IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10435

Modern Cryptography and its Terminologies

Ganesh Mishra[1], Ms. Sameera Khan[2]

Final Year Student, Amity School of Engineering & Technology, Amity University Chhattisgarh, Raipur, India[1]

Assistant Professor, Amity School of Engineering & Technology, Amity University Chhattisgarh, Raipur, India[2]

Abstract: Our world is turning into an e-world. A lot of data is created daily. The digital info that we share around needs to be protected by the unwanted craps, the intruders who gets into the database and make issues. Cryptography provides the methods through which one can safeguard our data. And in this paper, we are providing review on the types of modern cryptography and its various terminologies.

Keywords: cryptography, modern cryptography, safeguard, database.

I. INTRODUCTION

The word Cryptography means 'secret writing' which is a Greek word**.** As the people started to communicate with each other, they also wanted that they should have the communication selectivity. And later on, this thing become more important as this started helping in various aspects of life.

Although Cryptography had not been developed much in the past, but it had an elite history. It played a great role in the World War 2. And the codes devised by them were the most successful codes of the time. Cryptography involves manual techniques. Then there was modification in the actual forms and techniques for better results. And even today cryptography plays a major in a nation's defence system and serves as one of the major keys for nation and its people's welfare.

'Cryptography is the art and science of making a Crypto system that is capable of providing information security.'

Modern Cryptography is the combination from the worlds of mathematics, computer science and electrical which combine to form a secure world for us. It acts as a major pillar for computer and communication security, a world which is connected in a wide area network.

The terms like *plain text, cipher text, key, intruder, cryptanalysis, cryptology, encryption, decryption, code, cipher, and many more* are the various terminologies used in the world of Cryptography. And there exists the types of types of Modern Cryptography which are Private Key Cryptography and Public-Key Cryptography.

II. CRYPTOGRAPHY

Cryptography is the art and science of making a Crypto System that can provide information security. This technique is used for the secure communication to avoid the intruder both the condition. Earlier the concept of cryptography used to end up with the encryption only, but these days the cryptography is build up mathematics, computer science & these combination of mathematics and computer science results in various algorithm. This technique has become an important tool for the transmission of data. This has the mechanism that is specially designed to detect prevent or recover from many types of security attack, basically there are two types of security mechanism.

- Specific Security Mechanism: In this security mechanism, the mechanism works or is in relation with any of the protocol layer and provides the OSI security to the data.

- Pervasive Security Mechanism: They are not specific to any of the layers of security. It provides the use of an access to the combination of physical interface and network interface.

There are various services provided by cryptography, they are as follows:

i. Confidentiality: The work security has a resemblance with the words like confidentiality and privacy. Confidentiality is a service which is provided to keep the data hidden from the intruder and accessible only to the authorized users. The confidentiality provided ranges from physical to algorithm protection.

ii. Data Integrity: Data Integrity is the service that only allows the access of data to the authorized users. The ability to detect the manipulation of data by the unauthorized users is helpful to access the data integrity.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10435

iii. Authentication: The identification of the authorized user is called Authentication. The two users those are communicating with each other needs to be identified as well as the data must also be authenticated.

iv. Non-Repudiation: Non-Repudiation is a service which doesn't permit the denial of the actions by the user prior or later.

Cryptography can be classified into two categories –

- Classic Cryptography.
- Modern Cryptography.

III. TERMINOLOGIES

There are various terminologies used in cryptography. And some of them are described as below –
Cryptology - The Cryptography and cryptanalysis combine is known as Cryptology.
Cryptanalysis - The study of cryptographic security system is termed as cryptanalysis.
Cryptanalyst - The people who does the cryptanalysis and practices Cryptology is termed to be a cryptanalyst.
Encryption - Encryption is the process in which the modulation or the transformation of the message is done using the key.
Decryption - It is the reverse for encryption. It uses the defined key and decrypts the message.
Plain Text - The form of text which remains after the process of decryption.
Cipher Text - The form of encrypted message is known as cipher text.
Key - Key is the major element which is responsible for encryption and decryption.
Secret Key - It is the key which is majorly used in symmetric key cryptography.
Intruder - A person who intrudes into the data integrity or confidentiality and break or damage the security of the system is said to be an intruder.

IV. MODERN CRYPTOGRAPHY

It is the combination of mathematics, computer science & electricals. It lays the foundation of the computer communication and security. It ensures the security of digital information, transaction, and various sorts of computation. It majorly operates on binary bit sequences. It has a strong scientific approach as there is a stronger approach by using the algorithm. That is why these become unbreakable for the intruder.
There exist two types of modern cryptography -

- Private Key Cryptography (Symmetric Key Cryptography).
- Public Key Cryptography (Asymmetric Key Cryptography).

- SYMMETRIC KEY CRYPTOGRAPHY
In symmetric key Cryptography also known as private key cryptography a secret key is used. It is the key which is shared by both sender and receiver of the message. Sender and receiver both have the copy of the secret key, they share between them. The symmetric key cryptography uses stream ciphers or block ciphers. The block cipher takes block of plain text and a key as input and cipher text of same size as output. In stream cipher, a long stream of key in combination with plain text bit- by-bit or character-by- character. There are two types of modern cryptography:
i. DES: Data Encryption Standard (introduced around 1970 early designed by Horns Feistel by IBM). The key size used is of 56 bits. It is the type of symmetric key algorithm. The sender Ans receiver must have the same key. The 64-bit block is used to perform the encryption. The various application as that of military, commercials and various communication system uses the key size of 168 bit.

ii. AES: Advanced Encryption Standard (introduced in 1997 by an NISI and was developed by Joan Daeman and Vincent Rejmen). The 3DES algorithm is the algorithm that performs an operation three times on each block then that a DES does, but its functioning is slower than that of DES. Now AES, it is the advanced form for DES algorithm. These

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10435

have varieties of key sizes like 128, 192 and 256, which makes it different form DES and 3DES. And it performs a block size of 128 bit.

- ASSYMETRIC KEY CRYPTOGRAPHY

In asymmetric key cryptography also known as public key cryptography there are two keys used, one key to encrypt and another one to decrypt and the key used are never shared. The keys used for encryption and decryption of fact that is public key and private key. The public keys used for encryption can be made distributive but the private key which is used for decryption is kept secret. The asymmetric cryptography are as follows:

i. RSA: (Its name has been based on the people who introduced the algorithm Rivist, Shamir and Adleman in the year 1977) As it is a type of a Asymmetric Cryptography algorithm, the public key can be accessed by everyone and the private can be accessed by the authorized user only. This is profoundly used in transforming of the keys over an insecure channel. Its application is widely there in the electronic industry for the only money transaction.

ii. ElGamal: (Introduced by Taher ElGamal in 1985) this algorithm act as an alternative of RSA. It is based on the deffi-Helman key exchange, its major application is the digital signature generation algorithm called ElGamal signature schemes.

iii. ECC: (Eleptic Curve Cryptography) (introduced by Neal Koblitz and Victor Asmiller in 1998) Its application are in digital signature and pseudo random generator.

iv. BLOWFISH :(Introduced by Bruce Schneier) It interprets the block cipher of 64 bits with the help of variable of length key and it contain two parts data encryption and sub key generation.

V. CONCLUSION

In this paper we have presented a review on the various terminologies of cryptography and the types of modern cryptography. And then we've described about symmetric - key and asymmetric key.

REFERENCES

1. A Research Paper on Cryptography, Encryption and Compression Techniques - By Sarita Kumari.
2. A Review Paper on Network Security and Cryptography - By Dr. Sandeep Tayal, Dr. Nipin Gupta, Dr. Pankaj Gupta, Deepak Goyal, Monika Goyal.
3. A Study on Cryptography and Techniques - By Shivani Sharma, Yash Gupta.
4. An Overview of Modern Cryptography - By Ahemad al-Wahed, Haddad Sahhavi.
5. An Analysis Review of Encryption and Decryption for Secure Communication - By Vikas Agrawal, Shruti Agrawal, Rajesh Deshmukh.
6. A Review on Classical and Modern Encryption Techniques - By Ali Mir Arif Mir Asif, Sheikh Abdul Hannan.
7. A Review on Symmetric Key Encryption Techniques in Cryptography - By Saranya K, Mohanapriya R, Udhayan J.
8. Cryptography: A Comparative Analysis for Modern Techniques - By Fiqa Maqsood, Muhammad Mumtaaz ali, Muhammad Ahemad , Munam Alisha, (IJACSA)International Journal for Advanced Computer Science and Applications, Vol.8, No.6, 2017.
9. Application of Classical Encryption Techniques for Securing Data - A Threaded Approach - By Raghu M E, Ravishankar K C, April 2015.
10. Study on Modern Cryptography and their Security Issues - By Jyotirmoy Das.
11. An Introduction to Cryptography - By Mohammad Barakat, Christian Eder, Timo Hanky, September 20, 2018.
12. Cryptography and Network Security - By Atul Kahate.
13. Network Security Essential - By William Stallings.
14. Computer Networks - By Andrew S. Tanenbaum.
15. Cryptography and Network Security - By Behrouz A. Forouzan, Debdeep Mukhopadhyay.
16. Cryptography's Past, Present and Future Role and Society - By Francklin, 16 December 2012.