IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

A Review Paper on Cryptography

Shreyas M[1], Sudarshan U B[2], Rahul Verneker[3], Mrs. Ankitha S[4], Mr. Sayeesh[5]
Students, Department of Computer Science and Engineering[1,2,3]
Associate Professor, Department of Computer Science and Engineering[4]
Sr. Associate Professor, Department of Computer Science and Engineering[5]
Alva's Institute of Engineering and Technology, Mijar, Mangalore, Karnataka

Abstract: *Data security has become a top worry for everybody linked to the internet, as it has merged with our lives and grown at a breakneck pace over the previous several decades. Data security ensures that only the intended recipients have access to our information and prohibits any data modification or manipulation. Various techniques and approaches have been developed to reach this level of security. Cryptography is a set of techniques for encrypting data using specified algorithms that render the data unreadable to the naked eye unless decrypted using predefined procedures by the sender.*

Keywords: Cryptography

I. INTRODUCTION

Cryptography is a method of ensuring message confidentiality. In Greek, the phrase has a special meaning: "hidden writing." Nowadays, however, individuals and organisations' privacy is protected by high-level cryptography, which ensures that information delivered is secure and only the authorised receiver has access to it [1]. Cryptography is a traditional method that is continuously being explored, with historical roots. Examples reach back to 2000 B.C., when the ancient Egyptians used "secret" hieroglyphics, as well as other evidence in the form of secret writings in ancient Greece or the famous Caesar cipher of ancient Rome. Hundreds of millions of people use cryptography on a regular basis to protect data and information, while the majority are unaware of it. Cryptographic systems, in addition to being immensely helpful, are also extremely brittle, as a single programming or specification error might compromise them.

II. LITERATURE REVIEW

Susan et al. pointed out that network and computer security is a new and fast-moving technology within the computer science field, with computer security teaching to be a target that never stops moving. Algorithmic and mathematic aspects, such as hashing techniques and encryption, are the main focus of security courses. As crackers find ways to hack network systems, new courses are created that cover the latest type of attacks, but each of these attacks become outdated daily due to the responses from new security software. With the continuous maturity of security terminology, security techniques and skills continue to emerge in the practice of business, network optimization, security architecture, and legal foundation.

Othman O. Khalifa et al. demonstrated the primary basic concepts, characteristics, and goals of cryptography. They highlighted how communication has contributed to the advancement of technology in our day, i.e. the information age, and thus plays a vital role that demands privacy to be secured and assured when data is conveyed over the medium of communication.

Data communication, according to Nitin Jirwan et al. [6], is primarily based on digital data transmission, in which data security is prioritised when utilising encryption techniques to ensure that data reaches the intended users safely and without being compromised. They also exhibited several cryptography approaches, such as symmetric and asymmetric methods, that are used in the data communication process.

Sandeep Tayal et al. [7] stated in a review on network security and cryptography that the rise of social networks and commerce apps has resulted in massive amounts of data being produced daily by organisations all over the world. As a result, information security becomes a major concern when it comes to ensuring the secure transmission of data over the internet. This issue emphasises the need of cryptographic approaches as more people connect to the internet. This paper gives an overview of the many security approaches utilised by networks, including cryptography.

Anjula Gupta et al. [8] discussed the history and significance of cryptography, as well as how information security has

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

become a difficult problem in the computer and communications areas. This paper also provides various asymmetric algorithms that have given us the ability to protect and secure data, in addition to demonstrating cryptography as a way to ensure identification, availability, integrity, authentication, and confidentiality of users and their data by providing security and privacy.

Cryptography, privacy-enhancing technology, legislative developments related to cryptography, reliability, and privacy-enhancing technologies were all discussed in a research undertaken by Callas, J. [9]. He stated that the future of cryptography will be determined by how society uses it, which is determined by rules, present laws, and practises, as well as what society wants it to do. He stated that there are many gaps in the realm of cryptography that need to be filled by future scholars. Furthermore, the future of cryptography depends on a management system that generates strong keys to ensure that only the proper individuals with the right keys have access, and that others without the keys do not. Finally, Callas stated that people's views and beliefs on security and The privacy of communication varies.

As a result, cryptography will always play a role in data and information security, both today and in the future. Moving on to the objectives of cryptography, James L. Massey [10] pointed out that there are two objectives that cryptography seeks to achieve: authenticity and/or secrecy. He explored both Shannon's theory of theoretical secrecy and Simmon's notion of theoretical authenticity in terms of the security it provides (which can be either practical or theoretical).

Finally, Schneier [11] concluded that security secrecy is a fallacy, and that it is not ideal for security to remain hidden, because security that relies solely on secrecy can be vulnerable. It would be impossible to regain that secret if it was lost. In order to provide effective security, cryptography based on short secret keys that can be quickly shared and updated must rely on a basic principle, according to which cryptographic algorithms must be both strong and public. The only surefire method to increase security is to open yourself up to public scrutiny.

N. Varol et al. [12] investigated symmetric encryption, which is used to encrypt a specific text or speech. The content to be encrypted is first transformed into an encapsulating chipher that a cypher algorithm cannot understand.

Chachapara, K. et al. [13] investigated secure sharing in cloud computing with cryptography and developed a system that uses cryptography algorithms such as RSA and AES, with AES being the most secure algorithm in cryptography. Users of the cloud can produce keys for various users with varying rights to view their files.

Many discussions and developments about cryptography are generated, according to Orman, H. [14]. As the author stated, hash functions play a vital role in cryptography by providing nearly any number to any piece of data, and the years that MD5's flaws became known, it led to an unsettled feeling about how to design hash functions.

R. Gennaro [15] emphasised randomness in cryptography, explaining that a random process has unknown outcomes, and that this is why randomness is important in cryptography since it allows for the creation of information that an adversary cannot learn or predict.

B. Preneel [16] examined mass surveillance tactics and the security of ICT systems in the post- Snowden age, as well as known ways in which sophisticated attackers might bypass or undermine cryptography.

Sadkhan, S. B. [17] discussed the main processes and trends in cryptography from Julius Cesar's time to the modern era, as well as the current status of Arabic industrial and academical efforts in this field in the past, which are related to existing cryptographic and search for new evaluation methods for information security.

III. CRYPTOGRAPHY CONCEPT

The basic premise of a cryptographic system is to encrypt information or data in such a way that an unauthorised person cannot deduce its meaning. Cryptography is commonly used to send data via an unsecured channel, such as the internet, or to ensure that unauthorised persons do not comprehend what they are looking at in a case where they have accessed the information.

In cryptography, the obfuscated data is known as "plaintext," and the process of concealing it is known as "encryption." The encrypted plaintext is known as "ciphertext." This is accomplished by a set of principles known as "encryption algorithms." Typically, the encryption process uses a "encryption key," which is passed to the encryption algorithm together with the data as input. The receiving side can extract the information using a "decryption algorithm" and the associated "decryption key."

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

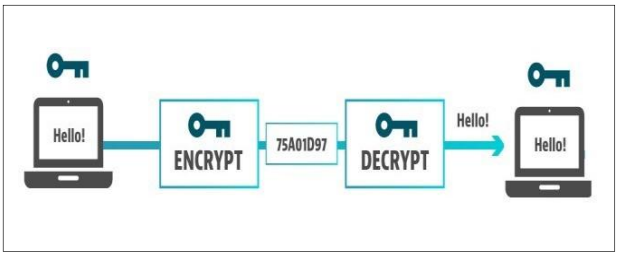

Figure 1: Cryptography concept

IV. HISTORICAL ALGORITHMS

This part will introduce a few historical algorithms, as well as pencil and paper examples for the nonmathematical reader. Long before public key cryptography was suggested, these techniques were developed and utilised.

4.1 Cipher

During the Gallic Wars, Julius Caesar, the Emperor of Rome, devised one of the oldest and earliest versions of cryptography. The letters A through We are encoded using the letters three positions ahead of each letter in the alphabet, while the remaining letters A, B, and C are represented by X, Y, and Z in this type of algorithm. This means that a "shift" of 3 is utilised, while any number between 1 and 25 could be used instead.

The Caesar cypher is easy to crack since it is one of the most basic instances of encryption. The letters that were shifted must be shifted three letters back to their original positions in order to decrypt the ciphertext. Despite this flaw, it may have been robust enough for Julius Caesar to utilise throughout his wars in the past. However, because the shifted letter in the Caesar Cipher is always three, anyone attempting to crack the ciphertext just has to shift the letters [19].

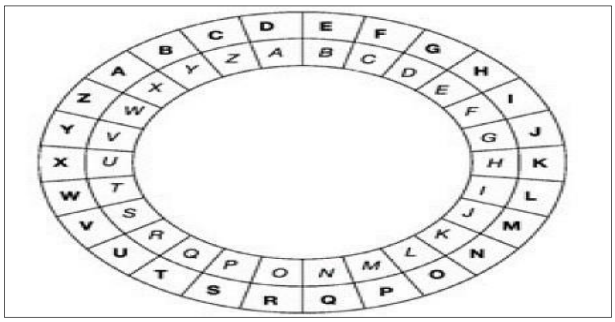

Figure 2: Caesar Cipher encryption wheel

4.2 Ciphers with Simple Substitutions

Take, for example, the Simple Substitutions Cipher, often known as the Monoalphabetic Cipher. In a Simple Substitution Cipher, the alphabet letters are placed in random sequence beneath the correctly written alphabet, as shown here:

A B C D E F G H I J K L M **D I Q M T B Z S Y K V O F**

N O P Q R S T U V W X Y Z

E R J A U W P X H L C N G

The same key is used for encryption and decryption. The rule of encryption is that "each letter is replaced by the letter below it," while the rule of decryption is the inverse. For example, the plaintext CAN's matching ciphertext is QDN [18].

4.3 Ciphers of Transposition

Other cypher families use a key and a specific rule to order the letters in plaintext to convert them to cypher text. Transposition is the process of changing the letters in plaintext using rules and a specific key. a type of columnar One of the simplest varieties of transposition cypher is the transposition cypher, which comes in two flavours: "full columnar

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

transposition" and "incomplete columnar transposition." A rectangular shape is used to represent the written plaintext horizontally, regardless of whether form is employed, and its width should correspond to the length of the key being used. The message can be written in as many rows as needed. When using complete columnar transposition, the plaintext is transcribed and any empty columns are filled with null to ensure that each column is the same length. Consider the following scenario:

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

Depending on the key, the cypher text is then derived from the columns. If we use the key "321654" in this case, the cypher text will be:

cvdng eiaii sdncn donox nsatt oivgh

When it comes to an incomplete columnar transposition cypher, however, the columns do not have to be filled in, therefore the null characters are left out. This results in columns of varying lengths, making deciphering the ciphertext more difficult without the key [20].

V. MODERN ALGORITHMS

5.1 Stream Ciphers

Stream cyphers use the key to generate pseudorandom bits, and the plaintext is encrypted by XORing the plaintext with the pseudorandom bits. In the past, stream cyphers were sometimes avoided because they were more easily broken than block cyphers. However, after years of development, the stream cypher has improved in security and can now be used in connections, Bluetooth, communications, mobile 4G, LS connections, and other applications.

In a stream cypher, each bit is encrypted separately. The synchronous stream cypher is one in which the key stream is dependent on the key, whereas the asynchronous stream cypher is one in which the ciphertext is dependent on the key stream. In Figure 3, a dotted line may be seen. If the stream cypher was present, it would be asynchronous; otherwise, it would be synchronous. The cypher feedback (CFB) [2] is an example of an asynchronous cypher.

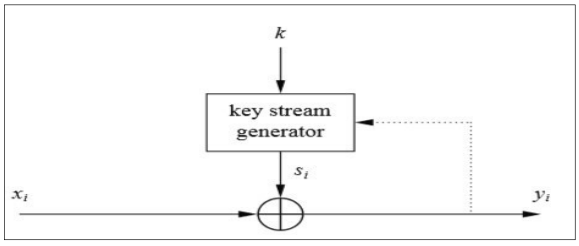

Figure 3: Asynchronous and synchronous types of stream ciphers

5.2 Block Cyphers

This type of cypher comprises of an encryption method and a decryption algorithm:

- The encryption method (E) and a plaintext block (P) are given a key (K), and C is the product, which consists of a ciphertext block. C = E can be used to express the encryption operation (K, P).
- The decryption algorithm (D) is the inverse of the previous process, which involves decrypting the ciphertext for the plaintext, P. P = D is a formula that can be written (K, C).

To make the block cypher more secure, a pseudorandom permutation (PRP) is used. An attacker will not be able to decrypt the block cypher and compute the output from any input if the key is kept secret. This is true as long as K's secrecy and randomness are guaranteed from the attacker's perspective. In a broad sense, this means that the attacker won't be able to spot any patterns in the data that's either input to or output from the block cypher.

The size of the block and the size of the key are commonly referred to in a block cypher. The value of both is crucial to the security. A 64-bit or 128-bit block is used in several block cyphers. Because it's critical that the blocks don't get too big, the memory footprint and ciphertext length are both minimal. A block cypher processes blocks rather than bits when it comes to ciphertext length. To put it another way, if we wish to encrypt a 16-bit message and replace the blocks with 128-bit blocks, we must first transform the message to 128-bit blocks; only then can the block cypher begin processing and output a 128-bit ciphertext.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

When it comes to memory footprint, we require at least 128-bit RAM to work with and process a 128-bit block. Most CPU registers are small enough to fit. Alternatively, dedicated hardware circuits can be utilised to do this. In most cases, 68 bits, 128 bits, and even 512-bit blocks are still short enough for efficient implementation. However, if the blocks grow in size (i.e., kilobytes), the cost and performance of the solution can suffer [19].

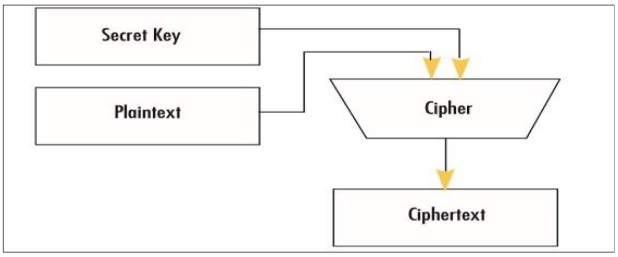

Figure 4: Block cipher diagram

5.3 Hash Functions

A memory footprint of at least 128 bits is required to interact with and process a 128-bit block. Most CPUs' registers are tiny enough to fit. Otherwise, dedicated hardware circuits can be employed. In most applications, 68 bits, 128 bits, and even 512- bit blocks are short enough for efficient implementation. However, if the blocks grow larger (in terms of kilobytes), the cost and performance of the system can suffer [19].

The one-way output of a hash function can be regarded a key aspect of it, as can the fact that it is collision resistant, meaning that finding another input that creates the identical result (known as collision) is difficult. There are two types of collision resistance that can be used:

- **Preimage Collision Resistance:** This type of hash function acts on an output Y, which is obtained by nontrivially identifying another input M with the same hash as Y.
- **Preimage Collision Resistance (Fig. 5):**
- **Second Preimage Collision Resistance:** this is the second type of hash function in which two messages (M1 and M2, which is chosen at random) are given and the match is nontrivial [21].

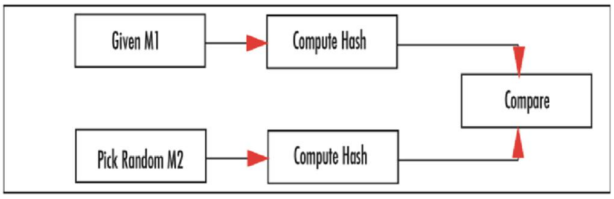

Figure 6: Second preimage collision resistance

5.4 Public-Key Cryptography

1. A cryptography revolution occurred with the invention of public key encryption. Even in the 1970s and 1980s, generic cryptography and encryption were clearly restricted to the military and intelligence communities. Cryptography only spread into other fields as a result of public key systems and methodologies.
2. Because the public key can be shared without fear of being compromised, public key encryption allows us to communicate without relying on secret channels. The following is a list of the public key's characteristics:
3. By using public key encryption, key distribution can be done over public channels, potentially simplifying the system's initial deployment and making maintenance easier when parties join or leave.
4. The need for a large number of secret keys is reduced when using public key encryption. Even if both parties want to communicate securely, each can store their own private key in a secure manner. Other people's public keys can be kept insecurely or retrieved as needed.
5. In open situations, public key cryptography is more appropriate, particularly when parties that have never met before want to communicate and cooperate securely. For example, a merchant may be able to reveal their public key online, and anyone who wishes to make a transaction can use the retailer's public key as needed when their

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

credit card information is encrypted [3].

VI. DIGITAL SIGNATURES

Digital signatures, unlike cryptography, did not exist prior to the creation of computers. With the introduction of computer communications, the need for digital signatures to be debated developed, particularly in business situations where numerous parties are involved and each must promise to keeping their declarations and/or proposals confidential. Unforgeable signatures were first mentioned hundreds of years ago, but they were handwritten signatures. Diffie and Hellman's paper "New Directions in Cryptography" [22] was the first to establish the concept of digital signatures.

As a result, in a circumstance where the sender and receiver do not have complete trust in one another, authentication alone will not be enough to bridge the gap. Something else is necessary, namely a digital signature that functions similarly to a handwritten signature [23].

6.1 Requirements for Digital Signatures:

- With the "digitalization" period that we are presently watching and living in, the interaction that produced the link between signature and encryption came into being. The following would be the prerequisites for an unforgeable signature schema:
- Each user should be able to create their own signature on any document of their choosing.
- Each user should be able to quickly determine whether or not a given string is the signature of a different user.
- No one should be able to generate signatures on documents that were not signed by the original owner [24].

6.2 Digital Signature Principles

It is critical both inside and outside the digital domain to be able to prove that a user or individual delivered a message. Handwritten signatures are used to accomplish this in today's society. When it comes to creating digital signatures, public-key cryptography is used. The basic principle is that the person signing a document or message uses a private key (called private-key), and the person receiving the message or document must use the matching public-key. Figure 7 illustrates the principle of the digital signature technique.

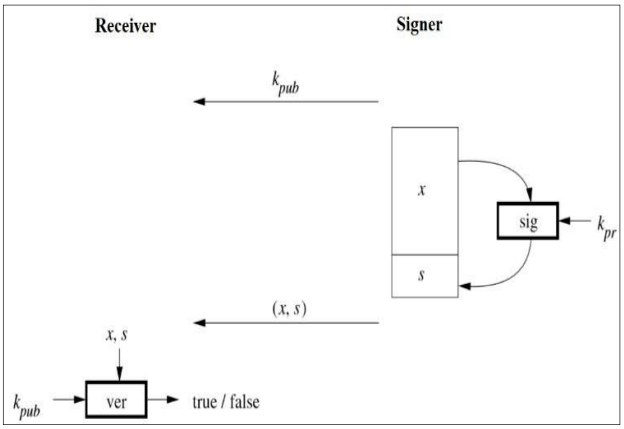

Figure 7: Digital signature principle (signing and verifying)

The signer initiates the procedure by signing the message x. The signing algorithm is a function belonging to the signer's private key (kpr), with the assumption that the signer will keep the private key secret. As a result, a relationship can be established between the message x and the signature algorithm; the message x is also provided as an input to the signature algorithm. The signature s is linked to the message x after it has been signed, and they are forwarded to the receiver in the pair of (x, s). It's also worth noting that, like putting a handwritten signature on a check or document, a digital signature is useless unless it's attached to a specific message.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

The digital signature itself has a huge integer value, such as a string of 2048 bits. A verification function is required to verify the signature, and both the message x and the signature s must be given as inputs to the function. The verification function will require a public key to link the signature to the sender who signed it, and the outcome will be either "true" or "false." If the message x was signed using the private key that is linked to the other key, the public verification key, the output would be true. Otherwise, the verification function's output would be false [2].

6.3 Digital Signature vs. Message Authentication

When communicating over an insecure channel, parties may want to include authentication in the messages they send to the receiver so that the recipient can identify if the message is genuine or if it has been altered. Message authentication generates an authentication tag for each message transmitted; recipients must validate it after receiving the message to ensure that no external attacker can generate authentication tags that are not being utilised by the communicating parties. Message authentication is similar to digital signature in certain ways, but the distinction is that in message authentication, just the second party is necessary to verify the message. There can be no third-party verification of the message's legitimacy or whether it was generated by the real sender. However, in the case of a digital signature, third parties can verify the signature's legitimacy. As a result, digital signatures have provided a message authentication solution [24].

VII. Conclusion

Authentication, integrity, confidentiality, and no-repudiation are only a few of the major security goals that cryptography helps to achieve. To fulfil these objectives, cryptographic algorithms are created. The objective of cryptography is to provide reliable, strong, and robust network and data security. We presented a summary of some of the research that has been done in the subject of cryptography, as well as an explanation of how the various algorithms used in cryptography for various security goals work in this paper. In order to protect personal, financial, medical, and ecommerce data while maintaining a reasonable level of privacy, cryptography will continue to be used in IT and business plans.

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, 2017, pp. 323-326.
[2]. Understanding Cryptography: A Textbook for Students and Practitioners, London: Springer, 2010. [2] B. Preneel, Understanding Cryptography: A Textbook for Students and Practitioners, London: Springer, 2010.
[3]. lntroduct:ion t:o Modern Cryptography, London: Taylor & Francis Group, LLC, 2008. [3] J. Katz and Y. Lindell, lntroduct:ion t:o Modern Cryptography, London: Taylor & Francis Group, LLC, 2008.
[4]. "Network Security: Focus on Security, Skills, and Stability," 37th ASEE/IEEE Frontiers in Education Conference, Milwaukee, 2007. S. J. Lincke and A. Hollan, "Network Security: Focus on Security, Skills, and Stability," 37th ASEE/IEEE Frontiers in Education Conference, Milwaukee, 2007.
[5]. "Communications cryptography," by O. O. Khalifa, M. R. Islam, S. Khan, and M. S. Shebani, in RF and Microwave Conference, 2004. Proceedings of RFM 2004, Selangor.
[6]. "Review and Analysis of Cryptography Techniques," by N. Jirwan, A. Singh, and S. Vijay
[7]. B. Schneier, "The Non-Security of Secrecy," Communications of the ACM, vol. 47, no. 10 (October 2004), pp. 120-120.
[8]. N. Varol, F. Aydoan, and A. Varol, "Cyber Attacks Targeting Android Cellphones," in Tirgu Mures, 2017: The 5th International Symposium on Digital Forensics and Security (ISDFS 2017).
[9]. K. Chachapara and S. Bhadlawala, "Secure cloud sharing using cryptography," 2013 Nirma University International Conference on Engineering (NUiCONE), Ahmedabad. H. Orman, "Recent Parables in Cryptography," IEEE Internet Computing, vol. 18, no. 1, 2014, pp. 82-86.
[10]. IEEE Security & Privacy, vol. 4, no. 2, pp. 64-67, 2006. [15] R. GENNARO, "IEEE Security &
[11]. Privacy," IEEE Security & Privacy, vol. 4, no. 2, pp. 64-67, 2006.
[12]. B. Preneel, "Cryptography and Information Security in the Post-Snowden Era," IEEE/ACM 1st International Workshop on TEchnical and Legal Aspects of Information Security,