Review on Importance of Cryptography and Its Effect on the World

Rahul Gupta
Department of Computer Science of Engineering,
Lovely Professional University, Phagwara, Punjab, India

Abstract— Cryptography is an effective technique to protect highly confidential and valuable information from cybercriminals. Cryptography is the practice of secure communication in the presence of third parties, and it provides various techniques and keys to protect information. The history of cryptography dates to ancient times, where people used various techniques to protect their messages from being intercepted or read by unauthorized individuals. Today, cryptography has evolved significantly, and there are different types and principles of cryptography, including symmetric key cryptography, asymmetric key cryptography, and hashing. Despite the effectiveness of cryptography in protecting information, there is always a possibility that cybercriminals could access confidential data. It is, therefore, crucial to keep up with technological advancements and learn how to outsmart cybercriminals to safeguard sensitive information.

Keywords:— Cryptography, Algorithms, code, encryption, decryption, Security, Cipher, Data Security, Symmetric, asymmetric.

1. INTRODUCTION

Cryptography is the science of secure communication, which involves converting information into a secret code that can only be deciphered by authorized parties. It is an essential tool for safeguarding sensitive information from unauthorized access and manipulation.

The importance of cryptography in today's world cannot be overstated. With the rapid advancement of technology, the need for secure communication has become more pressing than ever before. Cryptography is used to protect sensitive data such as financial transactions, personal information, and military secrets. Without cryptography, these data would be vulnerable to interception and manipulation by unauthorized parties, leading to disastrous consequences for individuals, businesses, and governments. The impact of cryptography on the world has been significant. It has enabled secure online transactions, protected intellectual property, and facilitated secure communication between governments and businesses. Cryptography has also played a crucial role in protecting privacy and freedom of speech in countries where these rights are under threat. The widespread adoption of cryptography has also led to the development of new technologies and industries. For example, blockchain technology relies heavily on cryptographic techniques to ensure the security and transparency of transactions. The growth of the cybersecurity industry is also a direct result of the increasing need for secure communication and data protection.

2. Literature Review

"Cryptography and Its Role in Securing the Information Society" by David A. Balenson, published in the Journal of Information Security - This article discusses the importance of cryptography in securing the information society, protecting privacy and intellectual property, and ensuring the integrity and confidentiality of data. It also highlights the role of cryptography in facilitating e-commerce and securing online transactions.

"The Role of Cryptography in Cybersecurity" by A. Nur Zincir-Heywood and Evangelos Kranakis, published in the IEEE Security & Privacy Magazine - This article discusses the role of cryptography in cybersecurity and its importance in protecting sensitive information, securing communication channels, and preventing cyber-attacks. It also explores the challenges and limitations of cryptography in the context of modern threats and emerging technologies.

"The Importance of Cryptography in Digital Forensics" by Thomas J. Holt and Adam M. Bossler, published in the Journal of Digital Forensics, Security and Law - This article discusses the importance of cryptography in digital forensics and its role in protecting evidence, ensuring data integrity, and facilitating the investigation of cyber-crimes. It also explores the challenges and opportunities of using cryptography in digital forensics.

"The Role of Cryptography in Blockchain Technology" by Muhammad I. Sarfraz and Sajid Hussain, published

in the Journal of Information Security and Applications - This article discusses the role of cryptography in blockchain technology and its importance in securing transactions, preventing fraud, and ensuring the transparency and accountability of distributed ledger systems. It also explores the challenges and opportunities of using cryptography in the context of blockchain-based applications.

"Cryptography and National Security" by Ryan Henry and Michael Sulmeyer, published in the Harvard National Security Journal - This article discusses the importance of cryptography in national security and its role in protecting military secrets, preventing espionage, and securing critical infrastructure. It also explores the challenges and trade-offs of balancing national security concerns with privacy and civil liberties.

"Cryptography and Network Security: Principles and Practice" by William Stallings - This book provides a comprehensive overview of cryptography and its applications in network security. It covers topics such as encryption, digital signatures, and key management, and discusses the impact of cryptography on modern society.

"The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography" by Simon Singh - This book explores the history of cryptography, from ancient civilizations to modern times. It discusses how cryptography has been used to protect secrets, wage wars, and secure communication, and highlights the importance of cryptography in modern society.

"Cryptography: An Introduction" by Nigel Smart - This book provides a beginner-friendly introduction to cryptography and its applications. It covers topics such as symmetric and asymmetric encryption, digital signatures, and key exchange protocols, and discusses he importance of cryptography in securing modern communication.

"Cryptonomicon" by Neal Stephenson - This novel explores the history of cryptography through the eyes of a group of codebreakers during World War II and their modern-day counterparts. It highlights the importance of cryptography in both historical and modern contexts and emphasizes its impact on the world.

"Applied Cryptography: Protocols, Algorithms, and Source Code in C" by Bruce Schneier - This book provides a practical guide to cryptography and its applications. It covers topics such as encryption, digital signatures, and authentication, and discusses the impact of cryptography on modern society.

3. Two major techniques in cryptography

3.1 Symmetrical Cryptography: -

Symmetric cryptography, also known as secret-key cryptography, is a type of encryption in which the same key is used for both encryption and decryption of data. The sender and receiver of the data must both have the key and agree on its use. Symmetric encryption algorithms are generally faster and require less processing power than asymmetric algorithms, but they suffer from the disadvantage of requiring the key to be transmitted securely between the sender and receiver.

One example of a symmetric encryption algorithm is the Data Encryption Standard (DES), which was developed in the 1970s and is still in use today. Other popular symmetric encryption algorithms include Advanced Encryption Standard (AES) and Blowfish. These algorithms use a block cipher method in which the message to be encrypted is divided into fixed-size blocks and then encrypted using the same key. Symmetric cryptography is widely used in many applications, including secure communication over the internet, digital signatures, and password protection. However, because of the need to securely transmit the key, it is generally not suitable for use in situations where the sender and receiver have not previously communicated and agreed on a key. As a result, public-key or asymmetric cryptography is often used in these situations.

3.2 Asymmetrical Cryptography: -

Asymmetric cryptography, also known as public key cryptography, is a cryptographic system that uses a pair of keys, one for encryption and the other for decryption. This contrasts with symmetric cryptography, which uses the same key for both encryption and decryption. In an asymmetric cryptography system, each user has a pair of keys, a public key and a private key. The public key is shared with others and is used to encrypt messages that only the holder of the private key can decrypt. The private key is kept secret and is used to decrypt messages that have been encrypted with the corresponding public key. Asymmetric cryptography has a number of advantages over symmetric cryptography. One of the main advantages is that it eliminates the need for a secure channel to transmit the key between the sender and receiver, which is a significant challenge in symmetric cryptography.

Asymmetric cryptography also allows for digital signatures and other important cryptographic operations that are not possible with symmetric cryptography alone.

4. Basic Concept of Cryptography

The basic concept of a cryptographic system is to transform plaintext into ciphertext using encryption algorithms and encryption keys to achieve confidentiality, integrity, and authentication of the information being transmitted. The encrypted information can only be read by someone who has the correct decryption key and decryption algorithm. Cryptography is commonly used to protect sensitive information, such as financial transactions, personal data, and military communications, and to secure digital signatures and certificates.

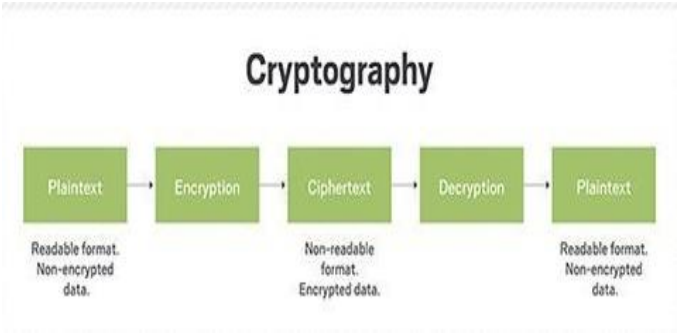

Figure.1 Concept of Cryptography
(Ref:https://www.techtarget.com/searchsecurity/definition/cryptography)

4.1 Some Important Principles of Cryptography:

4.11 Encryption: Encryption is one of the fundamental principles of cryptography, and it involves the process of converting plaintext into ciphertext using mathematical algorithms and a secret key. The ciphertext is unreadable and appears as a random sequence of characters or symbols. The purpose of encryption is to protect the confidentiality of the information being transmitted and prevent unauthorized access by third parties.

4.12 Authentication: Authentication is another fundamental principle of cryptography, and it involves verifying the identity of the sender of the information. Authentication is important to ensure that the information received is legitimate and has not been tampered with or modified by an unauthorized party.

4.13 Integrity: Integrity of information sent to the receiver is very important. This principle indicates that cryptography ensures the integrity of data by providing codes and digital keys to ensure that what we receive is genuine and from the intended person. The receiver is assured that the information received has not been modified or compromised during the process of transmission. For example, a cryptographic hash is utilized to ensure the integrity of the information.

4.2 Types Of Cryptography: -

4.2.1 Secret key Cryptography: -

Secret key Cryptography is a type of Cryptographic system that uses the same secret key for both encryption and decryption of the information. It is widely used in various applications but requires secure distribution and management of the secret key to ensure the confidentiality and integrity of the encrypted information.

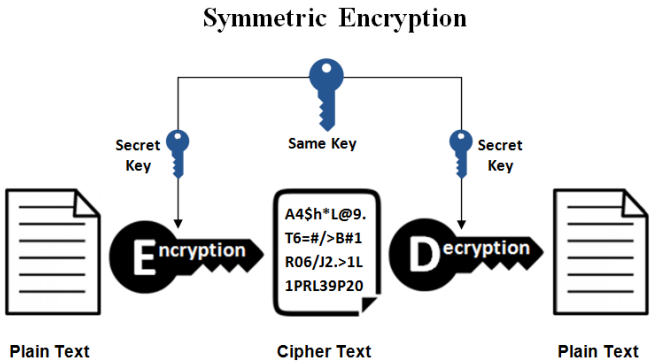

Figure.2 Secret key Cryptography.
(Ref: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences)

4.2.2 Public key Cryptography: -

Public key cryptography is a type of cryptographic system that uses two different keys for encryption and decryption of the information. The public key is made public, while the private key is kept secret. It allows for secure communication without the need for a pre-shared secret key and is commonly used for secure communication, digital signatures, and access control.

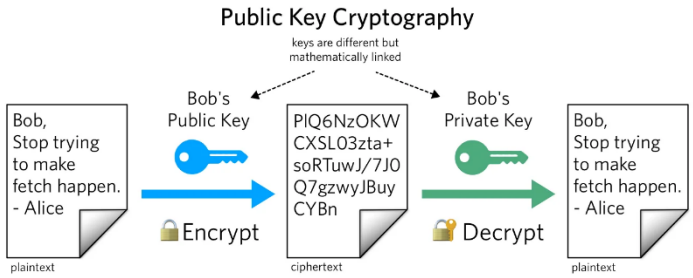

Figure.3 Public key Cryptography
(Ref: https://www.twilio.com/blog/what-is-public-key-cryptography)

5. HISTORICAL ALGORITHMS: -

These algorithms were designed and used long before public key cryptography was proposed.

5.1 Caesar Cipher: - The Caesar Cipher is one of the simplest examples of cryptography and is very easy to break by modern standards. However, it was considered a strong method of encryption in ancient times, particularly during the time of Julius Caesar when knowledge of the alphabet and the ability to read and write were not as widespread as they are today.

The Caesar Cipher belongs to the category of substitution ciphers, where each letter of the plaintext is replaced by another letter, number, or symbol. While the Caesar Cipher uses a fixed shift of 3, other substitution ciphers can use different types of shifts or even more complex rules for replacing letters.

Figure.4 Caesar Wheal

(Ref: https://tex.stackexchange.com/questions/103364/how-to-create-a-caesars-encryption-disk-using-latex)

Despite its simplicity, the Caesar Cipher is still used today as a basic introduction to cryptography for beginners and as a building block for more complex encryption methods. It is also sometimes used as a form of steganography, where the hidden message is not the ciphertext itself, but rather the fact that a message has been encrypted using the Caesar Cipher.

5.2 Simple Substitution Ciphers: -

The Simple Substitution Cipher, also known as the Monoalphabetic Cipher, is another example of a basic cryptography technique. In this cipher, each letter of the alphabet is mapped to a different letter in a one-to-one correspondence. The mapping is typically done by placing the letters of the alphabet in a random order below the normal alphabet. For example, A might be mapped to Q, B to Z, C to L, and so on. To encrypt a message, each letter of the plaintext is replaced with the corresponding letter in the mapping.

A	B	C	D	E	F	G	H	I	J	K	L
D	**I**	**Q**	**M**	**T**	**B**	**Z**	**S**	**Y**	**K**	**V**	**O**
M	N	O	P	Q	R	S	T	U	V	W	X
F	**E**	**R**	**J**	**A**	**U**	**W**	**P**	**X**	**H**	**L**	**C**
Y	Z										
N	**G**										

For example, the plaintext "CAN" might be encrypted as "QDN". The Simple Substitution Cipher is stronger than the Caesar Cipher, as it can be more difficult to break using frequency analysis or other techniques. However, it is still vulnerable to attacks such as letter frequency analysis, where an attacker can analyse the frequency of letters in the ciphertext to deduce the mapping used in the encryption.

Overall, the Simple Substitution Cipher is a basic cryptography technique that can be used for educational purposes or as part of more complex encryption algorithms. However, it is not suitable for use in high-security applications where stronger encryption methods are necessary.

5.3 Transposition Ciphers: -

A transposition cipher is a type of encryption method that rearranges the letters of a plaintext message without changing them to different symbols or characters. Instead, the transposition cipher changes the order of the characters in the message according to a specific rule and a key. The goal of a transposition cipher is to obscure the meaning of the original message, making it difficult to read or understand without knowledge of the key and the specific transposition rule.

One common type of transposition cipher is the columnar transposition cipher, which arranges the letters of the plaintext message into a rectangle shape with a width that corresponds to the length of the key. The message is then read column by column in a specific order determined by the key. Another example of a transposition cipher is the rail fence cipher, which rearranges the letters of the plaintext message in a zigzag pattern along a set number of rails, and then reads the characters off the rails in a specific order.

1	**2**	**3**	**4**	**5**	**6**
s	e	c	o	n	d
d	i	v	i	s	o
n	a	d	v	a	n
c	i	n	g	t	o
n	i	g	h	t	x

The cipher text is then derived from the columns depending on the key. In this example, if we used the key “321654”, the cipher text is going to be:

cvdng eiaii sdncn donox nsatt oivgh

6. MODERN ALGORITHMS: -

6.1 Stream ciphers: -

Stream ciphers are a type of symmetric-key cipher that encrypts plaintext by generating a keystream of random bits or bytes, and then combining it with the plaintext using bitwise XOR operation. The keystream is generated by a secret key and a nonce (a number used only once), and it is combined with the plaintext bit-by-bit, producing the ciphertext. Unlike block ciphers, which divide the plaintext into fixed-size blocks and encrypt each block independently, stream ciphers encrypt the plaintext continuously, bit-by-bit, and therefore, they are suitable for encrypting data in real-time applications such as streaming video or voice.

One advantage of stream ciphers is that they are usually faster and require less memory than block ciphers, which makes them suitable for applications with limited resources. However, they are vulnerable to certain attacks, such as a known-plaintext attack, in which an attacker can recover the key if they have access to both the plaintext and the corresponding ciphertext.

Examples of well-known stream ciphers include RC4, Salsa20, and ChaCha.

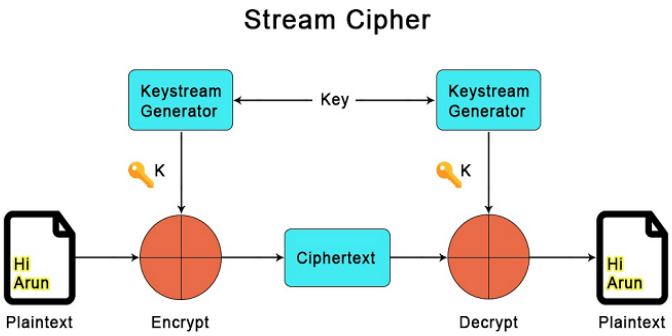

Figure.5 Stream Cipher
(Ref: https://www.javatpoint.com/block-cipher-vs-stream-cipher)

6.2 Block ciphers: -

A block cipher is a type of symmetric-key encryption algorithm that operates on fixed-size blocks of data, typically 64 or 128 bits in length. The plaintext is divided into blocks of equal size, and each block is encrypted independently using the same secret key. The most common mode of operation for block ciphers is the Electronic Codebook (ECB) mode, which encrypts each block of plaintext independently using the same key. However, this mode is vulnerable to certain attacks, such as a known-plaintext attack, in which an attacker can recover the key if they have access to both the plaintext and the corresponding ciphertext. To mitigate these attacks, other modes of operation have been developed, such as the Cipher Block Chaining (CBC) mode, which XORs each plaintext block with the ciphertext block of the previous block before encryption, and the output of this XOR operation is then encrypted. This adds a form of randomness to the encryption process and makes it more difficult for an attacker to recover the key. Other modes of operation include the Counter (CTR) mode, which uses a counter to generate a keystream that is XORed with the plaintext, and the Galois/Counter Mode (GCM), which combines the Counter mode with Galois field multiplication to provide both confidentiality and integrity protection.

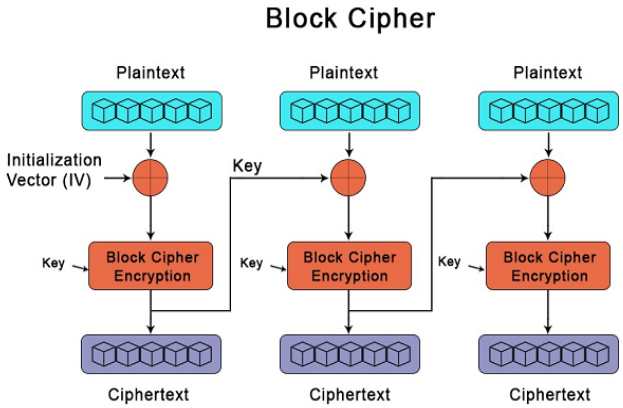

Figure.6 Block Cipher
(Ref: https://www.javatpoint.com/block-cipher-vs-stream-cipher)

Well-known examples of block ciphers include Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES.

6.3 Hash functions: -

A hash function is a mathematical function that takes an input (or message) of arbitrary size and produces a fixed-size output, called a hash or message digest. The output of a hash function is typically a sequence of digits or letters that uniquely represents the input message. Hash functions are used for a variety of purposes in cryptography and computer security, such as password storage, digital signatures, and message authentication codes (MACs). They are also used in data structures such as hash tables and bloom filters.

1. A good hash function should have several properties, including:

2. Determinism: The output of the function should be deterministic for the same input.

3.Uniformity: The output of the function should be uniformly distributed across the possible range of output values.

4.Collision resistance: It should be difficult to find two different inputs that produce the same hash output.

5.One-wayness: It should be computationally infeasible to determine the input from the output hash value.

6.Efficiency: The hash function should be efficient to compute.

7. Examples of commonly used hash functions include SHA-256, SHA-3, and MD5 (although MD5 is no longer recommended due to its vulnerabilities).

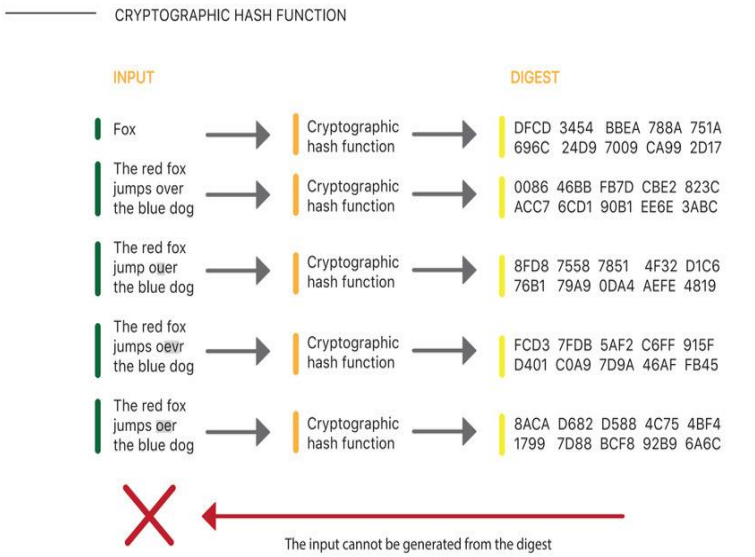

Figure.7 Hash Function

(Ref: https://www.researchgate.net/figure/Cryptographic-Hash-Function_fig4_327552198)

6.4 RSA Algorithm: -

RSA is a widely used public key encryption algorithm named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman. It is based on the mathematical properties of prime numbers and is commonly used for secure data transmission and digital signatures. In RSA, each user has a public key and a private key. The public key is used for encrypting messages, while the private key is used for decrypting messages. The security of the algorithm is based on the fact that it is difficult to factorize large composite numbers into their prime factors, which is the basis for the key generation process.

The key generation process involves the following steps:

Choose two large prime numbers, p and q.

→ Compute n = p x q.

- Compute the Euler's totient function of n, φ(n) = (p-1) (q-1).
- Choose an integer e such that 1 < e < φ(n) and e is coprime to φ(n).
- Compute the modular multiplicative inverse of e modulo φ(n), which is denoted as d, such that e x d ≡ 1 (mod φ(n)).
- The public key is (n,e) and the private key is (n,d).

To encrypt a message using RSA, the sender encrypts the message M by computing C = M^e (mod n) using the recipient's public key (n,e). To decrypt the message, the recipient computes M = C^d (mod n) using their private key (n,d).

RSA is also used for digital signatures, where the sender signs a message by computing a hash of the message and then encrypting the hash with their private key. The recipient can then verify the signature by decrypting the hash using the sender's public key and comparing it with the hash of the original message.

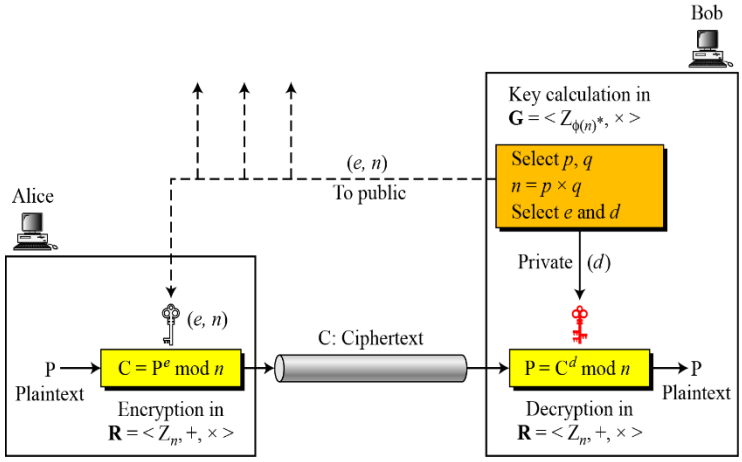

Figure.8 RSA Algorithm

(Ref: https://people.utm.my/marinama/files/2016/11/Ch-10-Asymmetric-Key-Cryptography-for-students.pdf)

6.5 Public key systems: -

The invention of public key encryption was a significant milestone in the field of cryptography, as it allowed for secure communication over public channels without the need for pre-shared secret keys. Prior to the development of public key encryption, cryptography was mainly used in military and intelligence applications, where secure communication was essential. However, the introduction of public key encryption opened new possibilities for secure communication in other areas, such as finance, e-commerce, and personal communication. The use of public key encryption eliminates the need for private channels to exchange keys, as the public key can be freely distributed without compromising the security of the system. This has made secure communication more accessible and convenient for individuals and organizations and has greatly improved the privacy and security of electronic communication.

1) Public key encryption allows for secure communication between parties without the need

for a shared secret key. This is because each party has a public key and a private key. The public key can be freely distributed, allowing anyone to encrypt messages that can only be decrypted by the private key holder. This means that key distribution can be done over a public channel, making the system's initial deployment much simpler.

2) Public key encryption eliminates the need for parties to share a secret key, which simplifies the storage of secret keys. Instead, each party generates their own public and private key pair, with the private key kept securely by the party and the public key distributed to other parties.

3) Public key cryptography is particularly well-suited for open environments where parties may not have interacted previously and where secure communication is required. This is because public key cryptography allows parties to establish secure communication without needing to pre-share a secret key, which can be impractical or impossible in open environments.

6.6 DIGITAL SIGNATURES: -

A digital signature is a mathematical scheme used to validate the authenticity and integrity of a digital message or document. It is similar to a handwritten signature, but instead of being a physical mark on a document, it is a digital code that is attached to the document. A digital signature provides the recipient with a way to verify that the message or document was sent by the claimed sender and that it has not been altered or tampered with in transit. Digital signatures are typically created using public key cryptography. The sender of a message or document uses their private key to generate a unique digital code, known as a signature, that is attached to the document. The recipient of the message or document can then use the sender's public key to verify that the signature is authentic and that the document has not been altered since it was signed.

The use of digital signatures provides several benefits, such as:

Authentication: Digital signatures provide a way to authenticate the identity of the sender of a message or document.

Integrity: Digital signatures provide a way to ensure that a message or document has not been tampered with in transit.

Non-repudiation: Digital signatures provide a way to prevent the sender from denying that they sent a message or document.

Digital signatures are commonly used in e-commerce, online banking, and other applications where the authenticity and integrity of digital transactions are critical.

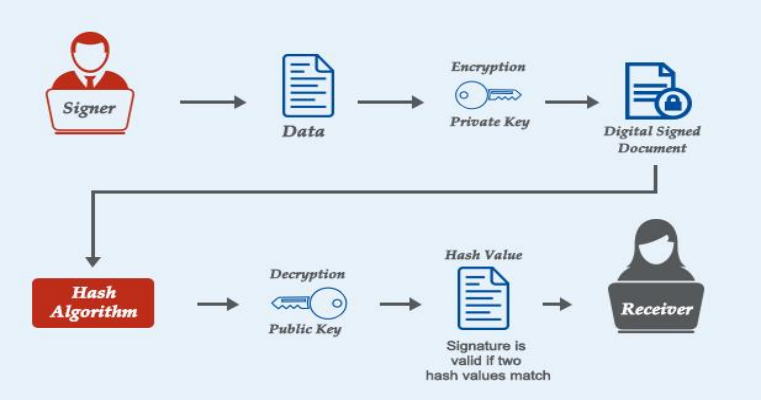

Figure.9 Digital Signature

(Ref: https://comodosslstore.com/blog/what-is-digital-signature-how-does-it-work.html)

CONCLUSION: -

Cryptography plays a crucial role in ensuring the confidentiality, integrity, and authenticity of digital communications and transactions in today's interconnected world. It allows individuals, organizations, and governments to securely store and transmit sensitive information, such as financial data, personal information, and classified government communications. The use of cryptography has led to significant advancements in areas such as e-commerce, online banking, and secure communication. It has also enabled the development of secure and decentralized systems, such as blockchain technology, which are revolutionizing the way we store and transmit data. However, cryptography is not a fool proof solution and can be vulnerable to attacks and breaches if not implemented correctly. As such, it is important for individuals and organizations to stay up-to-date on the latest cryptographic technologies and best practices to ensure the security of their data.

REFERENCES: -

1) N. Sharma, Prabhjot and H. Kaur, "A Review of Information Security using Cryptography Technique," International Journal of Advanced Research in Computer Science, vol. 8, no. Special Issue, pp. 323-326, 2017.

2) B. Preneel, Understanding Cryptography: A Textbook for Students and Practitioners, London: Springer, 2010.

3) J. Katz and Y. Lindell, lntroduct:ion t:o Modern Cryptography, London: Taylor & Francis Group, LLC , 2008.

4) S. J. Lincke and A. Hollan, "Network Security: Focus on Security, Skills, and Stability," in 37th ASEE/IEEE Frontiers in Education Conference, Milwaukee, 2007

5) O. O. Khalifa, M. R. Islam, S. Khan, and M. S. Shebani, "Communications cryptography," in RF and Microwave Conference, 2004. RFM 2004. Proceedings, Selangor, 2004

6) N. Jirwan, A. Singh and S. Vijay, "Review and Analysis of Cryptography Techniques," International Journal of Scientific & Engineering Research, vol. 3, no. 4, pp. 1-6, 2013 .

7) S. Tayal, N. Gupta, P. Gupta, D. Goyal and M. Goyal, "A Review paper on Network Security and Cryptography," Advances in Computational Sciences and Technology, vol. 10, no. 5, pp. 763-770, 2017.

8) A. Gupta and N. K. Walia, "Cryptography Algorithms: A Review," NTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH, vol. 2, no. 2, pp. 1667-1672, 2014.

9) White, T, Encrypted Objects and Decryption Processes: Problem-Solving with Functions in a Learning Environment Based on Cryptography. Educational Studies in Mathematics,72(1), p17-37, 2009.