IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 1, Jan 2022

An Explanation on Different Types of Attacks in Modern Cryptography System

Rajendra P. Pandey, Assistant Professor,
College of Computing Sciences and Information Technology, Teerthanker Mahaveer University,
Moradabad, Uttar Pradesh, India
Email Id- panday_004@yahoo.co.uk

ABSTRACT: ***Data may be transmitted and stored using cryptography in a specific format so that only the intended recipients can access it and use it. Cryptology, cryptanalysis, and cryptography are all closely linked fields of study. Most frequently, encryption and decryption are used to transform plaintext, also known as clear-text, into cipher-text. The act of converting plaintext back into plaintext is characterized as encryption. By identifying a flaw in a code, cypher, cryptography protocol, or important management scheme, a cryptographic attack is a technique for getting around the security of cryptographic system. Attacks are frequently classified according to the action taken by the perpetrator that are all reviewed in this paper. A thorough discussion on the types of attacks is also provided in this paper which was then followed by a concluding remark.***

KEYWORDS: ***Cryptography, Cryptology, Cryptographic Attack, Plaintext, Security.***

1. INTRODUCTION

The two components of cryptology are cryptography, which focuses on developing secret codes, and cryptanalysis, which is concerned with understanding the cryptographic method and cracking those hidden codes. A Cryptanalyst is someone who carries out Cryptanalysis. By identifying any weak points in the cryptosystem, it aids in the understanding of them as well as the ability to strengthen them and work on the algorithm to produce more secure secret codes. The plaintext of a ciphertext, for instance, may be extracted by a cryptanalyst. It can assist us in figuring out the encryption key or the plaintext[1]. As illustrated in the Figure 1; Cryptology is divided into Cryptography and Cryptoanalysis.

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 1, Jan 2022

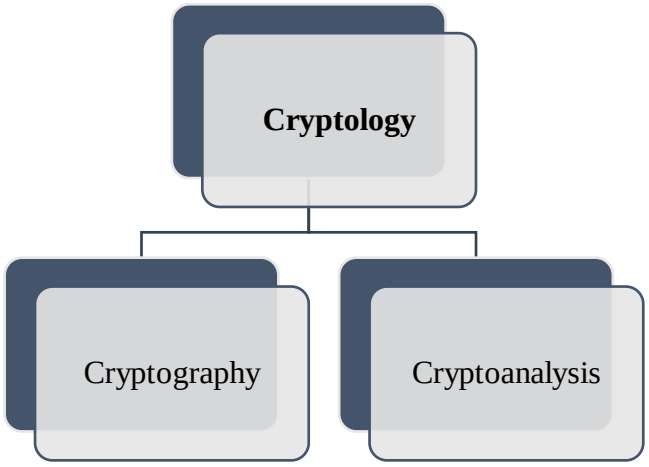

Figure 1: Illustrating the two main aspect of Cryptology; i) Cryptography and ii) Cryptoanalysis.

1.1. Cryptographic system

A cryptographic system must be attacked in order to identify its weak areas. Attacks like this are known as cryptanalytic attacks. The vulnerabilities depend on the algorithm's design as well as background understanding of the plaintext, which can be either a piece of plaintext code written in Java or a normal text written in English. So before attempting to employ the attacks, it is important to understand the nature of the plaintext [2], [3]. The act of concealing information in transit so that only the receiver may see it requires the use of cryptography. Information is encoded before being sent and decoded at the recipient's end by IT professionals to accomplish this. IT pros can encrypt data with either symmetrical or asymmetrical encryption using an algorithm. However, attackers are able to attack cryptosystems just like any other computer network[4].

1.2. Different Types of Cryptographic attacks

Cybercriminals have the ability to actively or passively assault encrypted data. In contrast to passive assaults, which include spying or data eavesdropping, active attacks may, as their name implies, alter or modify the system files, making them hazardous. Nevertheless, in order to reduce the dangers, programmers should be familiar with the many kinds of cryptographic attacks. They comprise [5] (Figure 2):

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 1, Jan 2022

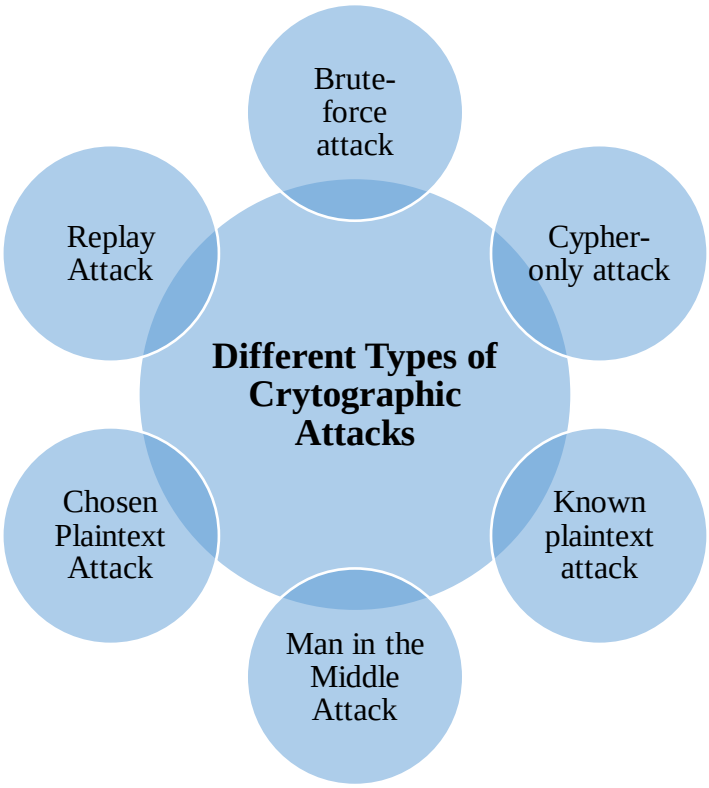

Figure 2: Illustrating the different types of Cryptographic attacks.

1.2.1. Brute-force attack

In a brute-force assault, every conceivable character combination is tested in an attempt to obtain the 'key' that will unlock an encrypted message. For smaller key spaces, brute-force assaults could take less time, but for bigger key spaces, it will take an incalculable length of time. Therefore, attempting brute-force attacks on contemporary encryption technologies is impracticable [6].

1.2.2. Cypher-only attack

The attacker in a "cipher-only" assault is familiar with the ciphertext of numerous communications that have all been encrypted with the same technique. Finding the "key," which may then be used to decode all communications, is the task facing the attacker. The "cipher-only" attack is arguably one of the simplest to carry out since it is simple to sniff out the cipher - text but challenging to accomplish because it requires knowledge of the encryption method [7].

1.2.3. Known plaintext attack

Contrary to Ciphertext-only attacks, hackers conducting a Known Plaintext attack have such a copy of the message that has previously been encrypted as well as the plaintext data that was used to create the ciphertext. With these kind of information, the attacker may bypass weak encryption protocols and conduct additional attacks [8].

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 1, Jan 2022

1.2.4. Man in the Middle Attack

Man in the Middle Attacks, as their name indicates, happen when a cybercriminal stands in the middle of a conversation between two people, listening in on everything they say and even learning how the encrypted session was set up. By replying to the initiation request, the hacker gains access to the session and creates a secure session with the communication's creator. The malevolent party then starts a second secure connection with the original receiver while assuming the originator's identity by utilising new keys. The person then stands in the middle of the communication and reads all of the data or traffic sent from the sender to the target audience [9].

1.2.5. Chosen Plaintext Attack

The chosen-plaintext attack is somewhat similar to known-plaintext assaults, but in this attack, the hacker takes a chance by picking a plaintext that matches the ciphertext that was produced. In order to decrypt subsequent communications, he may then evaluate both words to identify the key and know more about the complete encryption process.

1.2.6. Replay Attack

On cryptographic methods lacking temporal safeguards, replay attacks are utilised. Cybercriminals in this case eavesdrop on encrypted messages sent back and forth between two people, then repeat the messages to start a new session after requesting authentication. Use of timestamps in communication and the establishment of expiry times for all communications are the best ways to prevent replay attacks [10].

2. DISCUSSION

In the modern day, information governs practically every area of human existence, not just business. Therefore, it has become crucial to safeguard vital information against sinister actions like assaults. Let's think about the many forms of threats that information frequently faces. Attacks are often grouped according on what the attacker did. Thus, an assault can be either passive or aggressive. All communication-related fields have placed a high priority on security, which has also grown to be a major issue for every business working with heterogeneous data. We have cybersecurity professionals and experts all over the world to help us solve security difficulties, but it is tough to identify and hire these personnel owing to project-related costs.

In terms of research and development, the researchers have concentrated on a few problems in order to examine them and offer answers. In this paper we have reviewed different types of cryptographic attacks. However, the attacks on cryptosystems mentioned here are highly academic in nature, as the bulk of them originate in academics. Indeed, many scholarly attacks make unreasonable assumptions about the surroundings as well as the skills of the attackers. In a selected-ciphertext attack, for example, the attacker demands an unreasonable number of purposefully chosen plaintext-ciphertext pairings. It may not be entirely practicable. Nonetheless, the existence of any assault should be cause for concern, particularly if the attack strategy has the potential for development. Each cryptographic method has a distinctive quality that makes it possible for it to be used for a variety of network security applications. There are many new encryption methods available today, but the quick, secure methods of old will always provide a

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 1, Jan 2022

high level of security. Without a question, the age of information technology is here to stay. It is also true that, while technology develops at the same time, there is a constant risk of computer hackers attacking a system. Just like anything else, there are benefits and drawbacks to everything. The only surefire method to be secure is to keep your system up to date, stay informed about emerging IT trends, stick to reputable websites, and utilise encryption anytime you exchange information online.

3. CONCLUSION

Evidently, a few cybersecurity tenets form the foundation of the cryptographic attack landscape. Utilizing advanced encryption algorithms is thus the best defense against cryptography assaults. Asymmetrical encryption algorithms, which utilise separate keys to encrypt and decode the message, are also an option. This is superior to symmetric encryption that utilizes the same key for both message encryption and decryption. Thankfully, understanding cryptography is rather straightforward. To learn cryptography, unlike other professions, people don't need require a degree.

REFERENCES:

[1] F. Piper, “Introduction to cryptology,” *Inf. Secur. Tech. Rep.*, 1997, doi: 10.1016/s1363-4127(97)81322-2.

[2] J. Machicao, J. M. Baetens, A. G. Marco, B. De Baets, and O. M. Bruno, “A dynamical systems approach to the discrimination of the modes of operation of cryptographic systems,” *Commun. Nonlinear Sci. Numer. Simul.*, 2015, doi: 10.1016/j.cnsns.2015.01.022.

[3] T. Li, Z. Liu, J. Li, C. Jia, and K. C. Li, “CDPS: A cryptographic data publishing system,” *J. Comput. Syst. Sci.*, 2017, doi: 10.1016/j.jcss.2016.12.004.

[4] M. Backes and B. Köpf, “Quantifying information flow in cryptographic systems,” *Math. Struct. Comput. Sci.*, 2015, doi: 10.1017/S0960129513000662.

[5] Y. J. Kang, T. Y. Kim, J. B. Jo, and H. J. Lee, “An experimental CPA attack for arduino cryptographic module and analysis in software-based CPA countermeasures,” *Int. J. Secur. its Appl.*, 2014, doi: 10.14257/ijsia.2014.8.2.27.

[6] G. Sowmya, D. Jamuna, and M. V. Reddy Krishna, “Blocking of Brute Force Attack,” *Int. J. Eng. Res. Technol.*, 2012.

[7] C. Li and K. T. Lo, “Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks,” *Signal Processing*, 2011, doi: 10.1016/j.sigpro.2010.09.014.

[8] G. Chunsheng and G. Jixing, “Known-plaintext attack on secure kNN computation on encrypted databases,” *Secur. Commun. Networks*, 2014, doi: 10.1002/sec.954.

[9] M. Conti, N. Dragoni, and V. Lesyk, “A Survey of Man in the Middle Attacks,” *IEEE Communications Surveys and Tutorials*. 2016. doi: 10.1109/COMST.2016.2548426.

[10] P. Nagarsheth, E. Khoury, K. Patil, and M. Garland, “Replay attack detection using DNN for channel discrimination,” 2017. doi: 10.21437/Interspeech.2017-1377.