Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 6, May-2019, ISSN 2230-7540

A Research on Multilevel Encryption Process through Multiple Symmetric Keys

Sudesh Kumari*

Master of Technology, OPJS University, Churu, Rajasthan

Abstract – In an increasingly connected world, cryptography has become an essential component of the modem information systems. The emergence of the internet as a trusted medium for commerce and communication has made cryptography an essential component. The term cryptography is derived from the Greek language using the words krytos representing secret and graphos representing writing. As per Britannica Encyclopedia, cryptography is defined as practicing of the enciphering and deciphering of messages in secret code and renders them unintelligible to all except the intended receiver. As per Columbia Encyclopedia, cryptography is defined as the Science of secret writing. Cryptography is an art of using mathematics to encrypt and decrypt data. Cryptography converts vital data into secret code on transmission over public network. The original text or plaintext is converted into a coded equivalent called clear text via an encryption algorithm. The clear text is decrypted at the receiving end and converted into plaintext.

There are many algorithms or ciphers in use today. The cryptographic algorithms use a "key" which is a binary number with 40 to 1024 bits in length. The greater the number of bits in the key (cipher strength) leads for greater key combinations and longer time to break the code. The data are encrypted or locked by combining the bits in the key mathematically with the data bits using mathematical principles.

----------X----------

INTRODUCTION

With the expansion of the Internet and the growth of electronic commerce, cryptography has become critical to business transactions and legal exchanges. The Internet has made the transfer of data easy and has become an everyday part of our lives. Computers allow us to store and transmit data with ease. Data storage takes up much less space than a filing cabinet and data can be transmitted almost instantaneously using the Internet. The ease and speed of data transfer have led to the development of faster and bigger systems to handle large amounts of data. Some of these data is private and contains information that is only to be read by certain individuals. Also critical information are transmitted over the Internet. This information should be protected from unauthorized eyes. To achieve this goal, encryption is the technique used to protect the data.

Some of the earliest accounts of secret writing dates back to Herodotus, "the father of history" according to the Roman philosopher and statesman Cicero. In The Histories Herodotus chronicled the conflicts between Greece and Persia in the fifth century BC, which he viewed as a confi-ontation between fi-eedom and slavery, between the independent Greek states and the oppressive Persians. According to Herodotus, it was the art of secret writing that saved Greece from being conquered by Xerxes, King of Kings, and the despotic leader of the Persians.

Hence in parallel with the development of steganography, there was the evolution of cryptography, derived from the Greek word kryptos, meaning 'hidden'. The meaning of cryptography is not to hide the existence of a message, but rather to hide its meaning, a process of encryption. To render a message unintelligible, it is scrambled according to a particular protocol which is agreed beforehand between the sender and the intended recipient. Thus the recipient can reverse the scrambling protocol and make the message comprehensive. The advantage of cryptography is that if the enemy intercepts an encrypted message, then the message is unreadable. Without knowing the scrambling protocol, the enemy should find it difficult, if not impossible, to recreate the original message from the encrypted text.

Although cryptography and steganography are independent, it is possible to both scramble and hide a message to maximize security. For example, the microdot is a form of steganography that became popular during the Second World War. German agents in Latin America would

photographically shrink a page of text down to a dot less than 1 millimeter in diameter, and then hide this microdot on the top of the full stop in an apparently innocuous letter. The first microdot to be spotted by the FBI (USA) was in 1941, following a tip-off that the Americans should look for a tiny gleam from the surface of a letter, indicative of a smooth film. Thereafter, the Americans could read the contents of most intercepted microdots, except when the German agents had taken the extra precaution of scrambling their message before reducing it.

In such cases of cryptography combined with steganography, the Americans were sometimes able to intercept and block communications, but they were prevented from gaining any new information about German spying activity. Thus, cryptography is more powerful branch of communication because of its ability to prevent information from falling into enemy hands.

In turn, cryptography itself can be divided into two branches, known as transposition and substitution. In transposition, the letters of the message are simply rearranged, effectively generating an anagram. For short messages, such as single word , this method is relatively insecure because there are only limited number of ways of rearranging a handful of letters. However, as the number of letters gradually increases, the number of possible arrangements rapidly explodes, making it impossible to get back to the original message unless the exact scrambling process is known.

CRYPTOGRAPHY: AN OVERVIEW

Cryptography is derived from the Greek word kryptos, meaning hidden. The use of cryptography dates back to the early Egyptian civiHzation. Nearly 200 years later the “Caesar Cipher” was used to protect military communications of the Roman Empire. Also it seems reasonable to assume that people have tried to conceal information in written form since writing was developed and examples survive in stone inscriptions and papyruses showing that many ancient civilizations including the Egyptians , Hebrews and Assyrians all developed cryptographic systems. The first use of cryptography for correspondence was by the Spartans who (as early as 400 BC) employed a cipher device called a “scytale” to send secret communications between military commanders. The scytale consisted of a tapered baton around which was wrapped a piece of parchment inscribed with the message. Once unwrapped, the parchment appeared to contain an incomprehensible set of letters, however when wrapped around another baton of identical size, the original text appears. That is, the message is concealed to protect information.

Data encryption is conceptually straight forward, a message or item of data which is desired to keep private is transformed from its original or clear text to an encrypted or clear text form. Clear text data is secure from disclosure because the original data is disguised. This is helpful to protect data even when it cannot be controlled who has access it. This disguised is created by transforming the clear text in accordance with a set of rules and mathematical operations called an algorithm. Many of the cryptographic algorithms in use today use a “key” The key is simply a number (preferably a large one) used by the algorithm to transform plaintext to clear text, and vice versa. While it is possible to develop cryptographic algorithms which do not use a key, these are regarded as weaker than an inferior to those that do. These algorithms rely on the principle of “security through obscurity”, that is, the operations or algorithm used to transform the data is kept secret by the designer. To appreciate this important point DES algorithm was published and released into the public domain in 1976 and has withstood 20 years of scrutiny without being “cracked”.

Cryptography is the science of writing in secret code and is an ancient art. The first documented use of cryptography in writing dates back to Circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with the applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. Cryptography is necessary when communicating data over any untrusted medium, which includes just about any network, particularly the internet. Within the context of any application-to-application communication, there are some specific security requirements, including

- Authentication, proving one’s identity
- Privacy/Confidentiality, ensuring that no one can read
- Integrity, assuring that received message not altered
- Non-Repudiation, mechanism to prove sender really sent message

Thus cryptography not only protects data from theft or alteration, but can also be used for user authentication.

ROLE OF KEYS IN CRYPTOGRAPHY

A cryptography key is a numerical value provided as input to the encryption algorithm which causes it to perform its transformations in a unique way. In other ways given the same clear text as input to an encryption algorithm, different key values will produce different clear text as output. Knowledge

of the key value used for encryption is required to decrypt the data. Without the knowledge of the key value (assuming that the algorithm has no defects or weakness) the eavesdropper is forced to resort to brute force, trial and error approach to recover clear text from clear text, he may have to try decrypting the clear text with all possible key values to be sure of recovering the original clear text. Thus the cryptographic strength of encryption algorithm is at least partly on the size, or the number of possible values of the key.

The other determinant of cryptographic strength is the algorithm itself A flawed algorithm is one which allows the encryption transformation to be reversed without knowledge of the key. Good cryptographic algorithms are strongly one-way transformations, they are one way in the sense that it is easy to transform the clear text to clear text, but difficult to reverse the process. Achieving this one way property is the Grail of the cryptographic algorithm design.

So, key size (or key length) and algorithmic "one-wayness" is the two factors which determine cryptographic strength or security. These factors influence security as given below.

- A brute force attack will always be successful given enough time and / or computational resources. Longer keys simply force the opponent to expend greater time, or devote more resources to the attack. However, unless all data is protected with the single key value opponent mount a brute force attack for each item of data, in other words the opponent work just as hard to recover the second data item as did for the first data.

- Algorithm flaws pose a much more serious threat to security. Once again an algorithm flaw has been found, all data items are compromised, the key value is no longer necessary to reverse the encryption process, and no further work is required for the opponent to recover the clear text from any data item protected by the flawed algorithm.

SECURITY USES OF SECRET KEY CRYPTOGRAPHY

The Secret Key Cryptography (SKC) involves the use of a single key. Given a plain text, key encryption produces unintelligible data and decryption process reverses the encryption to yield the original message. Some of the uses of secret key system is given below.

Transmitting Over an Insecure Channel -

It is often impossible to prevent eavesdropping when transmitting information. For example, a telephonic conversation can be tapped, a letter can be intercepted, and a message transmitted on a LAN can be received by unauthorized stations. If the sender and receiver share a secret key, then by using secret key cryptography one can send messages to others on a medium that can be tapped, without worrying about eavesdroppers.

The job here is the sender should encrypt the message using the secret key and the receiver must decrypt the code using the same secret key to identify the message. The eavesdropper will see only the unintelligible data. This is the classic use of cryptography.

Secure Storage over Insecure Media-

If information is to be preserved but to ensure no one else to look at, it can be stored in media where no one can get it. For, invent a key and encrypt the information using the key and store it anywhere. It is safe so long as the key is remembered. Forgetting the keys, make the data irrevocably lost. So this must be used with great care.

Authentication-

It is helpful to identify the origin of the message and provide some assurance that is authentic. Also it is useful to verify the identity of a person logging onto the system and can be continued to verify the identity if someone tries to break into the connection and masquerade as a user.

Integrity Check-

A secret key scheme can be used to generate a fixed length cryptographic checksum associated with a message. To provide protection against malicious changes to a message, a secret checksum algorithm is required such that an attacker not knowing the algorithm cannot compute the right checksum for the message. This is called cryptography checksum. That is, given a key and a message; the algorithm produces a fixed length Message Authentication Code called MAC that can be sent along with the message. A MAC is often called MIC (Message Integrity Code). A typical MAC is at least 48 bits long. Such message integrity codes have been in use to protect the integrity of large interbank electronic fund transfers for quite some time. The messages are not kept secret from the eavesdropper, but their integrity is ensured.

MULTIPLE SYMMETRIC KEYS FOR MULTILEVEL ENCRYPTION PROCESS

The Multiple Symmetric Keys [MSK] are the secret keys that are used in the proposed muhilevel encryption system. The MSK are floating point numbers that are obtained from the solutions of two

real valued functional equations. The fimctional equations are materialized using the contents of user's personal information and digital signature. These inputs are analyzed based on the characteristics of characters and patterns are identified. It is assumed that there are n patterns in the input and these n patterns are treated as variables for the construction of functional equations. The number of elements in each pattern represents the coefficient of a variable. As a result, two real valued functional equations are coined with n patterns/variables and their solutions are the desired multiple symmetric keys of the proposed system. That is, the solutions of real valued functional equations are found using modified Newton-Raphson method. The convergence of the solutions to the functional equations is ascertained by Banach Fixed Point Theorem [BFPT].

Digital Signature-

Digital Signatures are created and verified by cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. Digital signatures use public key cryptography which employs an algorithm using two different but mathematically related keys, one for creating a digital signature or transforming data into a seemingly unintelligible form and another key for verifying a digital signature or returning the message to its original form. Computer equipment and software utilizing two such keys are often collectively termed as "asymmetric cryptosystem".

The complementary keys of an asymmetric cryptosystem for digital signatures are arbitrarily termed the private key, which is known only to the signer and used to create the digital signature, and the public key, which is ordinarily more widely known and is used by a relying party to verify the digital signature. If many people need to verify the signer's digital signatures, the public key must be available or distributed to all of them, perhaps by publication in an on-line repository or directory where it is easily accessible.

Although the keys of the pair are mathematically related, if the asymmetric cryptosystem has been designed and implemented securely, it is computationally infeasible to derive the private key from the knowledge of the public key. Thus, although many people may know the public key of a given signer and use it to verify that signer's signatures, they can not discover that signer's private key and use it to forge digital signatures.

Terminologies-

The BFPT or Contraction theorem concerns with certain mappings of a complete metric space to itself. It states sufficient conditions for the existence and uniqueness of a fixed point. The theorem also gives an iterative process by which one can obtain approximations to the fixed point. The important application of BFPT is to find solutions of linear algebraic equations, ordinary differential equations and integral equations.

Newton-Raphson Method-

The fundamental concept of fixed point iteration scheme is the root finding of a function. The above theorems suggest fixed point iteration schemes to uniquely determine roots of real valued functions. The Newton-Raphson method is also the most well-known fixed point iteration scheme for approximating the roots of an arbitrary function. Let xo be the initial approximate root of the real valued function f(x). Let xo + h be the exact zero of the function f(x).

SYMMETRIC KEY MANAGEMENT

Symmetric key encryption can keep the secrets safe. The symmetric keys are used to encrypt data and to recover the original information from the encrypted data. In order to save the megabytes of information, the keys used for, must be kept safe. The process of keeping all symmetric keys safe and available for use is known as key management. The key management may be useful to store key somewhere and it can be recalled whenever it is needed. The key management principle establishes complexity to access the original key which relies on another key. Many methods are available for key management. They are software based and hardware based methods. Most commonly used software method is Password-Based-Encryption method (PBE). Other key storage place is on a hardware device. The hardware devices are tiny computers called tokens and larger devices are called crypto accelerators.

Password Based Encryption-

It is easier and cheaper method to store cryptographic keys. It is a software method of securing the encryption key. The key is secured by encrypting the key using a symmetric key algorithm. In password-based encryption, blend the password and salt to form a Key Encryption Key (KEK). The KEK is then used to encrypt the symmetric keys. Thus the symmetric key is useftil to encrypt the data or information and KEK protects the symmetric key.

Hardware-Based Key Storage-

It was examined that the PBE was a possible way to store cryptographic keys. Another storage place is on a hardware device. The devices are tiny computers called tokens. Others are larger, tamperproof boxes, generally called crypto accelerators.

Token-

A token is a small plastic smart card or a plastic key or a small port attachment or rings like device. A token contains a small chip with a processor, an operating system of sorts, and limited input/output, memory, and hard drive storage space. The advantage of using token is that the attacker does not have access to them. The problem with token is that it requires a way to communicate with the computer. A token might use the serial or USB [Universal Serial Bus] port, or even a floppy drive to communicate with the computer. These devices hold the symmetric keys for securing the key information. The process of encryption is done after the keys are obtained from the tokens. Note that the tokens are connected to the computer for a few seconds at a time it needs the use of keys which limits the key vulnerability.

Crypto Accelerators-

The large hardware crypto devices are called crypto accelerators because they usually have specialized chips that perform cryptographic operations faster than generalpurpose microprocessors. Crypto accelerators can also store data more securely than can a regular computer. The crypto accelerator accepts the plaintext and generates the cleartext. This arrangement limits the key's vulnerability.

CONCLUSION

Nowadays many electronic devices are used in Internet for sending and receiving information. Each device has its own principle to safely send the information over communication lines. Even though, the communication was thought safe, eavesdroppers, hackers and attackers meddle to tamper or steal or break the logic of preserved information. To enhance safety, many mathematical techniques were developed and used by Organizations. These safety measures help to safe guard the information from the views of unauthorized people. However, after the implementation of breaking rapport logic, Industries and Organizations struggle for Universal Standards to protect their information. To fulfill the need of Industries and Organizations in the point of securing vital data, a novice cryptosystem is developed. A few existing systems viz DES, AES and Blowfish are discussed and the results of proposed method are compared with DES, AES and BF methods.

REFERENCES

1. Adams C. (2004). "Simple and Effective Key Scheduling for Symmetric Ciphers" Proceedings, Workshop in Selected Areas of Cryptography, pp. 129-133.
2. Anil K. Jain (2009). "Fundamentals of Digital Image Processing", Prentice Hall of Australia PTY, Limited, Sydney, 2009.
3. Black J. and Rogaway P. (2000). "CBC MACs for Arbitary-length: The three-key Constructions", In proceedings of Advances in Cryptology- Crypto 2000, LNCS 1880, Springer-Verlag, London, 2000.
4. Coppersmith D. (2004). "The Data Encryption Standard (DES) and Its Strength against Attacks" IBM Journal of Research and Development, Vol. 38, No.3, pp. 243-250.
5. Dalit Naor, and Moni Naor (2003). "Protecting Cryptographic keys: The Trace-and- Revoke Approach", Computer IEEE, Computer Society, pp. 47-53.
6. Elkeelany. O, Adegoke Olabisi (2007). "Case Study: Integrated Design of RC5 Encryption", in Proceedings of The IEEE Southeast Conference.
7. Impagliazzo R. and Kapron B.M. (2013). "Logics for reasoning about Cryptographic Constructions", In Proc. 44 IEEE Symposium on foundations of Computer Science, pp. 372-381.
8. Laud P (2004). "Symmetric encryption in automatic analyses for confidentiality against active adversaries". In Proc. 25* IEEE Symposium on Security & privacy, pp. 71-85.
9. Morris Dworkin (2011). "Recommendation for Block Cipher modes of operation: Methods and techniques". Tech. Report Sp 800-38A, NIST.
10. Serge Vaudenay (2003). "Decorrelation: A theory for block cipher security". Journal of Cryptology, Vol. 16, No. 4, Springer-Verlag, London, pp. 249-286.
11. Stallings. William (2006). "Cryptography and Network Security Principles and Practices" Fourth Edition, PHI Publications, India.

Corresponding Author

Sudesh Kumari*

Master of Technology, OPJS University, Churu, Rajasthan