e-ISJN: A4372-3114
p-ISJN: A4372-3115

ISSN: 2321-7782 (Online)
ISSN: 2347-1778 (Print)
Impact Factor: 7.327

Volume 8, Issue 7, July 2020

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

A Study on Information Security and Cryptography

Arockia Panimalar. S[1]
Assistant Professor
Department of IT & CT
Nehru Arts and Science College
Coimbatore, India

Mahalakshmi. K[2]
III B.Sc. IT
Department of IT & CT
Nehru Arts and Science College
Coimbatore, India

Pooja. M[3]
III B.Sc. IT
Department of IT & CT
Nehru Arts and Science College
Coimbatore, India

Abstract: Information is the most important asset of human resources. So protecting them is crucial. Information Security, also called as Infosec, is a system of preventing unauthorized access, use, divulgence, interruption, revamping, inspection or deleting the data. Information security is configured around 3 objectives known as CIA – Confidentiality, Integrity, and Availability. One of the main techniques used to secure the information is Cryptology. Cryptology technique was initially used in times of world war to provide secrecy for written messages.

Keywords: Information, Infosec, CIA, Cryptology.

I. INTRODUCTION

Cryptology is the mathematical and Computational Algorithm that underpin and encompasses both Cryptography and Cryptanalysis. Cryptanalysis concept is highly specialized and intricate. Cryptography is used to secure the information through encryption Algorithms. Cryptography fortifies the information by encrypting and decrypting data. Cryptography renders diverse important information security services such as authentication, confidentiality, integrity and non-repudiation. Cryptographic protocols make cryptography user-friendly and authorize end-user to protect their Information Modern cryptography pin it's trust on cryptographic keys for encoding and decoding messages combined and fused with cryptographic algorithms. Depending on the type of keys used, cryptography is classified as either symmetric or asymmetric key cryptography which ensures the data confidentiality. The most commonly used basic algorithms are:

1. Public Key Encryption (symmetric)
2. Private Key Encryption (asymmetric)

A. History

The theoretical foundation of cryptography was spread out around in India and China 3000 years ago. The ancient cipher of the Greek historian Polibio formed a table, with rows and columns, to connect a letter to a duplet number. The popular Caesar's Cipher is based on an algorithm of shifting three positions, mathematically y = (x + 3) mod 26. Julius Caesar is accredited with the invention of the Caesar cipher. Basically, Caesar's Cipher was created to avert his secret messages falling in the vicious hands. World War II routed ample advancement in information security and pronounced the beginning of the professional field of information security. From the outset of the 21st century telecommunications, computing hardware and software, and data encryption has been promptly emerging.

B. Ciphers

According to cryptography, a **cipher** (also written as cypher) is an algorithm for executing encryption or decryption operations. Ciphers do not entail meaning. They are mechanical operations and algorithms that are carried out on chunks of letters. Most modern ciphers can be classified in many ways:

- ✓ Block ciphers
- ✓ Stream ciphers
- ✓ Symmetric key algorithms
- ✓ Asymmetric key algorithms

1) Substitution Cipher

In this technique, each letter of the message is supplanted with a single character. The units of the plaintext are replaced by letters, numbers or symbols to encrypt the messages and encode it into a cipher text.

2) Monoalphabetic Substitution

The letter-for-letter or symbol-for-symbol substitution encrypting technique is called Monoalphabetic Substitution. It is one of the weakest ciphers used, which is similar to Caesar cipher.

3) Shift Cipher

Shift Cipher is also called as Caesar cipher. If understood, the decoding of this cipher is plain-sailing. It is an altered format of the substitution cipher. By shifting the alphabet a few positions in clock-wise or anti-clockwise direction, a simple classic sentence can become obscured.

4) Polyalphabetic Cipher

To make ciphers more perplexing to crack, Blaise de Vigenère from the 16th-century of France proposed a polyalphabetic substitution technique. In this cipher, instead of a one-to-one relationship (1:1), there is a one-to-many (1:M). A single letter can have multiple substitutes and positions.

II. Quantum Cryptography

The concept of quantum cryptography existed in 1990s. This technique makes use of Quantum mechanics. The area of quantum cryptography is still experimental but the initial reports are promising. Quantum Cryptography uses light packets, also called as photons. These photons behave peculiarly. They can be polarized when they are passed through a polarizing filter, which is similar to sunglasses filtering the excessive sunrays. When the photons are passed through a polarizing filter, photons tend to travel in the direction of the filter's scale.

To generate a Caesar cipher in Quantum cryptography, we must use two sets of polarizing filter. One set consists of a horizontal filter and a vertical filter. This option is called Rectilinear bases, where bases are a coordinate system. The second sets of filters are rotated 45 degrees and are called Diagonal bases. We have assigned for direction as 0 and other as 1, for each basis. The message will be passed at great speed and accuracy. The qubits are the bits that are sent one at a time.

- ✓ Two cryptographic principles are:

  1. Messages must contain some Redundancy.
  2. Some method is required to foil replay attack.

III. ENCRYPTION TECHNIQUES

Public Key Encryption

One of the most used ancient encryption techniques is the Public key encryption. It is a type of Cipher Architecture also called as public key cryptography. It utilizes a pair of keys, for encrypting and decrypting the data. One of the keys in the pair is a public key. Encoding the message or plain text, results in a cipher message which is encrypted by a public key. [3]The encrypted message can decoded only by the decryption process. Decryption uses another key in the pair. This encryption technique is also called asymmetric encryption (Fig.1) because it makes use of two keys instead of using a single key (symmetric encryption).

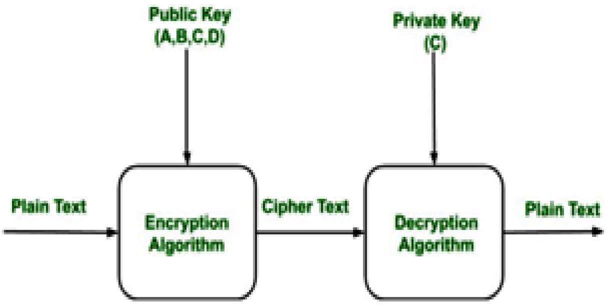

Fig 1: Public Key Encryption Algorithm

Signcryption

Signcryption is the latest research that constitutes the combination of the digital signature and the public key encryption t the same time. The crucial advantage of this new method is that the is less than the sum for the cost of digital signature and the encryption.[6]

- ***Rivest–Shamir–Adelman***

The Rivest–Shamir–Adelman (RSA) is a public key cryptosystem. RSA was the subject of extensive cryptanalysis. In a complexly technical indeed paper, Boneh reviews all cryptanalytic attacks on RSA and concludes that nothing is significant. Most of the cryptographers consider factorization as a solid base for a secured cryptographic system.

- ***Cryptographic Hash Functions***

The MD4, MD5 and SHA/SHS (Secure Hash Algorithm or Standard) are the most popularly used hash functions. The improved version of MD4 is MD5.

- ***Digital Signature***

The digital signature is a protocol that confirms agreement to a message as a real signature. A digital signature is a mathematical scheme where only the sender alone can sign and other receivers are not allowed modify or alter but only to recognize it. A valid digital signature ensures the recipient that the message was created by a known sender, and that it was not altered during the transmission. Digital signatures are commonly used for software distribution, financial transactions, online certifications and verification of user's identity.

- ***Digital Certificates***

A Digital certificate or identity certificate) is a digital copy of a document which can be accessed remotely. It uses a digital signature to combine public key with the information of a person or an organization. The certificate is used as verification for a public key which belongs to an authorized individual. Contents of a typical digital certificate:

i. Serial Number

ii. Subject

iii. Signature Algorithm

iv. Issuer

v. Valid-From

vi. Valid-To

vii. Key-Usage

viii. Thumbprint Algorithm

IV. Cryptography Attacks

The cryptographic attacks are performed by the attackers or hackers to steal the information of the user. Some of the attacks include:

1. Ciphertext Only Attacks (COA)
2. Known Plaintext Attack (KPA)
3. Chosen Plaintext Attack (CPA)
4. Brute Force Attack (BFA)
5. Birthday Attack
6. Side Channel Attack (SCA)
7. Timing Attacks
8. Power Analysis Attack

V. Principles of Infosec

1. *Authentication*

Authentication is the process of verifying the user's identity basically by username and password. Now-a-days, authentication is done by biometric such as finger print and face recognization.

2. *Confidentiality*

The authorized person is only permitted to access and use the information. This is called as Confidentiality. The information is made confidential inorder to prevent that information from the access of unauthorized person like Hackers. Confidentiality is most essential (but not sufficient) for maintaining the privacy and personal information of all people. Encryption Technique is used to encode the information and only can be decoded with the decryption key. Hence when the information is hacked in the middle of transmission, it becomes unreadable without a decryption key.

3. *Integrity*

Integrity ensures that the information can't be modified by unauthorized users. The information are accurate in information systems which can be manipulated only by the permitted appropriate users.

4. *Non-repudiation*

Non-repudiation refers to ensuring that a transmitted message or text is sent and received by the sender and the receiver. Non-repudiation assures that later the sender and receiver of a message cannot deny having sent the message or received the message.

5. *Availability*

Availability ensures that the information systems are reliable and makes sure that data is accessible, dependable and available at timely manner.

VI. Information Security Concerns

✓ *Logic Bombs*

A logic bomb is intentionally left to carry out a malicious function on a computer system which is hidden for a specific period of time.

✓ *Malware*

Malware refers to a type of software that executes harmful, unauthorized, or unawared activity. Malware can also be a computer virus, worms, and trojans. Malware is a software and is a malicious combination.

✓ *Phishing and Targeted Phishing Scams*

Phishing through Internet and scamming the targeted person in an electronic communication system.

✓ *Backdoors*

A backdoor is also known as “trap door,” is a way to access a computer program or system that bypasses normal mechanisms.

VII. Conclusion

Privacy is a myth in the modern Society. Cyber-attacks and machine’s computational power are rapidly evolving. So information should be highly secured. Honey Pot Technique or Honey Encryption is one of the new techniques discovered where the unauthorized user would be provided with the deployed documents for each incorrect decoding. Quantum Key Distribution makes use of the Quantum cryptography where keys are embedded over fiber optics in Photons (Lights). Encryption is also used in Online payments, Data in Cloud, databases and Emails.

References

1. Computer and Information Security Handbook, John Vacca
2. Legal Issues in Information Security, Joanna Lyn Grama
3. Beautiful Security, Andy Oram, John Viega
4. http://searchsecurity.techtarget.com/
5. Innovative Cryptography, Nick Moldovyan; Alex Moldovyan.
6. Cryptography for Developers, Tom St Denis.
7. Signcryption (Short Survey), Yevgeniy Dodis
8. http://en.wikipedia.org/wiki/SeparatiSe_of_duties
9. https://www.cryptomathic.com/

AUTHOR(S) PROFILE

Ms. Arockia Panimalar. S, is working as an Assistant Professor in the Department of Information Technology and Computer Technology at Nehru Arts and Science College, Coimbatore. She has published papers in International Journals and presented papers.

Ms. Mahalakshmi. K, is studying B.Sc. IT in the Department of Information Technology and Computer Technology, Nehru Arts and Science College, Coimbatore. She has presented papers in conferences and published papers in International Journals.

Ms. Pooja. M, is studying B.Sc. IT in the Department of Information Technology and Computer Technology, Nehru Arts and Science College, Coimbatore. She has presented papers in the conference.