International Journal of Scientific Engineering and Science
Volume 1, Issue 12, pp. 58-60, 2017. ISSN (Online): 2456-7361

Cryptography and Related Techniques

Nitish Arora[1], Pankaj Goel[2], Akshay Sehgal[3], Dr. Shaveta Bhatia[4]
[1, 2, 3]Student, FCA, MRIIRS
[4]Associate Professor, FCA, MRIIRS

Abstract*—Securing information includes various approaches in order to protect and mitigate threats that can cause severe damage to precious information and resources which are available all over the internet and computer systems. Cryptography is a technique utilized to secure personal data by encoding it and protecting it by giving authorized and secure access there by ensuring safety. This paper explores various new technologies like circular encryption, password based cryptography. In addition, this paper will dive deep into cryptanalysis and its applications*.

***Keywords*—** *Cryptography, symmetric key, asymmetric key, cryptanalysis, password based encryption, salt.*

I. INTRODUCTION

Connectivity offers amazing benefits as vast population is shifting online. Because of the need for connectivity, businesses have to operate online and grow in new areas. This causes the data and assets to become vulnerable and the need for securing and protecting comes into play. Imagine a world where our texts, emails, our calls are all subject to recording and being a matter of public data. Would we ever feel comfortable performing in exchange of information? Use of cryptography is a great choice to safeguard our data.

Cryptography is the combination of two words CRYPT (Secret) and GRAPHEIN (to write). It is the art of writing the data secretly. Cryptography is the study and application of techniques to secure communication from the outer world. It is necessary in order to maintain data confidentiality, data integrity and authentication. Cryptography enables you to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. For example, unapproved access and utilize, misappropriation, change, and obliteration.

Also shown in the paper is Cryptanalysis which is a technique the involves the analysis of the hidden aspects of the system. This can recognize the pattern and help find weakness in encryption.

This also covers technique of Circular encryption. When data is dependent on the keys are used more often then this type of encryption is helpful.

Some people choose passwords that are not strong or can be easily guessed that leaves data open to threats and hackers can smoothly temper or destructs the data. For this purpose Password Based Encryption comes into play. It produces key bytes that are random and unpredictable.

II. CRYPTOGRAPHY

Cryptography refers to the science and art of transforming message to make them secure and free from attacks. Cryptography provides confidentiality, integrity, authentication, and non-repudiation of messages. It is the change of intelligible and reasonable information into a shape which can't be comprehended so as to secure information.

Cryptography alludes precisely to the procedure of hiding the substance of messages, the word cryptography originates from the Greek word "Kryptos", that implies covered up, and "graphikos" which implies composing. Cryptography is the exploration of utilizing science to encode and decode information.

Modern cryptography methodologies have their existence in the different disciplines which include mathematics, computer science, and electrical engineering. Applications of cryptography have their existence in different sectors and areas like military communications, electronic and electrical commerce, Automated teller machines cards, computer passwords and many others.

Types of Cryptography:

A. Symmetric key cryptography

In Symmetric key Cryptography same key is used for both encryption and decryption. It's very fast technique of encryption and decryption. The size of the encrypted text is usually the same or less than the plain text.

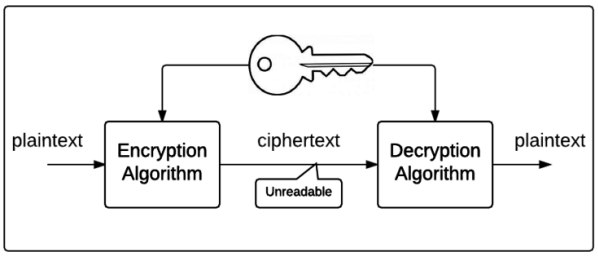

Fig. 1. Symmetric encryption & decryption.

B. Asymmetric key cryptography

In Asymmetric Key Cryptography one key is used for encryption and another key is used for decryption. It is slower than Symmetric cryptography. The size of the cipher text generated in this scheme is more than the plain text.

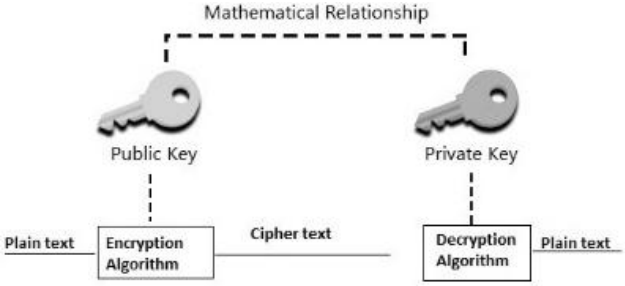

Fig. 2. Asymmetric encryption and decryption.

Volume 1, Issue 12, pp. 58-60, 2017. ISSN (Online): 2456-7361

III. CRYPTANALYSIS

It's the study of analyzing information system in order to study the hidden aspects of systems. It deals with finding the encryption key for breaking cryptographic algorithm without knowledge of the encryption. Cryptanalyst means a person who breaks codes of cryptography and it is also known as intruder. It may also try to recognize pattern, find weakness in the encryption. There are three main line attacks which are:

A. *Ciphertext-Only Attack*

Cipher text attack is an attacking technique where the attacker has the knowledge or access of only the set of chiphetexts .If the information or plain text can be deduced from the ciphertext or the key itself then the attack is successful. Information of any amount obtained from ciphertext is a success.

B. *Known-Plaintext Attack*

Known plaintext attack model is an attacking technique where attacker has knowledge or access to both plaintext (crib) and its corresponding ciphertext. All this can be used to discover further important information say secret keys, code books. It's used sometimes by hackers to see their progress by matching the plain text with their decoded text and get an idea if they are on the right track.

C. *Chosen-Plaintext Attack*

Chosen plaintext attack model is an attacking technique where attacker chooses the random plaintexts in order to obtain the corresponding ciphertexts. Goal of the attacker here is to gain important information that reduces the security applied in the encryption algorithm. It is further divided into two types:

- *Batch Attack* – It's an unprofessional type of attack where the cryptanalyst chooses all the plaintexts before it is encrypted
- *Adaptive Attack* – It's a professional type of attack where the cryptanalyst chooses only succeeding plaintext.

Brute Force Attack

It is a cryptanalytic attack which can be used to decrypt any of the encrypted data. It is a trial and error type hacking. The attacker tries many passphrases in order to find or guess the correct password. The attacker can also try to guess the key which generates from the password by utilizing key derivation. It's called exhaustive key search. This works for shorter passwords very well. Longer passwords takes long time so they require another method known as dictionary attack. The amount of time to decode depends on the length of the password.

IV. SECURITY

Computer security uses a shield to secure information from robbery or being hacked. It's a significant portion of organizational budget is spent on man aging information. These have several security related objectives like confidentiality (secrecy) and integrity means protect information value and accuracy.

Network security use implies a need for automated tools for protecting files and other information. The use of networks and communications facilities for carrying data between users and computers is also growing. Network security measures are needed to protect data during transmission.

Various techniques of cryptography can be used of which some are mentioned in this paper. They provide pretty good protection against online threats.

V. PASSWORD BASED ENCRYPTION

Encryption calculations can be separated into two unmistakable classifications: symmetric and uneven. These are likewise regularly alluded to as ordinary and open key encryption calculations. Regular encryption utilizes a similar key for both encryption and unscrambling.

These protocols are designed as to be secure in the situation where the secret key and password that is shared between two users is extracted from a set of values that is very small. But some protocols are vulnerable because they tend to be in category of guessing attacks and have risk of revealing password in the online conversation.

As the passwords chosen by users are weak they can be broken by brute force attacks by breaking security of encryption.

It's a Symmetric encryption procedure where the keys are passwords and key generation is a password sampling algorithm.

A. *Salt Generation*

The salt is a random number which is used as an addition to the encrypted password, in order to make difficult for the intruder to hack into the system and guess the password through brute force attack scheme. It can be generated by two ways.

- It can be done using a cryptographic random number generator for example Yarrow and Fortuna.
- The other way of generating the salt is by computing salt by using the Key Derivation Function S=KDF

(Q, M) Where Q is the passphrase and M is plaintext message. Of the steps mentioned, step no. 1 is preferred method of salt generation, however in certain cases where the random number generator is not available method no. 2 will provide sufficient security.

The important element of the Password based encryption is shown in figure:

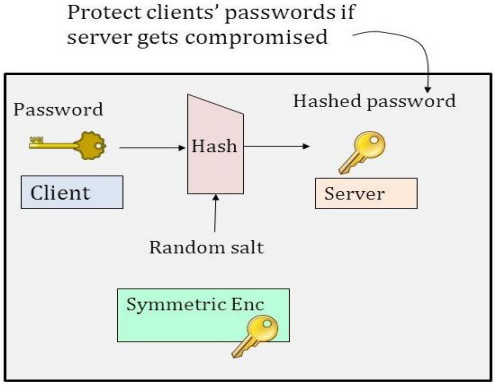

Fig. 3. Use of salt generation.

B. Iteration Count

Iteration count uses fixed number C with PRF (Password Random Function). Iteration count will increase the cost of producing keys from a password. As the number of iteration increases, the cost of exhaustive search for passwords increases. The minimum of thousand iteration is recommended.

VI. CIRCULAR ENCRYPTION

Circular encryption system is safe even when encrypting data which are dependent on the keys that are oftenly used. Especially it remains safe under the ''key cycle" utilization. When we have the period of private pairs (pk,sk) for i=1……n, and encrypt sk .

Sometimes situation arised in key-management systems are related to anonymous credential systems. Also, safety regarding key cycles plays the role related to saint security of protocols which are used in encryption to figure out the security of robust instantiations of protocols.

The existing encryption system is secured when keys cycle are present was extensively used till date. On one hand we had no any invention that satisfy the notion of security on the other hand there is no any examples of secured encryption system that behaves like apparently insecure in the presence of key cycles. Here we make an encryption system which is more secured than plaintext attacks under the decision assumption.

VII. CONCLUSION

Cryptography ensures that the precious data is confidentially transmitted and could not be tempered by anyone trying to hack the data. It means unauthorized person cannot understand the message received and play with it or temper it. Only the person who has the decipher key can decode the message. There are various terminologies discussed which are used for different purposes depending on the type of data used. Password based encryption is used where simple and vague passwords which are very easy to guess are used. It has 2 methods salt generation and iteration count. Also discussed above is Circular Encryption which safeguards the data that depends on oftenly used keys. Cryptanalysis can be used to break security of cryptographic systems. This paper is all about security and how to remain safe in an world which is online and interconnected.

ACKNOWLEDGEMENT

This work has been possible under the knowledge of Dr. Prasenjit Banerjee and Dr. Shaveta Bhatia. We are sincerely thankful to them for their efforts and assistance.

REFERENCES

[1] Management, Enterprise and Benchmarking Century, Budapest, 2017.
[2] L. Gong, M. A. Lomas, R. M. Needham, and J. H. Saltzer, "Protecting poorly chosen secrets from guessing attacks," *IEEE Journal on Selected Areas in Communications*, vol. 11, issue 5, pp. 648–656, 1993.
[3] D. P. Jablon, "Strong password only authentication key exchange," *ACM SIGCOMM Computer Communication Review*, vol. 26, issue 5, pp. 5-26, 1996.
[4] S. Kumari, "A research paper on cryptography encryption and compression techniques," *International Journal of Engineering and Computer Science*, vol. 6, issue 4, pp. 20915-20919, 2017.