IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Review on Cryptography

[1]Smruthi Ranjan Pradhan, [2] Samuel David Raj, [3]Harshitha MG, [4]Ms. Archana A,

[5]Ms. Gloriya Priyadarshini

[1]Student, [2]Student, [3]Student, [4]Assitant Professor, [5]Head of the Department
Bachelor of Computer Applications ,Department of Computer Science St. Philomena's College ,Mysore, India

Abstract: With the internet having reached a level that merges with our lives, growing explosively during the last several decades, data security has become a main concern for anyone connected to the web. Data security ensures that our data is only accessible by the intended receiver and prevents any modification or alteration of data. In order to achieve this level of security, various algorithms and methods have been developed. Cryptography can be defined as techniques that cipher data, depending on specific algorithms that make the data unreadable to the human eye unless decrypted by algorithms that are predefined by the sender.

I. INTRODUCTION

Cryptography is a technique to achieve confidentiality of messages. The term has a specific meaning in Greek: "secret writing". Nowadays, however, the privacy of individuals and organizations is provided through cryptography at a high level, making sure that information sent is secure in a way that the authorized receiver can access this information [1]. With historical roots, cryptography can be considered an old technique that is still being developed. 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 [2].

Billions of people around the globe use cryptography on a daily basis to protect data and information, although most do not know that they are using it. In addition to being extremely useful, it is also considered highly brittle, as cryptographic systems can become compromised due to a single programming or specification error [3].

II. CRYPTOGRAPHY CONCEPT

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix graphy means "writing".

In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

2.1 Techniques used For Cryptography:

In today's age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

Features of Cryptography are as follows:

Confidentiality:
Information can only be accessed by the person for whom it is intended and no other person except him can access it.

Integrity:
Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

Non-repudiation:
The creator/sender of information cannot deny his or her intention to send information at later stage.

Authentication:
The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

2.2 Types of Cryptography:

In general there are three types of cryptography:

- Symmetric Key Cryptography:

It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System (DES).

- Hash Functions:

There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

- Asymmetric Key Cryptography:

Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

III. CRYPTOGRAPHIC ALGORITHMS

The cryptographic protection of a system against attacks and malicious penetration depends on two dimensions:

- The strength of the keys and the effectiveness of mechanisms and protocols associated with the keys
- The protection of the keys through key management (secure key generation, storage, distribution, use and destruction).

Strong algorithms combined with poor key management are as likely to fail as poor algorithms embedded in a strong key management context. According to NIST(National Institute of Standards and Technology), cryptographic algorithms that are either FIPS(Federal Information Processing Standards)-approved or NIST-recommended must be used if cryptographic services are needed. These algorithms have undergone extensive security analysis and are continually tested to ensure that they provide adequate security. Cryptographic algorithms will usually use cryptographic keys and when these algorithms need to be strengthened, it can often be done by using larger keys.

3.1 Classes of Cryptographic Algorithms

There are three general classes of NIST-approved cryptographic algorithms, which are defined by the number or types of cryptographic keys that are used with each.

3.1.1 Hash functions

A cryptographic hash function does not use keys for its basic operation. This function creates a small digest or “hash value” from often large amounts of data through a one-way process. Hash functions are generally used to create the building blocks that are used in key management and provide security services such as:

- Providing source and integrity authentication services by generating message authentication codes (MACs)
- Compressing messages for generating and verifying digital signatures
- Deriving keys in key-establishment algorithms
- Generating deterministic random numbers

3.1.2 Symmetric-key algorithms

Also referred to as a secret-key algorithm, a symmetric-key algorithm transforms data to make it extremely difficult to view without possessing a secret key.

The key is considered symmetric because it is used for both encrypting and decrypting. These keys are usually known by one or more authorized entities. Symmetric key algorithms are used for:

- Providing data confidentiality by using the same key for encrypting and decrypting data.
- Providing Message Authentication Codes (MACs) for source and integrity authentication services. The key is used to create the MAC and then to validate it.
- Establishing keys during key-establishment processes
- Generating deterministic random numbers

3.1.3 Asymmetric-key algorithms

Also referred to as public-key algorithms, asymmetric-key algorithms use paired keys (a public and a private key) in performing their function. The public key is known to all, but the private key is controlled solely by the owner of that key pair. The private key cannot be mathematically calculated through the use of the public key even though they are cryptographically related. Asymmetric algorithms are used for:

- Computing digital signatures
- Establishing cryptographic keying material
- Identity Management

3.2 Security Services Provided by Cryptographic Algorithms

Specific security services can be achieved by using different cryptographic algorithms. Often, a single algorithm can be used for multiple services.

3.2.1 Hash Functions

A hash function is often a component of many cryptographic algorithms and schemes, including digital signature algorithms, Keyed-Hash Message Authentication Codes (HMAC), key-derivation functions/methods and random number generators. A hash function operates by taking an arbitrary, but bounded length input and generating an output of fixed length. This output is often referred to as hash, hash value, message digest or digital fingerprint. FIPS180 (Secure Hash Standard) and FIPS202 (Secure Hash Algorithm-3) define the approved hash functions.

3.2.2 Symmetric-Key Algorithms for Encryption and Decryption

Encryption provides confidentiality of data by transforming the “plaintext” into “ciphertext.” Decryption transforms ciphertext back to plaintext. AES and 3DES are the approved symmetric-key algorithms used for encryption/decryption services. 3DES is likely to be retired in the near future.

3.2.3 Advanced Encryption Standard (AES)

The AES is based on the Rijndael algorithm, which was invented by Cryptomathic’s previous chief cryptographer Vincent Rijmen together with his fellow researcher Joan Daemen. AES encrypts and decrypts data using 128/192/256-bit keys into 128-bit blocks.

3.2.4 3DES / Triple DEA (TDEA)

3DES is a symmetric-key block cipher which applies the DES cipher algorithm three times to each data block. The official name as used by NIST is the Triple Data Encryption Algorithm (TDEA).TDEA encrypts and decrypts data using three 56-bit keys into 64-bit blocks. TDEA has two additional variations:

Two-key TDEA (2TDEA) using 3 keys, however key 1 and key 3 are identical. This leads to 112 effective bits.Three-key TDEA uses 3 different keys, leading to 168 bits. 2TDEA is widely used in the payment card industry as it provided a good trade-off of security and compute time. However, evolving technology made it inappropriate to withstand attacks. As of December 21, 2015, 2TDEA can only be used for decryption purposes. A comparative study (Alanazi et al., 2010), pointed out that even 3DES (also referred to as 3TDEA) is vulnerable to differential cryptanalysis. The Advanced Encryption Standard (AES) proved itself to be much safer, being strong against differential cryptanalysis, but also against truncated differential or linear cryptanalysis as well as against interpolation and square attacks.

Modes of Operation for the application of AES and TDEA

Cryptographic modes of operation are algorithms which cryptographically transform data that features symmetric key block cipher algorithms, in this case AES and TDEA. The modes of operation solve the problems that occur with block-cipher encryption: when multiple blocks are encrypted separately within a message that could allow an adversary to substitute individual blocks, often without detection. To alleviate this, NIST prescribes the combination of the applied algorithm with

- variable initialization vectors (special data blocks used in an initial step of the encryption and in the subsequent and corresponding decryption of the message) and/or
- feedback of the information that has been derived from the cryptographic operation.

3.2.5 Message Authentication Codes (MACs)

MACs can be used in providing authentication for the origin/source and integrity of messages. This cryptographic mechanism resolves the problem of adversaries altering messages by creating a MAC key that is shared by both the message originator and the recipient.

3.2.6 Digital Signature Algorithms

Digital signatures are used with hash functions to provide source authentication, integrity authentication, and support for non-repudiation. The Digital Signature Algorithm (DSA), RSA algorithm and ECDSA algorithm are approved by FIPS 186 for use in generating digital signatures.

3.2.7 Key Establishment Schemes

Key transport and key agreement are two types of automated key establishment schemes that are used to create keys that will be used between communicating entities. The sending entity encrypts the keying material, which is then decrypted by the receiving entity.

3.2.8 Discrete Logarithm based Key-Agreement Schemes

Discrete logarithm based public-key algorithms rely on schemes that use finite field math or elliptic curve math. Ephemeral, static or both keys may be used in a single key-agreement transaction.

3.2.9 Key Establishment Using Integer-Factorization Schemes

Integer factorization based public-key algorithms are used for key establishment schemes where one party always has and uses a static key pair, while the other party may or may not use a key pair.

3.2.10 Security Properties of the Key-Establishment Schemes

It is not always practical for both parties to use both static and ephemeral keys with certain applications, even though using both types of keys in key-establishment schemes provides more security than schemes that use fewer keys.

3.2.11 Key Encryption and Key Wrapping

Key encryption further enhances the confidentiality and protection of a key by encrypting the said key. The process of key unwrapping then decrypts the ciphertext key and provides integrity verification.

3.2.12 Key Confirmation

Key confirmation provides assurance between two parties in a key-establishment process that common keying materials have been established.

3.2.13 Key Establishment Protocols

Protocols for key establishment specify the processing that is needed to establish a key along with its message flow and format.

3.2.14 RNGs (Random Number Generators)

RNGs are needed to generate keying material and are classified into two categories: deterministic and non-deterministic.

IV. CIPHER SYMBOLS

cipher, any method of transforming a message to conceal its meaning. The term is also used synonymously with ciphertext or cryptogram in reference to the encrypted form of the message. A brief treatment of ciphers follows. For full treatment, see cryptology.

All ciphers involve either transposition or substitution, or a combination of these two mathematical operations—i.e., product ciphers. In transposition cipher systems, elements of the plaintext (e.g., a letter, word, or string of symbols) are rearranged without any change in the identity of the elements. In substitution systems, such elements are replaced by other objects or groups of objects without a change in their sequence. In systems involving product ciphers, transposition and substitution are cascaded; for example, in a system of this type called a fractionation system, a substitution is first made from symbols in the plaintext to multiple symbols in the ciphertext, which is then super encrypted by a transposition. All operations or steps involved in the transformation of a message are carried out in accordance to a rule defined by a secret key known only to the sender of the message and the intended receiver.

Cipher devices or machines have commonly been used to encipher and decipher messages. The first cipher device appears to have been employed by the ancient Greeks around 400 BCE for secret communications between military commanders. This device, called the scytale, consisted of a tapered baton around which was spirally wrapped a piece of parchment inscribed with the message. When unwrapped the parchment bore an incomprehensible set of letters, but when wrapped around another baton of identical proportions, the original text reappeared. Other simple devices known as cipher disks were used by European governments for diplomatic communications by the late 1400s. These devices consisted of two rotating concentric circles, both bearing a sequence of 26 letters. One disk was used to select plaintext letters, while the other was used for the corresponding cipher component.

In 1891 Étienne Bazeries, a French cryptologist, invented a more sophisticated cipher device based on principles formulated by Thomas Jefferson of the United States nearly a century earlier. Bazeries's so-called cylindrical cryptograph was made up of 20 numbered rotatable disks, each with a different alphabet engraved on its periphery. The disks were arranged in an agreed-upon order on a central shaft and rotated so that the first 20 letters of the message plaintext appeared in a row; the ciphertext was then formed by arbitrarily taking off any other row. The remaining letters of the message were treated in the same way, 20 letters at a time.

Advances in radio communications and electromechanical technology in the 1920s brought about a revolution in cryptodevices—the development of the rotor cipher machine. One common type of rotor system implemented product ciphers with simple monoalphabetic substitution ciphers as factors. The rotors in this machine consisted of disks with electrical contacts on each side that were hardwired to realize an arbitrary set of one-to-one connections (monoalphabetic substitution) between the contacts on opposite sides of the rotor.

The rotor cipher machine was used extensively by both the Allied and the Axis powers during World War II, with the most notable such device being the German Enigma machine. The application of electronic components in subsequent years resulted in significant increases in operation speed though no major changes in basic design. Since the early 1970s, cryptologists have adapted major developments in microcircuitry and computer technology to create new, highly sophisticated forms of cryptodevices and cryptosystems, as exemplified by the Fibonacci generator and the implementation of the Data Encryption Standard (DES) through the use of microprocessors.

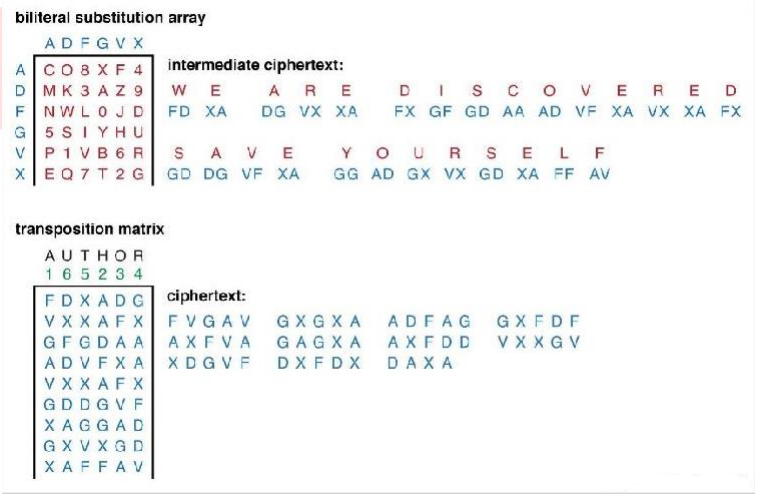

Fig 1.1

V. CONCLUSION

Cryptography plays a vital and critical role in achieving the primary aims of security goals, such as authentication, integrity, confidentiality, and no-repudiation. Cryptographic algorithms are developed in order to achieve these goals. Cryptography has the important purpose of providing reliable, strong, and robust network and data security. In this paper, we demonstrated a review of some of the research that has been conducted in the field of cryptography as well as of how the various algorithms used in cryptography for different security purposes work. Cryptography will continue to emerge with IT and business plans in regard to protecting personal, financial, medical, and ecommerce data and providing a respectable level of privacy.

REFERENCES

[1] https://www.geeksforgeeks.org/cryptography-and-its-types/ .
[2] https://www.cryptomathic.com/news-events/blog/summary-of-cryptographic-algorithms-according-to-nist .
[3] Cryptography Report by Abdalbasit mohammed
[4] 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.
[5] B. Preneel, Understanding Cryptography: A Textbook for Students and Practitioners, London: Springer, 2010.
[6] J. Katz and Y. Lindell, lntroduct:ion to Modern Cryptography, London: Taylor & Francis Group, LLC, 2008.
[7] S. J. Lincke and A. Hollan, "Network Security: Focus on Security, Skills, and Stability," in 37th ASEE/IEEE Frontiers in Education Conference, Milwaukee, 2007.
[8] https://www.britannica.com/topic/cryptology/Vigenere-ciphers
[9] 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.