iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VIII **Month of publication:** Aug 2023

DOI: https://doi.org/10.22214/ijraset.2023.55512

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

Various Cyber - Attack on Encryption Algorithm

Dr. Bhumika Charnanand[1], Chetan Rathod[2]
[1]*Department of Computer Science, School of Science & Technology, Vanita Vishram Women's University,Surat*
[2]*Research Scholar, Department of Computer Science, Saurashtra University, Rajkot*

***Abstract:** With the rapid advancement of technology across various fields, the significance of security has grown exponentially. As information is transmitted over networks or stored in devices, the question of data security has become a critical aspect of technology. To address this concern, data encryption is employed, wherein the data is encoded in a secure manner. However, the pressing question remains: can data truly be safeguarded against all cyber-attacks? In order to encrypt data, different algorithms are utilized, each with its own unique characteristics and level of security. The purpose of this paper is to delve into the impact of various types of attacks on these encryption algorithms. By examining the vulnerabilities and weaknesses of different encryption methods, we aim to gain a comprehensive understanding of the effectiveness of these algorithms when subjected to cyber-attacks.*
***Keywords:** Encryption Algorithms, Cyber Attack. Data Security, Integrity, Cipher, Cryptography, Cryptanalysis.*

I. INTRODUCTION

Cryptography is a crucial technique used to create secret codes for secure data transmission over networks[1][8], while cryptanalysis involves the study of cryptographic algorithms and the process of breaking these codes. Individuals skilled in cryptanalysis are known as cryptanalysts. In cryptographic algorithms, a key is employed to transform plain text into unreadable cipher text or encoded data, which is then transmitted over the network. At the receiving end, this cipher text is decrypted using the appropriate key to regenerate the original plain text[2]. This process can be achieved through two different methods: symmetric and asymmetric encryption. In symmetric encryption, a single key is utilized for both the encryption and decryption processes. Notable examples of symmetric algorithms include DES (Data Encryption Standard), triple DES, AES (Advanced Encryption Standard), RC4, RC6, and Blowfish. On the other hand, asymmetric encryption involves the use of two distinct keys: a public key for encryption and a private key for decryption. An example of an asymmetric algorithm is RSA (Rivest-Shamir-Adleman)[9].

There are two types of algorithms based on the manner in which cipher keys are applied. The first is block cipher, which involves dividing the data into fixed-sized chunks known as blocks. Encryption is then performed on each individual block, generating a block cipher[3]. The second method is stream cipher, where data is processed in a continuous stream[4]. This method comprises two main components: a key stream generator, which produces the stream cipher, and a mixing function, often implemented as an XOR function, which combines the stream cipher with the plain text to produce the cipher text.

It is worth noting that the choice between symmetric and asymmetric encryption depends on various factors such as security requirements, computational efficiency, and key management complexity. Symmetric encryption is generally faster and more efficient for bulk data encryption, whereas asymmetric encryption excels in scenarios involving secure communication between two parties without the need for a shared secret key.

II. TYPES OF ATTACK ON CRYPTOGRAPHY

Cryptography attacks can be broadly categorized into two types: passive attacks and active attacks. Each type of attack aims to compromise the security of sensitive data and information through different means. Let's delve into the details of each attack type and explore some common attack techniques and their effects on various cryptography algorithms.

III. PASSIVE ATTACKS

A passive attack involves the attacker intercepting the communication between parties without interrupting the flow of data. The attacker's objective is to gain unauthorized access to sensitive information without altering its content. This type of attack focuses on eavesdropping and obtaining confidential data[5]. The intercepted information can then be analyzed or used for malicious purposes.

IV. ACTIVE ATTACKS

In contrast to passive attacks, active attacks not only involve unauthorized access to data but also include tampering with the data or communication channels. The attacker actively modifies or manipulates the information to their advantage.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

Active attacks aim to disrupt the integrity, authenticity, or availability of the data being transmitted[5]. They can have more severe consequences compared to passive attacks, as the attacker actively alters the information.

Now, let's explore some common types of cryptography attacks and their effects on various algorithms:

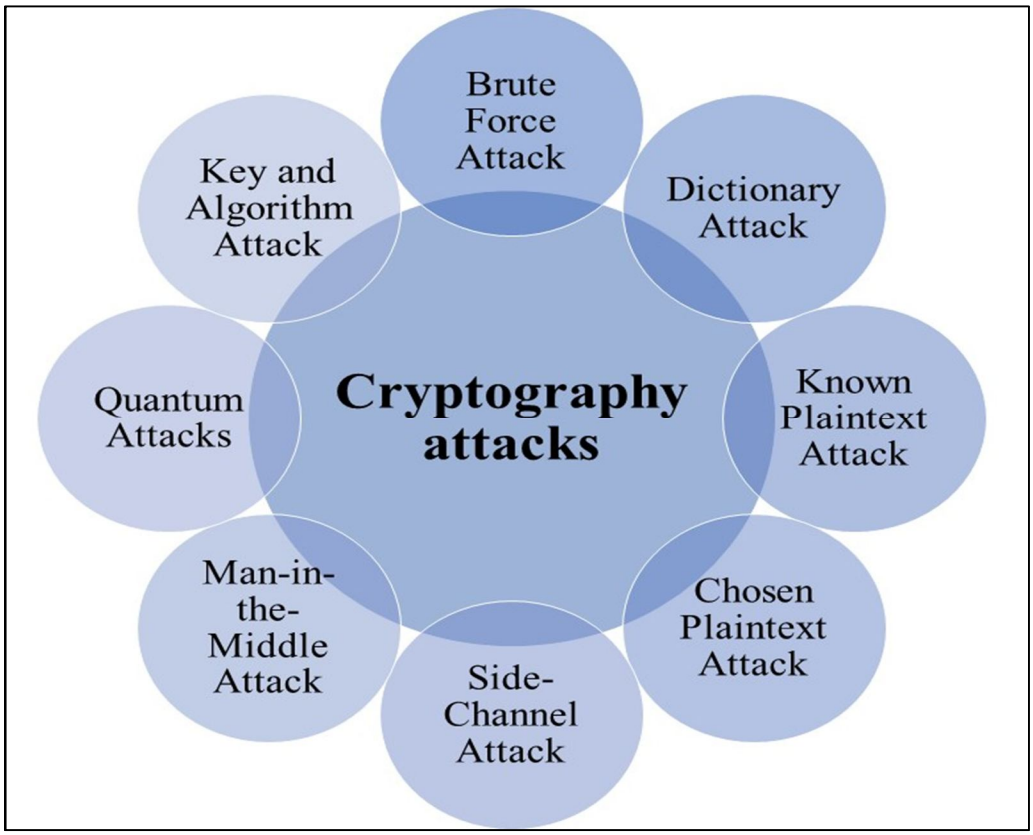


Fig 1: Types of Cryptography attacks[7]

A. Brute Force Attack

In a brute force attack, an attacker approaches encryption like trying every possible combination of keys to unlock a treasure chest. Imagine you have a lock with a key, and the attacker wants to open it. They start trying every single key they can think of, one after the other, until they stumble upon the correct one that opens the lock. If the encryption method used is not strong or the key isn't complex enough, the attacker might succeed relatively quickly. However, if the encryption is robust and employs a long and intricate key, it becomes exceedingly difficult and time-consuming for the attacker to test every possible key combination. Strong encryption methods are designed to withstand this type of attack.

B. Dictionary Attack

In a dictionary attack, the attacker uses a list of commonly used passwords or phrases, much like using a dictionary of words. It's like trying out simple passwords that many people use, such as "password123" or "qwerty," in an attempt to unlock encrypted information. People often choose easy-to-guess passwords, and this type of attack capitalizes on that fact. By using a list of these predictable passwords, the attacker hopes to find a match and access the encrypted data. To defend against dictionary attacks, it's crucial to use strong and unique passwords that aren't easily guessable.

C. Man-in-the-Middle Attack

Imagine you're sending messages to your friend, and there's a sneaky third person who intercepts and reads your messages before passing them along to your friend. This sneaky person also sends messages pretending to be you, tricking your friend into thinking they're still talking to you. This is what happens in a man-in-the-middle attack. The attacker secretly gets in between two people who are communicating, so they can eavesdrop on the conversation or even alter the messages being exchanged. It's a breach of privacy and trust between the communicating parties.

D. Known Plaintext Attack

In a known plaintext attack, the attacker has both the encrypted message and the original, unencrypted message that corresponds to it. With this information, they analyze how the encryption process works. By comparing the two versions of the message, they try to figure out the secret key or find weaknesses in the encryption method. Modern encryption techniques are designed to resist this type of attack by making sure the encrypted message doesn't reveal any obvious patterns or clues about the key used to encrypt it.

E. Side-Channel Attack

A side-channel attack is a bit like figuring out a secret by paying attention to things that aren't actually the secret itself. Imagine trying to guess a password by listening to the sound of someone typing it. In this type of attack, the attacker doesn't directly crack the encryption; instead, they observe unintended information leaks that occur during the encryption process. For instance, the attacker might analyze the power consumption of a device performing encryption or measure the electromagnetic radiation it emits. These subtle cues could inadvertently reveal information about the encryption key or the data being processed. To counter side-channel attacks, encryption methods must be implemented with care to prevent these leaks.

F. Quantum Attacks

Think of a quantum computer as a super powerful math solver. Regular computers use bits, which can be 0 or 1, but quantum computers use qubits, which can be 0, 1, or both at the same time. This enables them to solve certain math problems much faster than regular computers. Quantum attacks leverage these super-fast computers to crack encryption that relies on the difficulty of certain mathematical problems. For example, RSA and Elliptic Curve Cryptography (ECC) are encryption methods vulnerable to quantum attacks because quantum computers can efficiently solve problems that these methods are built upon. Researchers are developing new encryption methods, known as post-quantum cryptography, that can resist quantum attacks.

G. Chosen Plaintext Attack

Imagine you're sending secret notes, and an attacker gets to decide what those notes contain. They then watch how you turn those notes into secret codes. By analyzing the relationship between your original notes and the coded messages, the attacker tries to find weaknesses in the encryption process. This type of attack can reveal patterns or vulnerabilities that might not be obvious from just studying the encrypted data. A strong encryption method should remain secure even if attackers know what kind of messages are being encrypted.

H. Key and Algorithm Attack

In this scenario, think of the encryption process like a puzzle. The encrypted data is the puzzle, and the key is the piece that solves it. An attacker studies the encrypted data closely, examining how it changes when different keys are used. They might try to exploit patterns or weaknesses in the encryption algorithm itself. If they succeed in figuring out how the encryption works and deduce the key, they can unlock the encrypted data. This is why it's essential to keep the encryption key secret and to use strong encryption methods that are resistant to these types of attacks.

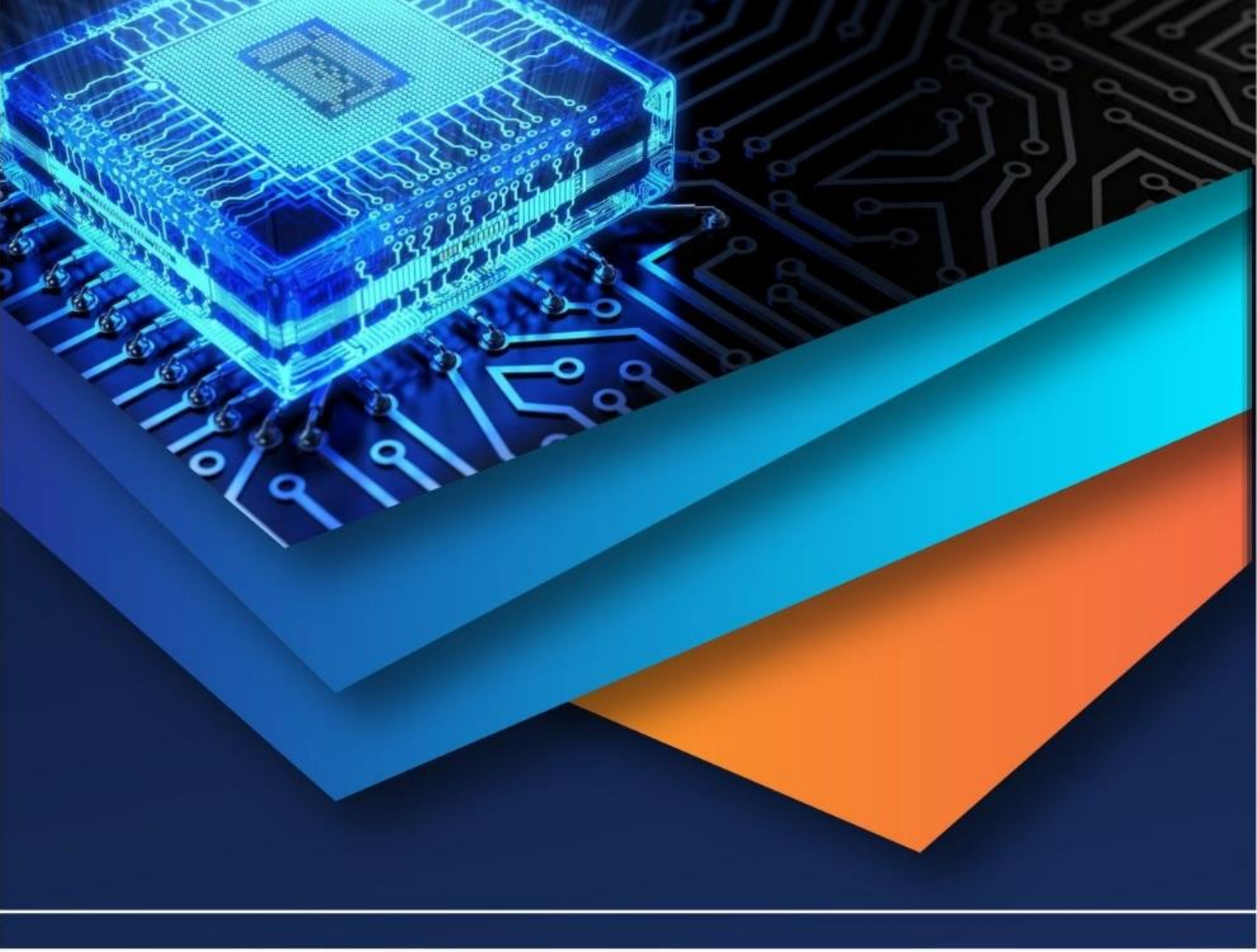
V. CONCLUSION

In conclusion, while cryptography serves as a fundamental pillar for securing data shared over networks, it is not impervious to the efforts of determined hackers aiming to unveil the original information from encrypted data. These malicious actors employ various types of attacks in their pursuit of sensitive data across networked environments. Each of these attacks exerts its influence on cryptography algorithms in distinctive ways. Furthermore, the impact of these attacks varies depending on the encryption techniques in use. Consequently, the diverse landscape of encryption methods is met with a corresponding array of attack strategies, underlining the critical importance of prudent algorithm selection and rigorous implementation practices to fortify the safeguarding of information in networked communications. Staying attuned to the evolution of cryptographic methods and embracing robust security measures remains paramount to counteracting emerging threats and vulnerabilities.

REFERENCES

[1] Mohammed, Abdalbasit & Varol, Nurhayat. (2019). A Review Paper on Cryptography. 1-6. 10.1109/ISDFS.2019.8757514.
[2] F. Piper and S. Murphy, Cryptography: A Very Short Introduction, London: Oxford University Press, 2002
[3] J. P. Aumasson, SERIOUS CRYPTOGRAPHY A Practical Introduction to Modern Encryption, San Francisco: No Starch Press, Inc, 2018

[4] B. Preneel, Understanding Cryptography: A Textbook for Students and Practitioners, London: Springer, 2010.
[5] Jagpreet Kaur, K .R. Ramkumar, The recent trends in cyber security: A review, Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 8, Part B, 2022, Pages 5766-5781
[6] W. Chen, W. Du, W. Ma, J. Li, N. Li, Y. Zhang, A survey on quantum cryptography, Chin. J. Electron., 27 (2) (2018), pp. 223-228
[7] Web content available at : https://www.packetlabs.net/posts/cryptography-attacks/
[8] Web content available at : Cryptography Research Paper - 3123 Words | Studymode
[9] Bhumika Charnanand, Ashish Chaturvedi, Comparative Analysis of standard Cryptographic Algorithms for better implementation of cryptographic Technique, Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)2021.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY