IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111225

Network security using cryptography

Samiksha A. Karmankar[1], Vijay M. Rakhade[2], Lowlesh N. Yadav[3]

Student, Computer Science & Engineering, Shri Sai College of Engineering and Technology, Bhadrawati, India[1]

Assistant Professor, Computer Science & Engineering, Shri Sai College of Engineering and Technology, Bhadrawati, India[2]

Head of Department, Computer Science & Engineering, Shri Sai College of Engineering and Technology, Bhadrawati, India[3]

Abstract: Cryptography is the science of information security. The word stands resultant from the Greek kryptos, meaning concealed. Cryptography contains techniques such as microdots, merging words through images, and other ways to hide in order in storage or transfer. Modern cryptography interconnects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography contain ATM cards and laptop passwords.

Cryptology before the modern age was almost the same as Encryption, the translation of information from an understandable state to apparent nonsense. The sender retained the ability to decrypt the data and avoid redundant persons being able to read it.

Keywords: Security, Cryptography, Decryption, Encryption.

I. INTRODUCTION

Human beings from ages had two inherent needs – 1. To converse and share information and 2. To commune selectively. These two requirements gave rise to the art of coding communication so that only deliberate people could have access to the information. Unlawful people could not extract any information, even if the scrambled communication fell into their hands.

The art and science of concealing messages to introduce silence in information security are predictable as cryptography. The term ‘cryptography’ was coined by linking two Greek words, ‘Krypto’ significance hidden and ‘graphene’ meaning writing.

II. HISTORY OF CRYPTOGRAPHY

The name "cryptography" is derived from the Greek “Kryptos” meaning hidden.

The preface "crypt " means "hidden" or "vault," and the suffix "graphy" stands for "writing."

The origin of cryptography is usually from around 2000 B.C., with the Egyptian practice of hieroglyphics. These contained complex pictograms, the full meaning of which was only known to an elite few.

The first acknowledged use of a modern cipher was by Julius Caesar (100 B.C. to 44 B.C.), who did not trust his messengers when collaborating with his governors and officers. For this purpose, he formed a system in which every character in his messages was exchanged by a character three places ahead of it in the Roman alphabet.

In modern times, cryptography has turned into a battleground for some of the world's best mathematicians and computer scientists. The capability to securely store and transfer sensitive information has been verified as a critical factor in success in war and business.

Since governments do not want positive entities in and out of their countries to have access to methods to receive and send hidden information that may be a risk to national interests, cryptography has been subject to several restrictions in many countries, ranging from limitations of the usage and transfer of software to the public dissemination of mathematical ideas that could be used to develop cryptosystems.

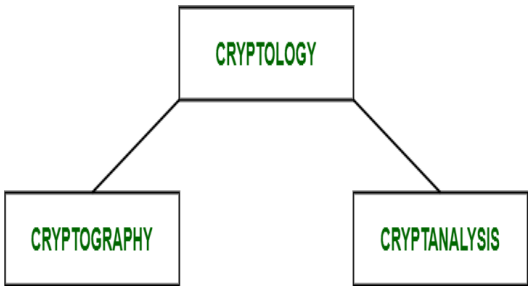
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111225

III. CONTEXT OF CRYPTOGRAPHY



Cryptology, the study of cryptosystems, can be partitioned into two parts:

- Cryptography
- Cryptanalysis

A. WHAT IS CRYPTOGRAPHY?

Cryptography is the art and science of making a cryptosystem that can provide information safety. Cryptography deals with the actual security of digital information. It refers to the design of a device based on arithmetical algorithms that offer essential information security services. You can think of cryptography as the organization of a large toolkit containing different techniques in a safety application.

B. WHAT IS CRYPTANALYSIS?

The art and science of contravention of the cipher text are recognized as cryptanalysis. Cryptanalysis is a related branch of cryptography and they composed co-exist. The cryptographic procedure consequences in the cipher text for broadcast or storage. It involves the learning of cryptographic mechanisms with the meaning to break them. Cryptanalysis is also used through the design of the new cryptographic technique to test their security strength.

IV. SECURITY SERVICES OF CRYPTOGRAPHY

The primary purpose of using cryptography is to give the following four basic information security services. Let us now see the likely goals intended to be satisfied by cryptography.

A. CONFIDENTIALITY

Confidentiality is the basic security service provided by cryptography. It is a safety service that keeps them in order from an unauthorized person. It is from time to time referred to as privacy or secrecy. Confidentiality can be achieved through many means starting from physical security to the use of arithmetical algorithms for information encryption.

B. DATA INTEGRITY

It is a safety service that deals with identifying any alteration to the data. The information may get modified by an illegal entity intentionally or accidentally. Integrity service confirms whether data is whole or not since it was last created, transmitted, or stored by an authorized user.

Data integrity cannot prevent the change of data but provides a means for detecting whether data has been manipulated illegally.

C. AUTHENTICATION

Authentication provides the recognition of the originator. It confirms to the receiver that the data established has been sent only by a recognized and established sender.

Authentication service takes two variants –

- Message authentication identifies the creator of the message with no regard router or scheme that has sent the message.
- Entity authentication is the pledge that data has been received from a specific entity, say an exacting website.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111225

• Apart from the originator, authentication may also provide a declaration about other parameters related to data such as the date and time of formation/transmission.

D. NON-REPUDIATION

It is a security repair that ensures that an entity cannot refuse the possession of a previous commitment or an action. It is a guarantee that the original creator of the data cannot deny the formation or transmission of the said data to a recipient or third party. Non-repudiation is a property that is most attractive in situations where there is the probability of an argument over the exchange of data. For example, once an arrangement is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation repair was enabled in this transaction

V. COMPONENTS OF A CRYPTOSYSTEM

The many mechanisms of a basic cryptosystem are as follows –

A. PLAINTEXT

It is the data to be protected during communication.

B. ENCRYPTION ALGORITHM

An arithmetical process creates a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takings plaintext and an encryption key as input and produces a ciphertext.

C. CIPHERTEXT

It is the twisted version of the plaintext produced by the encryption algorithm using a precise encryption key. The ciphertext is not guarded. It flows on the public channel. It can be interrupted or compromised by anybody who has access to the communication channel.

D. DECRYPTION ALGORITHM

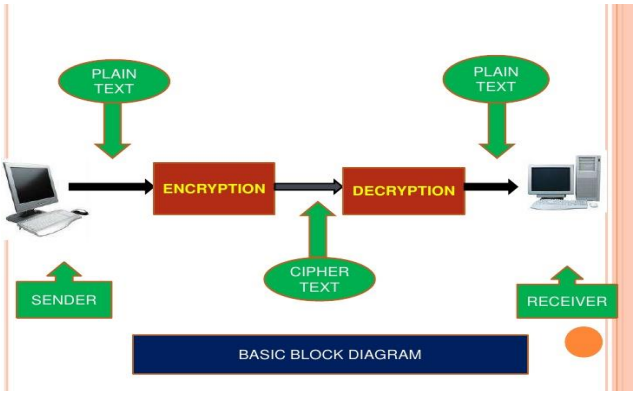
It is a numerical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takings a ciphertext and a decryption key as input and outputs a plaintext. The decryption algorithm reverses the encryption algorithm and is thus closely connected.

E. ENCRYPTION KEY

It is a cost that is recognized by the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in arrange to calculate the ciphertext.

F. DECRYPTION KEY

It is a worth that is known to the receiver. The decryption key is connected to the encryption key but is not for all time identical to it. The receiver inputs the decryption key into the decryption algorithm all along with the ciphertext in route to the plaintext. For a given cryptosystem, a set of all likely decryption keys is called a key space. An interceptor (an attacker) is an illegal entity that attempts to determine the plaintext. Can see the ciphertext and might know the decryption algorithm.



IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111225

VI. TYPES OF CRYPTOSYSTEM

Basic There are two types of cryptosystems based on how encryption-decryption is carried out in the system –

- Symmetric Key Encryption
- Asymmetric Key Encryption

The main difference between these cryptosystems is the association between the encryption and the decryption key. Logically, in any cryptosystem, both keys are closely linked. It is practically not possible to decrypt the ciphertext with a key that is not related to the encryption key.

A. SYMMETRIC KEY ENCRYPTION

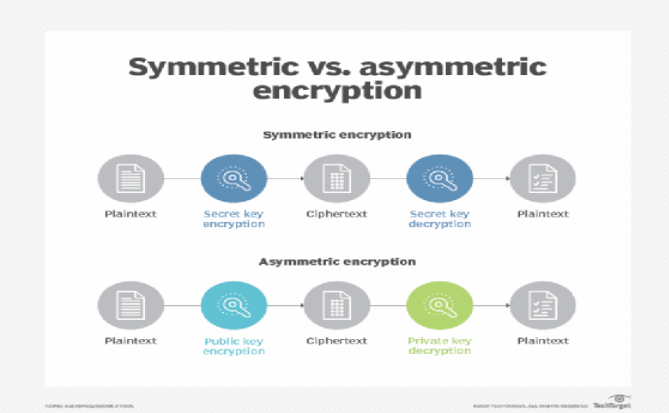
The encryption process where the same keys are used for encrypting and decrypting the in order is known as Symmetric Key Encryption.
The learning of symmetric cryptosystems is referred to as symmetric cryptography. Symmetric cryptosystems are too now and then referred to as secret key cryptosystems.
A few famous examples of symmetric key encryption methods are − Digital Encryption Standard (DES), TripleDES (3DES), IDEA, and BLOWFISH. Paper ID: ART20204060 DOI: 10.21275/ART20204060 5

B. ASYMMETRIC KEY ENCRYPTION

The encryption process where unlike keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption. Though the keys are different,
they are exactly related, and hence, retrieving the plaintext by decrypting ciphertext is possible.

Examples of public-key cryptography include:

- RSA used widely on the internet
- The elliptic Bow Digital Signature Algorithm (ECDSA) used by Bitcoin
- Digital Signature Algorithm (DSA) approved as a Federal Information Processing Standard for digital signatures by NIST in FIPS 186-4



VII. CONCLUSION

Network security is a vital factor that many organizations consider. An attack or threat may reason substantive loss of order or data to an organization. It may also destroy critical infrastructure. It is, therefore, the best conclusion to change a reliable security policy for the firm's network.

The above network security strategies can play an important role in justifying the risks that the safe may experience in its operational environment. All the security rules should ensure that the information and data are confidential without disturbing their availability or integrity.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111225

REFERENCES

[1] Thakur, J. and Kumar, N., 2011. DES, AES & Blowfish: Symmetric key cryptography algorithms model-based performance analysis. International journal of emerging technology & advanced engineering, 1(2), pp.6-12.
[2] Al-Shabi, M.A., 2019. review of symmetric and asymmetric cryptography algorithms in information security. International Journal of Scientific and Research Publications (IJSRP), 9(3), pp.576-589.
[3] Dooley, J.F., 2018. History of cryptography and cryptanalysis: Ciphers and their algorithm. Springer.
[4] Mogollon, M. ed., 2008. Cryptography and Security Services: Mechanisms and Applications. IGI Global.
[5] Zhou, X. and Tang, X., 2011, August. Research & implementation of RSA algorithm for encryption and decryption. In Records of 2011 6th international forum on strategic technology (Vol. 2, pp. 1118-1121). IEEE.
[6] Delfs, H., Knebl, H., and Knebl, H., 2002. Introduction to cryptography (Vol. 2). Heidelberg: Springer.
[7] Coron, J.S., 2006. What is cryptography? IEEE security & privacy, 4(1), pp.70-73.
[8] Dobbertin, H., 1996. Cryptanalysis of MD5 compress. rump session of Eurocrypt, 96, pp.71-82.

