MAT JOURNALS

Journal of Analog and Digital Communications
Volume 4 Issue 1

Cryptography Algorithm

Anurag Rawal*, Gaurav Chhikara, Gaganjot Kaur, Hitesh Khanna
Student, Department of CSE Manav Rachna University
Faridabad, Haryana, India
****Email:** anurag.rawal07@gmail.com*
DOI: http://doi.org/ 10.5281/zenodo.2606230

Abstract

With the arrival and outbreak of high speed internet, www (World Wide Web) and growth of social media, online transaction, application and business, organization across the globe produce too much amount of data every second. Data Security is the most basic and extreme measures to ensure secure passage of information through internet. As the number of user's increases rapidly throughout the globe tremendously which directly entice cracker for doing cyber-attack. Moreover data security is becoming necessity as we are heading towards digital globalization. In this paper we will discuss various algorithm used so far starting from classical ciphers to the modern day's hash function for ensuring safer transmission of information.

Keywords: *Cryptography, Encryption, Decryption, Ciphers, Ciphers Text, Cryptosystem.*

INTRODUCTION

Cryptography is a Latin word compromised of two word Krypts and graphhein which means "hidden or secret" and "study or writing", respectively. Thus, cryptography is an art or way and the science behind secret writing. Cryptography is about composing a set of protocols so that no one can understand the data except sender and receiver thus cryptography is very convenient for data integrity and authentication purposes. Cryptography has evolved too much from classical cipher, in which letter substitution took place to modern day cryptosystem in which it is very difficult for people to decrypt and encrypt data too easily [1].

Today's our entire world is relying on web and its application . Information security plays significant role in securing modern communication systems. The most important objectives of information security are authentication, confidentiality, data integrity and non-repudiation here come the requirement of securing our privacy by ways of Cryptography. Cryptography plays a significant role for secret writing. It is the art of securing data. Cryptography is used to assure that the contents of a message are very confidentiality transmitted and wouldn't be altered. Cryptography provides range of security goals to make sure of privacy of information. The idea of encryption by which we can encode our valuable data in secret code and not to be able readable by unauthorized person even it is hacked [2].

Cryptography plays an important role in securing information during data transmission which is a big issue for both sender and receiver. Thus, cryptography emerges as a significant tool for safer communication [3].

Cryptography allows the data or information to transmit through network in unidentified ways so that the intruder's cannot understand the data. Due to the mechanism of cryptography only sender and intended receiver can read or understand the message. Cryptography has evolved throughout its lifetime, starting from letter substitution to modern day unbreakable public key cryptosystem [4]. Applications of cryptography include e-commerce, online truncation through

credit or debit cards, crypto currencies, pc passwords, and military communications [5].

In Cryptography there are some Significant Terms

1. Plain Text:
   Secrete message or information which is readable and will be encrypted.
2. Cipher Text or Encrypted Text:
   Data obtain after encrypting the information with the help of a key is known as cipher text.
3. Key:
   It is a word or value that is used for encryption of plaintext and decryption of cipher text.
4. Encryption:
   It is the technique of converting the data into encrypted form i.e. In non-understandable format with the help of key is called encryption
5. Decryption:
   It is the technique of converting the encrypted data in plain text i.e. In understandable format with the help of key is called decryption.
6. Crypto Analyst:
   Crypto Analyst is the person who is expert in breaking cipher text, cipher and cryptosystem.

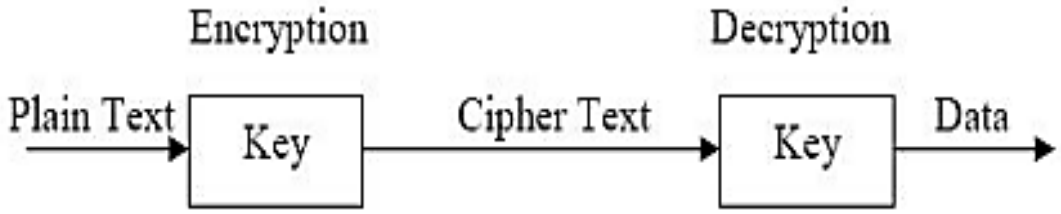

Figure 1: *A simple block diagram to understand Cryptography*

The above block diagram shows how cryptography works, simple message or information which is readable gets converted into cipher text and then converted back to plain text with the help of decryption [6].

Objective of cryptography

- **Authentication**: This mechanism facilitates to establish proof of identities. This method assures the origin of the message is properly known.
- **Access Control**: This principle states that who have the control over the access of data.
- **Availability**: The principle of availability states that resources ought to be out there to approve users.
- **Confidentiality**: This Principle states that only sender and receiver can process the content of message or information.
- **Integrity**: This mechanism assures the data or information reaches to receiver will remain the same.
- **Nonrepudiation**: This mechanism refers to the ability to ensure that a user cannot deny the sending of data or message that they originate.

LITERATURE SURVEY

Till now, you have studied about the concept and terminology used in cryptography algorithm. In this section we will share our research work [7].

We have found that how cryptography had evolved through time; centuries ago cryptography algorithm was mainly used for military and democratic purposes to present day scenario where these algorithms were mainly used for securing data and secured communication [8].
We have studied many research papers and found out the need of 3 algorithm system:

- Private Key cryptography algorithm is used to ensure data privacy and confidentially, as the sender generate key to encrypt information, the same key should be known to receiver to decrypt data.
- Public key cryptography algorithm is used to ensure data authentication and data non-repudiation, as only person who knew about the secret key can decrypt message.
- Hash Function is used to ensure message integrity as any change in the message results in the production of different hash value text.

We studied many attacks which can be done on cryptography algorithm to find the strength of algorithm [9]. The basic intention of a hacker or attacker is to break algorithm by means of finding plaintext from cipher text to obtain the key. Some of the attacks that were used by attacker are discussed as follows:

- **COA** (Ciphertext Only Attacks): In this attack the attacker has a set of cipher text from which he or she computes the plaintext.
- **KPA** (Known Plaintext Attack): In this attack the attacker knows plaintext of some cipher text from which he or she have to determine other cipher text.
- **CPA** (Chosen Plaintext Attack): In this attack the attacker has the text of his choice encrypted which means he or she has the cipher-text and plain-text pair of his or her choice through which he or she can determine the encryption key.
- **Dictionary Attack**: In this attack the attacker maintain the dictionary of cipher-text and the corresponding plain-text and to decrypt the data he or she refers to that dictionary.
- **Brute force Attack**: In this attack the attacker determine the key by attempting all possible keys. This attack takes too much amount of time.
- **MIM** (Man in Middle Attack): In this attack the attacker determine the key during key exchange step in public key cryptography.
- **Fault analysis Attacks**: In this attack the attacker introduce some error in the algorithm and study the error to get some resourceful information which results in breaking of algorithm.

CRYTOGRAPHY ALGORITHM

On the basis of key, Cryptography algorithm divided into 3 sub categories:

1. Private key Cryptography: Use only one key for encryption and decryption, also known as Secret key Cryptography or Symmetric key cryptography

Mostly used for:

- Privacy
- Confidentiality

2. Public key cryptography: Use different key for encryption and decryption , also known as Asymmetric key cryptography

Mostly used for:

- Authentication
- Non-repudiation
- Key exchange

3. Hash function: A function that converts a numerical value into another compressed numerical value. The input is of erratic length but output is always of fixed length.

Mostly used for:

- Message integrity.

Symmetric (Secret) key Cryptography:

Both encrypted and decrypted keys are same or if decrypted key can easily be computed from encrypted key.

Example: - Caesar cipher, DES, AES.

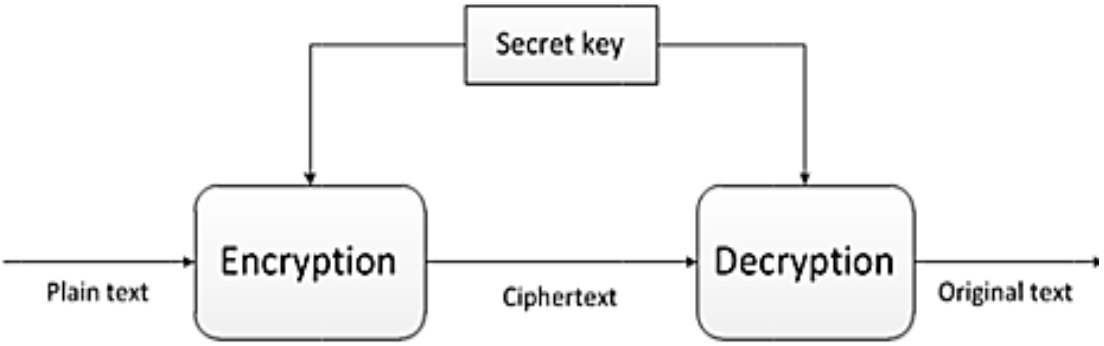

Figure 2: *Block diagram of secret key cryptography*

Secure key exchange is a major problem. We must kept encrypted key secret since anybody who knows it can easily determine decrypted key resulting in leakage of information.

Algorithm Used:

DES

DES stands for Data Encryption standard, developed in the early 1970 and uses the Fiestel function for encryption and decryption data. Encryption and decryption key are same in DES.

It is block cipher which has 64 bit block size out of which 56 bit for key length and rest 8 bit for error detection. It uses 16 round of permutation for encrypting data. Decryption process is same exactly as of encryption with the difference that decryption is done in reverse order.

AES

AES stands for Advanced Encryption standard, published in early 1977 to overcome the drawback of DES. It is a symmetric block cipher which means encryption and decryption key are exactly same. It has a 128 bit block size with variable key length of 128, 192 or 256 bits. It encrypts 128 bits data block into 10(128 bits), 12(192 bits) and 14(256 bits) round respectively according to the key size, mostly 256 bit key length is used. AES permutation has four stages of substitute bytes, shift rows, mix columns and add round key.

IDEA

IDEA stands for international Data Encryption Algorithm, first described in 1991 by James Massey and Xuejia Lai. Encryption and decryption key are same .It is a block cipher which has 64 bit block size with 128 bit key length. IDEA algorithm use 3 different algebraic function i.e., XOR, Addition modulo 216, Multiplication modulo 216 + 1, which uses 16 bit sub block to operate. IDEA is based on the perception of substitution permutation structure with 8 rounds. Same algorithm is used in reversed for decryption.

BLOWFISH

Designed in early 1993 as a substitute or replacement for IDEA algorithm. It is a symmetric block cipher which means encryption and decryption key are same. It works on 64 bit block size with variable key length ranging from 32 bit to 448 bit. It has 16 rounds or less depending upon key length .It is one of the most secure cipher. It is free from copyright and patents for encryption and decryption your data. No attack till now is a hit towards Blowfish , even though it suffers from susceptible problem.

TWOFISH

First published in 1998, as a successor of Blowfish Algorithm. It is a symmetric block cipher based on feistel structure having block size of 128 bit with 16 round of permutation and key size of 128 , 192 ,

256 bit . It uses 4 S-Packing containers (relying on keys) and same set of rule is used in reversed for decryption. Designed to be distinctly comfortable and notably flexible, nicely-suitable for big microprocessors, 8 bit smart card.

Asymmetric (Public) key cryptography
Both encrypted and decrypted keys are different and the computation of decrypted key from encrypted key is non-feasible.
Example: - RSA, Elgamal, DHA.

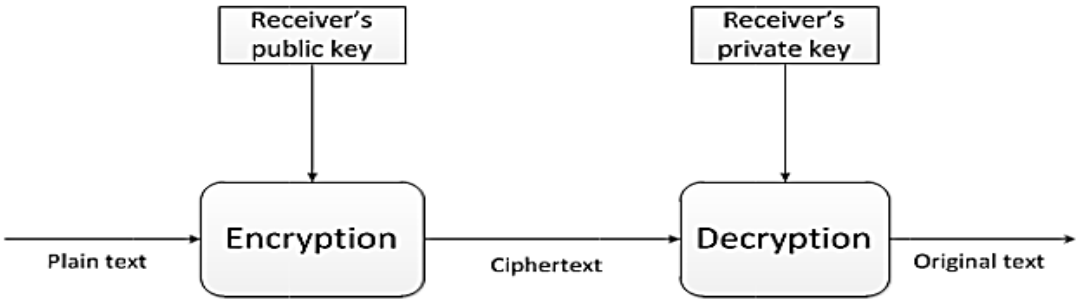

Figure 3: *Block diagram of public key cryptography*

Encrypted key is made public and decrypted key is kept secret which solve the problem of secret key sharing.

Algorithm Used

RSA

RSA is named after the mathematicians Ron Rivest, Adi Shamir and leonard Adleman. First published in 1977, it is an asymmetric block cipher, which means both encryption and decryption key are different .It is also known as public key algorithm as one of the key is known to everyone. RSA uses a variable size encryption block and a variable size key. For encryption purpose the RSA user published the product of prime number and one of the prime number which is of the order of 1028 bit or 309 decimal digits.

No one can determine the prime factor of the product from one auxiliary value, which makes it very difficult for attacker to decrypt data or information except user who knows the secret key. RSA algorithm ensures the safety of data.

Diffie-Hellman

After the success of RSA algorithm, Diffle and Hellman came up to a method for securely exchange key over a public channels. This is the first ever algorithm for practically implementing public key exchange. The algorithm was published shortly after RSA in 1977. It is a block asymmetric cipher which means both keys are different.

The Diffie – Hellman algorithm allocates users to establish a shared secret key and to communicate. This algorithm helps in one way authentication.

DSA

DSA stands for digital signature algorithm. The digital Signature set of rules can be utilized by the recipient of a message to confirm that the message has no longer been altered at some stage in transit in addition to ascertain the originator's identification. A digital signature is a digital model of a written signature in that the virtual signature can be utilized in proving to the recipient or a 3rd party that the message became, in fact, signed by the originator. Digital or Virtual signatures may also be generated for stored facts and applications in order that the integrity of the facts and packages can be validated at any later time.

ECC

ECC stands for Elliptic curve cryptography. First published in 1985, it is based on public key cryptography. ECC algorithm is an alternative for RSA as it works more efficiently than RSA algorithm. RSA algorithm is very difficult to break but ECC algorithm on the other hand is infeasible to break. To make RSA algorithm more secure, user increment the key size to 3072 bit RSA public key which work as efficiently as 256 bit ECC public key. ECC algorithm works on the mathematical problem i.e. it is impossible for anyone to find the logarithm of a random elliptic curve element with respect to a publicly known base point (which works as public key). ECC reduces the storage problem as it works too efficiently on smaller key size.

Hash Function

It is a function which takes an input and return a fixed-size alpha numeric string.
Ideal hash must have these 3 properties

- Hash can be easily computed for any data.
- Very difficult for user to calculate alpha numeric text of a given input.
- Same hash should not be produced for slightky different input.

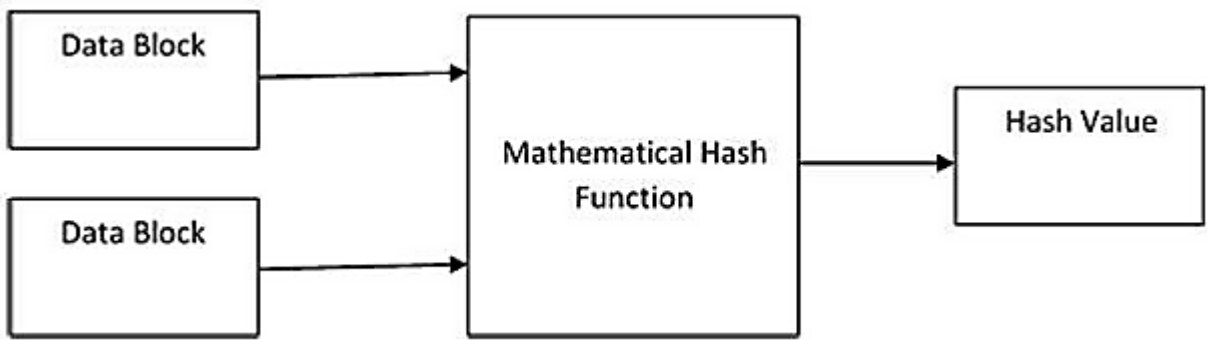

Figure 4: *Block diagram on working of hash function.*

A hash function takes a string of any length as input and produces a string of fixed length that acts as a form of "signature" for the info provided. In this way any individual knowing the "hash value" is unable to understand the input, however solely the one that is aware of the input will prove the "hash value" is made from that input.

Algorithm Used

MD5

Stands for message-digest algorithm, derived from MD-4. Designed in 1995 as a replacement for MD-4 hash function. This hash function produces 128 bit hash value, typically expressed in text format as a 32 digit Hexadecimal number. MD5 hashing algorithm is a one way cryptography function that accepts a message of any length as input and returns output as a fixed-length digest value which will be used for authenticating the original message. MD5 has been utilized in a wide variety of cryptographic applications, commonly used to verify data integrity.

TIGER

This algorithm was first published in 1995 by Ross Anderson and Eli Biham for efficiency on 64-bit platforms. Hash value size for tiger is 192 bit. Tiger hash function is a one way hash function operates on 64 bit words, maintaining 3 words of state and processing 8 words of data. It has 24 round, which has combination of different operation, mixing with XOR addition and subtraction, rotates, and s-box lookups and a very efficient key scheduling algorithm for deriving 24 round keys from the 8 input

word. Tiger hash function has no usage restriction or patent.

SHA 1

SHA stands for secure hash algorithm, first published in 1995 as a successor of SHA-0. This hash function produces 160 bit hash value, which can be expressed in text format as a 40 digit Hexadecimal number. SHA-1 uses 80 rounds of different of different cryptographic operations to encrypt data. SHA-1 is commonly used in different applications and environments where the need for data integrity is very high. It is also used to identify data corruption and checksum errors.

WHIRLPOOL

It is a cryptography hash function, designed in early 2000. It takes input of any length less than 2^256 bits and returns a 512-bit output. The Whirlpool hash function is based on block cipher for the compression function. The process of encryption consists of updating the state with four round functions over 10 rounds. The four round functions are as follows Sub Bytes, Shift Columns, Mix Rows and Add Round Key. The 512-bit Whirlpool hashes are typically represented as 128-digit hexadecimal numbers. The encryption key input for each iteration is the intermediate hash value from the previous iteration; the plaintext is the current message block and the feed forward value is the bitwise XOR of the current message block and the intermediate hash value from the previous iteration.

CONCLUSION

As we are moving towards digital globalization, we done most of our task through internet. By using internet we are sending and receiving too much information, but there is always a chance or probability of our information may get hacked by some bad people. So to protect our data, we must use the algorithm of cryptography to encrypt and decrypt our information. In this paper we have analyzed the different Cryptography algorithm. To sum up all algorithm are unique in its own way and have different purposes for securing different application. By reading many papers we have find out that BLOWFISH Algorithm is most secure in all symmetric algorithm. The experimental results of many paper showed that BLOWFISH algorithm has better efficiency than all other block cipher. The next algorithm which is used to protect our data is RSA, which is used in too many application till date. We have read too many paper on RSA algorithm, this algorithm is widely used for research purposes. To make our information more secure RSA algorithm can be used with other algorithm, s like RSA & DES, RSA & AES, RSA & DIffie Hellman, RSA & IDEA, RSA & Blowfish, RSA & Twofish .Some paper which we read were too good and effective which we can be used for future work or research. This paper provides beginners to work in this field. This paper give them a better understanding about Cryptography terminology, its types and different algorithm. They might get ideas about their work from this review paper.

REFERENCES

1. Global journals GJCST_Volume13/4-A-Study-of-Encryption-Algorithms https://globaljournals.org/GJCST_Volume13/4-A-Study-of-Encryption-Algorithms.pdf
2. Volume 8, No. 4, May 2017 International Journal of Advanced Research in Computer Science REVIEW ARTICLE Available Online at www.ijarcs.info© 2015-19, IJARCS 358 A Review on Symmetric Key Cryptography Algorithms http://ijarcs.info/index.php/Ijarcs/article/viewFile/3777/3258
3. International Journal of Computer Applications (0975 –8887) Volume 61–No.20, January 2013 12 Symmetric

Algorithm Survey: A Comparative Analysis https://arxiv.org/ftp/arxiv/papers/1405/1405.0398.pdf
4. International Journal of Computer Applications (0975 –8887) International Conference on Advancements in Engineering and Technology (ICAET 2015) 1 Asymmetric Algorithms and Symmetric Algorithms http://research.ijcaonline.org/icaet2015/number4/icaet4049.pdf
5. An overview on cryptography by Gary C. Kessler https://www.garykessler.net/library/crypto.html
6. http://www.geeksforgeeks.org/
7. http://cryptofundamentals.com/
8. https://www.tutorialspoint.com/
9. http://www.ijettcs.org/Volume4Issue1/IJETTCS-2015-01-01-12.pdf/

Cite this Article as:
Anurag Rawal, Gaurav Chhikara, Gaganjot Kaur, & Hitesh Khanna. (2019). Cryptography Algorithm. Journal of Analog and Digital Communications, 4(1), 31–38. http://doi.org/10.5281/zenodo.2606230