AN EVALUATION OF ENCRYPTION, DECRYPTION, AND THE ROLE OF CRYPTANALYSIS WITHIN MODERN CRYPTOGRAPHIC METHODS

Najimova Baxtigul Abdilkasim qizi
Karakalpak State University named after Berdakh Economics faculty, Department of fundamentals of Management and Economics, 3rd year student majoring in Marketing
najimovabaxtigul1@gmail.com

Annotation: *This paper evaluates the fundamental components of modern cryptographic systems, focusing on the mechanics of encryption, decryption, and the counter-balancing role of cryptanalysis. It analyzes the structural divisions between symmetric, asymmetric, and hash functions within digital platforms. Furthermore, it examines how cryptanalysis identifies operational vulnerabilities within implementation pipelines rather than breaking mathematical algorithms directly. The study concludes that securing digital economy infrastructures requires a comprehensive approach that reinforces both cryptographic algorithms and systematic implementation workflows.*

Key words: *Cryptography, Encryption, Decryption, Cryptanalysis, Symmetric Cryptography, Asymmetric Cryptography, Hash Functions, Data Integrity.*

INTRODUCTION

Cryptography is the process of hiding or coding information so that only the person a message was intended for can read and interpret it. The art and science of cryptography have been used to encode sensitive messages for thousands of years, and it continues to serve as the structural backbone for modern bank cards, computer passwords, and secure e-commerce platforms.

A cryptographic algorithm utilizes a specialized key (which can be a secret private key or a public key consisting of a specific string of bits) to systematically convert readable plaintext into scrambled ciphertext, or vice versa. This mathematical framework is actively used to keep digital communication safe, private, and secure between interacting parties.

Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it. The art of cryptography has been used to code messages for thousands of years and continues to be used in bank cards, computer passwords, and ecommerce.

A cryptographic algorithm uses a key (secret key and public key), a string of bits, to convert plaintext to cipher text or vice versa. It is utilized to keep communication safe and secure between two parties.

The Importance Of Cryptography

Cryptography remains important to protecting data and users, ensuring confidentiality, and preventing cyber criminals from intercepting sensitive corporate information. Common uses and examples of cryptography include the following:

Privacy and confidentiality

Individuals and organizations use cryptography on a daily basis to protect their privacy and keep their conversations and data confidential. Cryptography ensures confidentiality by encrypting sent messages using an algorithm with a key only known to the sender and recipient. A common example of this is the messaging tool WhatsApp, which encrypts conversations between people to ensure they cannot be hacked or intercepted.

Cryptography also secures browsing, such as with virtual private networks (VPNs), which use encrypted tunnels, asymmetric encryption, and public and private shared keys. It plays a similar role in cloud encryption, where data stored and transmitted in cloud environments is encoded to ensure it remains protected from unauthorized access.

Authentication

Authentication verifies the definitive identity of the communicating entities. Cryptography provides cryptographic proofs, such as digital certificates, to ensure that a sender or a user accessing a financial database is exactly who they claim to be, thereby preventing spoofing and identity theft in electronic transactions.

Integrity

Similar to how cryptography can confirm the authenticity of a message, it can also prove the integrity of the information being sent and received. Cryptography ensures information is not altered while in storage or during transit between the sender and the intended recipient. For example, digital signatures can detect forgery or tampering in software distribution and financial transactions.

Nonrepudiation

Cryptography confirms accountability and responsibility from the sender of a message, which means they cannot later deny their intentions when they created or transmitted information. Digital signatures are a good example of this, as they ensure a sender cannot claim a message, contract, or document they created to be fraudulent. Furthermore, in email nonrepudiation, email tracking makes sure the sender cannot deny sending a message and a recipient cannot deny receiving it.

What is Encryption?

Encryption is the process of scrambling or enciphering data so it can be read only by someone with the means to return it to its original state. It is a crucial feature of a safe and trustworthy Internet. It helps provide data security for sensitive information.

How Encryption works?

Encryption is commonly used to protect data stored on computer systems and data transmitted via computer networks, including the Internet. Financial transactions and private messaging communications often use encryption to increase security. Encryption is important when we need to find out whether data has been tampered with (data integrity), to increase people’s confidence that they are communicating with the

people they think are communicating with (authentication) and to be sure that messages were sent and received (non-repudiation).

For data communicated over a network, modern encryption scrambles data using a secret value or key known only by the recipient and the sender. For stored data, the secret value is typically known only by the data owner. There are different types of encryption and the best systems balance safety and efficiency.

What is Decryption?

Decryption is a process through which the already encrypted data or ciphertext is returned to its readable form, usually referred to as plaintext. A piece of data becomes unreadable if it is encrypted since it undergoes some special algorithm with a unique key. Thus, it will become undecipherable for any person who does not possess the right decryption key. The process of decryption, hence, involves the application of the right decryption algorithm together with the appropriate key of decryption so that the encryption is reversed and an original form is restored from the given data.

How Does Decryption Work?

The decryption process typically involves the following steps:

● Receiving the encrypted data: The next step involves the recipient receiving the ciphertext, followed by its decryption. The recipient gets the jumbled-up characters that are unreadable.

● Application of decryption algorithm: In the recipient's system, a predefined decryption algorithm is applied to the ciphertext. By definition, this has to be the same as the one securing the data in the first instance with an encryption algorithm.

● Application of the decryption key: A decryption key is applied to the algorithm. This would reverse the encryption process if the right key was in place.

Types of Cryptography

The majority of encryption techniques can be divided into three categories: symmetric cryptography algorithms, and asymmetric cryptography algorithms, and hash functions while hybrid systems like the SSL internet protocols do exist.

The types of cryptography:

1. Symmetric Key Cryptography
2. Asymmetric Key Cryptography
3. Hash Functions

Symmetric Key Cryptography

Symmetric key encryption, commonly referred to as private key cryptography, secret key cryptography, or single key encryption, uses a single key for both the encryption and decryption processes. Every user needs to have access to the same private key in these kinds of systems. Private keys can be exchanged using a Diffie-Hellman key agreement or, more accurately, through a secure key exchange technique like a previously established secure communication channel such as a private courier or secured line.

So we can use the same key to lock and unlock messages. It is like having a secret code that you and your friend both know. It is very simple and fast. The two parties share the key in a secure way.

Two categories of symmetric key algorithms exist:

● Block Cipher − The cipher algorithm operates on a fixed-size block of data in a block cpher. As an example, eight bytes of plaintext are encrypted at a time if the block size is eight. When handling data larger than the block size, the user interface for the encrypt/decrypt process typically calls multiple times the low-level cipher function.

● Stream Cipher − Stream ciphers transform data one bit (or one byte) at a time instead of operating on a block basis. Simply say, a stream cipher uses a given key to generate a keystream. The plaintext data is then XORed with the generated keystream.

Asymmetric Key Cryptography

Unlike symmetric encryption cryptography, we use two keys in this type of cryptography: one for encryption and second one for decryption. Since these keys can be reused several times and are only used once per message, they do not need to be kept secret. Public-key systems are the most common use case for asymmetric key cryptography.

Two keys are utilised in asymmetric encryption: a secret key and a public key. Because of this, another name for these algorithms is public key algorithms (PKA). Since only the intended recipient's private key can be used to decipher an encrypted message, public key cryptography is typically thought to be more secure than symmetric encryption methods, even though one key is made available to the public.

Asymmetric key cryptography has many examples, like the followig:

● Rivest, Shamier, and Adleman (RSA) − One of the first widely used public key cryptosystems for secure data transmission, the RSA algorithm was founded in 1977 and is named for its authors, Rivest, Shamier, and Adleman.

● Elliptic curve cryptography (ECC) − It is a modern type of asymmetric encryption that generates very strong cryptographic keys using the algebraic structures of elliptic curves.

Hash Functions

A hash function is like a special mathematical function which takes an input of arbitrary data like text, numbers, or files and converts it into a fixed-length string called a hash. We can say it is like a fingerprint for your data. Hash function can process any size of data but always gives output of fixed length value. The output is much smaller than the input.

Suppose you own a library that has millions of volumes. You are not going through each book's page by page in the hope to quickly find a specific book. An index will be used instead, connecting unique page numbers (hashes) to book titles (data). Hash functions behave similarly for storing and retrieving data.

The following claims about a decent hash function are accurate for all purposes and reasons:

● Collision-resistant – Data integrity is maintained by generating a new hash whenever any part of the data is changed.

● One-way – This function cannot be undone. To ensure data security, a digest needs to make it impossible to locate the original data.

What is cryptanalysis?

Cryptanalysts examine cryptographic systems with the aim of discovering vulnerabilities or flaws that could be exploited, breaking the system's security.

Cryptanalysts use a variety of techniques to analyze how encrypted information might be cracked. These techniques range from mathematical analysis of encryption algorithms to exploiting weaknesses in the way the encryption was implemented.

Weaknesses may arise in the pipeline that implements cryptographic algorithms. The goal of cryptanalysis is precisely, to understand how cryptography is implemented within a system and identify weaknesses within this pipeline. A weakness itself may render the cryptographic implementation as ineffective.

For example, your messaging app may use strong encryption protocols for all data in transit between the user device and the backend communication servers. A security weakness may exist in the messaging app itself. For example, a vulnerability may allow malicious actors to read the keystrokes when typing a message and then exfiltrate this information to an external server.

This information will be sufficient to reproduce the original message from the sender, without having to access or decrypt the user's encrypted data. A decryption key is not required to read the message. This is because the cryptography algorithm only protects data in transit, not the plaintext produced and stored within the application or device itself.

Conclusion

Modern cryptography is essential for securing the digital economy through encryption, decryption, and hash functions. While symmetric and asymmetric methods protect data speed and key exchange, cryptanalysis proves that mathematical strength alone is not enough. True digital security depends on the entire implementation pipeline, requiring continuous updates to protect software and hardware platforms from evolving system vulnerabilities.

REFERENCES:

1. What Is Cryptography?
https://www.fortinet.com/resources/cyberglossary/what-is-cryptography

2. What is Cryptography? Rudra Mehta Feb 8, 2024 https://medium.com/@rudra-mehta/what-is-cryptography-a4cf707d46f6

3. What is Encryption?
https://www.internetsociety.org/issues/encryption/what-is/

4. What is Decryption? How It Enhances Data Security Author: SentinelOne Updated: July 16, 2025 https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-decryption/

5. Cryptography - Types
https://www.tutorialspoint.com/cryptography/cryptography_types.htm

6. What is Cryptanalysis? A Detailed Introduction By Muhammad Raza APRIL 21, 2025 https://www.splunk.com/en_us/blog/learn/cryptanalysis.html