Proposed symmetric key cryptography algorithm for data security”, First International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), pp. 159-162, (2016).

[3] Jean-Sebastian Coron, “What is cryptography?”, IEEE Journal on Security and Privacy, Vol. 4, Issue 1, pp. 70-73, (2006).

[4] Sourabh Chandra, Smita Paira, Safikul Alam, Dr. Goutam Sanyal, “A comparative survey of symmetric and asymmetric key cryptography”, International Conference on Electronics, Communication and Computational Engineering (ICECCE), pp. 83-93, (2014).

[5] Rohit Minni, Kaushal Sultania, Saurabh Mishra, Durai Raj Vincent, “An Algorithm to Enhance Security in RSA”, Forth International Conference on Computing Communication and Network Technologies (ICCCNT), pp. 1-4, (2013).

[6] Madhura A. Patil, Pradeep T. Karule, “Design and implementation of keccak hash function for cryptography”, International Conference on Communication and Signal Processing (ICCSP), pp. 0875-0878, (2015).

[7] Sonali Patil, Prashant Deshmukh, “An Explication of Multifarious Secret Sharing Schemes”, International Journal of Computer Applications (0975-8887), Vol. 46 – No.19, pp. 5-10, (2012).

[8] Sonali Patil, Prashant Deshmukh, “Analyzing relation in Application semantics and extended capabilities for Secret Sharing Schemes”, International Journal of Computer Science Issues (IJCSI), Vol. 9 , Issue 3, No. 1, pp. 219-226, (2012).

[9] Sonali Patil, Prashant Deshmukh, “A Novel (t, n) threshold Secret Sharing using Dot product of Linearly independent Vectors”, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 2, Issue 7, pp. 2521-2524, (2013).

[10] Sonali Patil, Prashant Deshmukh, “A Proactive Secret Sharing in Dot Product of Linearly Independent Vectors”, International Conference on Recent Trends in Information, Telecommunication and Computing, pp. 199-206, (2014).

[11] Sonali Patil, Nikita Rana, Dhara Patel, Prajol Hodge, "Extended Proactive Secret Sharing using Matrix Projection Method", International Journal of Scientific & Engineering Research (IJSER), Vol. 4, Issue 6, pp. 2024-2029, (2013).

[12] Sonali Patil, Sandip Sathe, Pravin Mehetre, Deepak Shinde, Kiran Bhalerao, Pawankumar Pandey, "Secure and Verifiable (2,2) Secret Sharing Scheme for binary images", International Journal of Computer Science Issues (IJCSI), Vol. 10, Issue 1, No. 2, pp. 290-293, (2013).

[13] Sonali Patil, Prashant Deshmukh, "Verifiable Image secret sharing in matrix projection using watermarking", International Conference on Circuits, Systems, Communication and Information Technology Applications (ICSCITA), pp. 225-229, (2014).

[14] Prashant Deshmukh, Sonali Patil, "General Access Structure Secret Sharing in Matrix Projection", International Journal of Computer Applications (IJCA), Vol. 107, Issue 13, pp. 6-9, (2014).

[15] Sonali Patil, Kapil Tajane, Janhavi Sirdeshpande, "General Access Structure for Modulo-2 Secret Sharing Scheme", International Journal of Engineering Research and Technology, Vol. 1, Issue 8, (2012).