# The Cryptosystem: A Quick Overview

**Ratna Sarkar, Stuti Banerjee, Pallabi Sadhukhan,**
**Mandira Majhi, Anwesha Das, Rupak Bhattacharyya***
Department of Mathematics
Bijoy Krishna Girls' College, Howrah
5/3, Mahatma Gandhi Rd, Howrah, West Bengal 711101, India
*sarkarratna651@gmail.com, stutibanerjee6293@gmail.com, sadhukhanpallabi87@gmail.com, mandiramajhi7@gmail.com, dasanwesha6291@gmail.com,* mathsrup@gmail.com*

***Abstract:*** One of the most sophisticated technologies currently and for the near future is the cryptosystem. The complete system, encompassing the fields of cryptography and cryptanalysis, a wide range of mathematical methods and algorithms, as well as suggestions for future developments, will be covered in this article.

***Keywords: Encryption, decryption, cipher-text, plain-text, algorithm.***

## I INTRODUCTION

A cryptosystem converts ordinary text into cypher text. This conversion is based on the decryption as well as the encryption process, which uses a variety of approaches to make it easier. This system has a history of 4000 years. In literature, cryptography was first found around 1900 B.C. Continuous development of cryptography has provided us secure communication, money transactions, emails, and any online service. It keeps the data of the secure and safe and sometime hide the actual address of them in presence of third party and in future also, not only cryptography in fact the whole cryptosystem will be remarkable for its huge contribution in the history of technology.

A *Cryptosystem* is an implementation of cryptographic techniques. It is basically a pair of algorithms; one for encryption data and another for decryption. Before discussion, we need to know what is cipher. Actually, *Cipher* is an algorithm, applied target cipher text from plain text via encryption process.

*Cryptology* is nothing but an art of writing and sewing codes. Cryptology can be classified into two parts; Cryptography and Cryptanalysis.

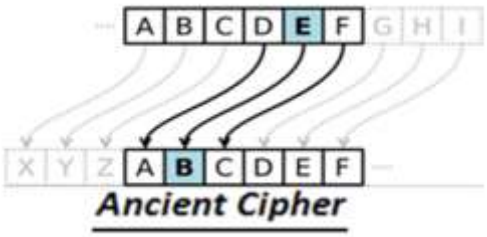
Figure 1 depicts different parts of cryptology.

## II CRYPTOGRAPHY

In cryptology, *Cryptography* is a specialized area of cyber security. It is an art of creating codes. We will now discuss a brief history of cryptography.

***Ancient Cipher:***

- Have a history of at least 4000 years.
- In 1900 B.C. an Egyptian scribe used some unusual hieroglyphs.
- 2000 years ago, Julius Caesar used a variant which was a shift by 3 ciphers i.e. ‘c’ was replaced by ‘f’.




- Roger Brawn described several methods in 1200 s.
- Geoffrey Chaucer included several ciphers.
- Leon Alberti devised a cipher wheel, and described the principles of frequency analysis in the 1460s.
- During 16th century, Vignere designed the first cipher using encryption key with a mathematical expression for reminder in division.

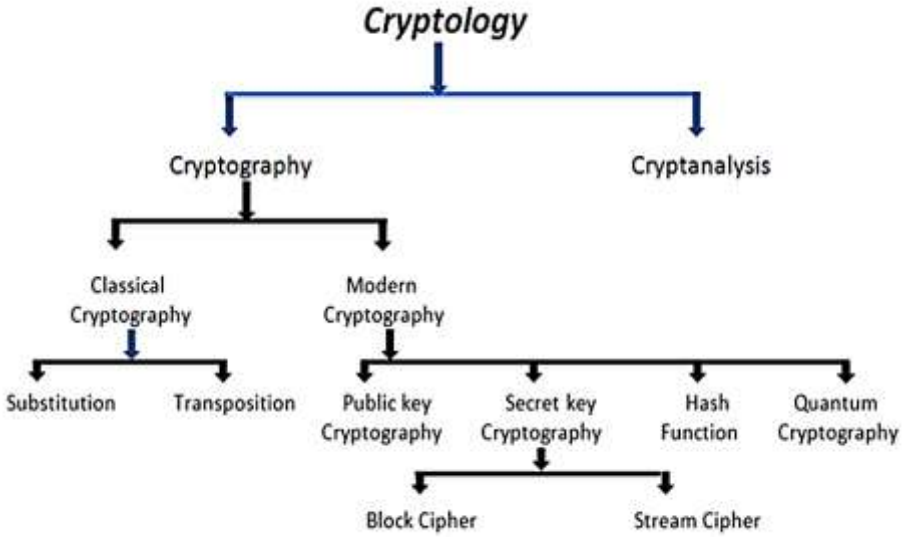
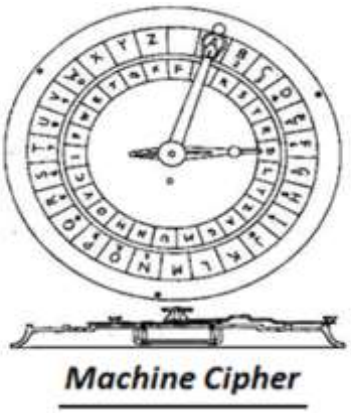



**Figure 1: Cryptology**

***Machine Cipher:***

- In 1790 s, Jefferson Cylinder was developed consists of 36 disks with a random alphabet of which order of disks was key.




- In 1817, the Wheatstone disc was invented by wads worth and developed by Wheatstone in 1860's to generate polyalphabetic Cipher.

- Enigma Rotor machine, a very important class of Cipher machine, heavily used during end World War, providing substitution using a continuously changing alphabet theory.

# III CLASSIFICATION OF CRYPTOGRAPHY

Cryptography can be classified into two parts; Classical Cryptography and Modern Cryptography.

## III A CLASSICAL CRYPTOGRAPHY

Classical Cryptography is mathematics-based cryptography. Its security lies on the tremendous complexity of the mathematical problems, which depend on the computational difficulties of factorization of huge integers.

*Classical cryptographic* techniques consist of two main components:

- Substitution
- Transposition

In *Substitution Cipher*, the letters have been replaced by alternative letters and in *Transposition Cipher*, the letters are arranged in different order. Here the cipher may have two types; either *Monoalphabetic* i.e. only one Substitution or Transposition is used or *Polyalphabetic* i.e. several Substitution or Transposition are used. Together they from *Product Cipher*.

***Advantages of Classical Cryptography:***

- It is indestructible when using the one-time pad.
- It is simple to accomplish by hand; no computer is necessary.
- It safeguards the plain text against casual snooping.

***Disadvantages of Classical Cryptography:***

- When using the one-time pad, it is inconvenient and necessitates a personal meeting to swap the pads.
- If the OTP is not used, anyone who is even somewhat interested in what you wrote and is familiar with cryptography will be able to crack the encryption.

## III B MODERN CRYPTOGRAPHY

This sort of cryptography is based on numerous mathematical concepts such as number theory, probability theory, and so on. It is, more precisely, the cornerstone of communication along with computer security.

There are two key modules in contemporary cryptography: Encryption and decryption.

Any information may be safeguarded by coding using encryption. Only one individual has access to the information. It can cover any data with secret code so that the real meaning of the data is hidden from any opportunistic person or hacker.

*Decryption* is a process that returns encrypted information to its original from. This is reverse process of encryption. It decodes the encrypted message by a password so that only receiver can describe the massage.

The message that we are able to read, understand before encryption or after decrypting is called *Plain Text.*

The message or data that couldn't be understood by any of us after encryption is called *Cipher Text.*

***How does the Encryption and Decryption process take place?***

In its simplest form, the normal, or plain text, is encrypted through the encryption process using a unique mathematical formula known as the "encryption algorithm," converting the plain text into an unintelligible text, or cypher text, which would be useless to a third party with malicious intent due to its jumbled nature. Now the cipher text is decrypted by the receiver who has the key already to decrypt the message. Like encryption, the decryption uses mathematical formulae, known as C decryption algorithm. In this case, only the receiver knows the protocols to decode that information.

***Encryption vs Decryption:***

Encryption is the process which encodes and disguises the message's content, performed by the message sender. Where decryption is the process which decodes an obscured message, carried out by the message receiver.

The type of cypher employed to encrypt the data and the potency of the decryption keys needed to convert the encrypted data back to plain text directly affect the security offered by encryption.

For classifying cryptographic algorithms, the *Modern Cryptography* can be categorized on the bases of number of keys that are employed for encryption and decryption.

**SECRET KEY CRYPTOGRAPHY**

A single key is used in this technique for encryption as well as decryption. The sender uses the key to encrypt the plain text to convert it to cipher text and send it to receiver while the receiver uses the identical key to get back the plain text. This cryptography is sometimes referred to as symmetric encryption since it only requires a single key for both encryption and decryption. Secret key Cryptography schemes are generally categorized in *Stream Cipher* and *Block Cipher*.

- ***Stream Cipher:*** It operates on a single bit at a time and uses some kind of feedback mechanism to keep the key changing. Among the several characteristics of Stream Cyphers, two stand out:
  1. Self-synchronizing
  2. synchronised.
- ***Block Cipher:*** Block Ciphers are the scheme that encrypts one fixed- Size block of data at a time. It encrypts a group of plain text of size n and creates the Cipher text of same size.

The main algorithms are mentioned below:

- **DES (Data Encryption Standard):** One of the most well-known and well-studied **SKC** schemes, designedly **IBM** in the 1970s and adopted by **NIST** (*National Institute for Standards and Technology*) in 1997. It uses 56-bit encryption key and operates on 64 bits of data. It initially permutation of that and then divide in 32 bit each. But now it is an out-dated method as I was rejected because of the **NSA** (*National Security Agency*). DES has been replaced with the more secure key AES.
- **AES (Advanced Encryption Standard):** This became the official success or to DES in *December 2001*. AES uses an SKC scheme called Rijndael, a block cipher, designed by *Belgian Cryptographers*. It uses *10, 12*, or *14* rounds with each version using a different key size that is *128, 192*, or *156* bits. State is arranged in *(4*4)* matrix and all rounds are

identical except the last one. It is chosen to secure classified information and is used to encrypt sensitive data in software and hardware all around the world.

- **Triple- DES (3DES or TDES):** A variant of DES which employs up to three 56- bit keys and makes three encryption or decryption passes over the block. It was a replacement to DES in early 2000s.
- **Blowfish:** Blowfish is a 64-bit symmetric block cypher designed for 32-bit CPUs with huge data caches. Key lengths can range from 32 to 448 bits. It is noticeably quicker than DES.
- Many more algorithms like The Need ham-Schroder algorithms, The International Data Encryption Algorithm (IDEA), Twofish, ARIA etc., are there to be mentioned.

***Disadvantages of Symmetric Key Cryptography:***

- **Key Storage and Recovery** *Symmetric Cryptography* requires sharing of secret keys between both parties and to maintain the secrecy, a trust channel i.e. designated controller is needed which carries third party risk.
- **Key Distribution** Due to many more lines of communication between both parties, the need to implement more controllers become very unrealistic and hence key distribution is *vulnerability*.

**PUBLIC KEY CRYPTOGRAPHY (PKC)**

It has been said to be the most significant new development in the last crypto system in which both parties can communicate over a non-secure communication on channel without sharing a key. These two keys are required for encryption and decryption respectively and due to presence of a pair of keys, it is also referred as a *Symmetric Cryptography*. Like Secret Key Cryptography, Public Key Cryptography also provides us some useful algorithms:

- **The RSA Algorithm:** Ron Rivest, Adi Shamir, and Leonard Adleman of Massachusetts Institute of Technology published the first public description of this technique in 1977. This is used in hundreds of software products and is suitable for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size key and a variable size encryption block. The public key includes n and a derivative of one of the factors of n, so that an attacker will never beadle to determine and so it is very secure.
- **The Elliptic Wave Theory Algorithm:** A PKC algorithm, based levels of security with small keys comparable to RSA and other PKC methods. This uses algebraic functions to generate security between key pairs. It was designed for limited power and or memory using devices.
- **The Diffie- Hellman Algorithm:** Diffie and Hellman developed their own method after the RSA algorithm was revealed. It is also known as exponential key exchange, a form of digital encryption that generates decryption keys by raising integers to particular powers.

***Public Key Infrastructure (PKI)***

As the public key has become very important in the encryption and decryption process of cipher text between the sender and receiver, extensive researches are done to make it much more secure and robust. More specifically, this is a very sophisticated form of Asymmetric Cryptography. The Certificate Authority (CA), the digital certificate, the LDAP or X.500 directories, the registration authority are the specific components of the Public Key Infrastructure.

***LDAP protocol***

**LDAP**, an acronym, stands for lightweight Directory Access Protocol. It is a database protocol, used for the updating and searching of the directories, run over the TCP/IP network protocol. LDAP protocol is used in PKI to contain information and data, relates to the digital certificates. It also stores public and private key storage locations and levels too.

***Drawbacks of public key cryptography:***

Beside advantages, public key cryptography has a serious disadvantage and that is, it is two or three times slower than Secret Key Cryptography.

***Comparison between Secret and Public Key Cryptography:***

In Secret Key Cryptography, secrecy of the key must be completely assured, but in PKI, only half of the secrecy has been maintained.

Secondly, Secret Key Cryptography utilizes the same key for both encryptions and decryption but Public Key Cryptography uses different keys for each.

**HASH FUNCTION**

Hash Function, also called message digest and a one-way mathematical function provides another type of encryption. It converts a string of characters into a fixed length value or key, a hash value derived based on the plain text that makes recovering the contents or length of the plain text difficult.

Hash algorithms provide a digital finger print of a file's contents. Even the slightest change can be deleted by it, resulting a huge change to the resulting hash. It is also used to ensure whether the data is changed by virus or any 3rd party and employed to encrypt passwords. Hash functions also provide us the way to secure encryption with help of Algorithms.

***Message Digest (MD) Algorithms:*** A Hash Algorithm, a series of byte-oriented algorithms, produces a 128-bit hash value from an arbitrary length message.

After *MD2* and *MD4*, *MD5* was developed by Rivest, after having some report in previous. It is designed for fast processing in software but slower than *MD4* because of more manipulation. Though several weaknesses are there, it is implemented in a hefty quantity of products.

***Secure Hash Algorithm (SHA)****:* Algorithm for *NIST's Secure Hash Standard (SHA).*

- ***SHA- 1:*** It produces a **160-bit** Hash value.
- ***SHA- 2:*** It comprises five algorithms in the SHA: *SHA-1* plus *SHA-224*, *SHA-256, SHA-384*, and *SHA-512* which can produce Hash values 224, 256, 384 or 512 bits in length. It recommends *SHA-1*, *SHA-224*, and *SHA-256* for messages less than $\mathbf{2^{64}}$-bits in length and employs a 512-bit block size; *SHA-384* and *SHA-512* for messages less than $2^{128}$ bits in length and employs 1024-bit block size.

Different types of cryptographic schemes have their specific functions. Each cryptographic scheme is designed for a single cryptographic application. Follow the following examples:

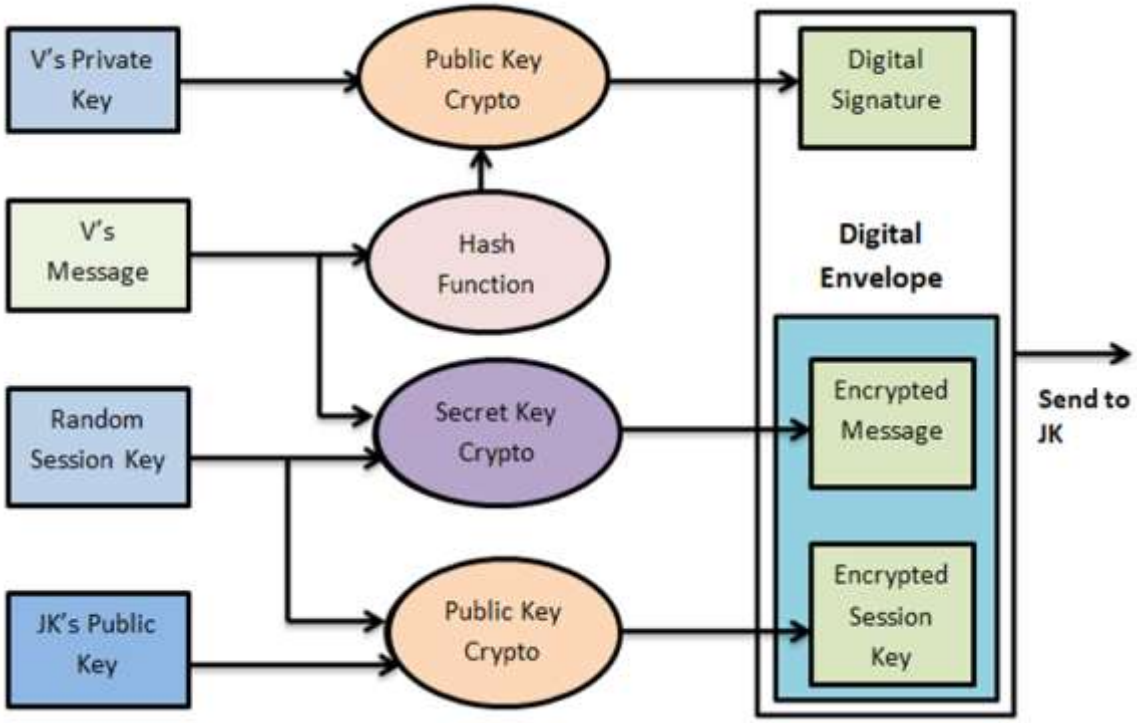
- Hash function is a type of cryptographic scheme that ensures data integrity. The Hash Function is largely reliable which never gives the same value to two different data.
- The messages are protecting by the Secret Key by encrypting them which maintains the privacy of messages. The specific session key which sender user to encrypt data, receiver

has to decrypt data with that same key. Thus Secret Key plays a main role in symmetric key encryption.

- In asymmetric key encryption, Public key are used as key exchanger. Asymmetric scheme is acceptable when receiver will decrypt the message with its own private key after encrypting it with the receiver's Public key even after the sender has locked the sessions with its different private keys.

Although a public key is used to encrypt messages directly, a private key can calculate values thousands of times faster than a public key.

The works of these three schemes can be observed together from the diagram below.




***Importance of Encryption:***

- **Integrity:** It proves that, since the message was sent, the content is unchanged.
- **Authentication:** It confirms the message's origin.
- **Confidentiality:** It encodes the message's content.
- **Nonrepudiation:** It prevents senders from denying they sent the encrypted message.

***Types of Encryption:***

Here we will discuss over several types of Encryption.

- ***Cloud Storage Encryption:*** **Cloud encryption** is almost identical to in-house encryption. This service is offered by cloud storage providers where data or text is transformed using encryption algorithms and then placed in cloud storage.
- ***HTTPS:*** This type of encryption enables website encryption by running **HTTP** over **TLS** protocol. A public key certificate has to be deployed in order for the webserver to be able to encrypt all information.
- ***End-to-end Encryption (E2EE):*** The end-to -end encryption, the most secure way to communicate, privately and securely online, prevents third party from reading private

communications. Encrypted communication circuit, provided by **TLS** *(Transport Layer Security*), is not always enough. In that case, the actual content being transmitted is encryption by client software before passing to web client and decrypted by only the recipient. *Facebook, WhatsApp* use this encryption process.

- ***Network –level Encryption:*** Network Encryption is implemented through *Internet Protocol Security* (**IPsec**). At the network transfer layer, which is above the data link level but under the app-location level, crypto services are applied.

Beside these four, many other encryption types such as

***Bring Your Encryption (BYOE):*** Customers can utilise their own encryption software using it.
***Column-level Encryption:*** Every cell in a certain column has the same password.
***Deniable Encryption:*** There are several techniques to decode a text that has been encrypted like

***Encryption as a Service (EaaS):*** Subscription model.
***Link-level Encryption:*** Encrypts data when it leaves host.
***FDE:*** Encryption at the hardware level.
***Field-level Encryption:*** The ability to encrypt data in specific fields on a webpage.

***Trust Models***

There a number of trust models are employed by various Cryptographic Schemes like

- ***PGP Web of Trust -*** It is a widely used private e-mail scheme based on *Public Key* algorithms. The *PGP* users hold their own of trusted public keys makes their own determination about the trust-worthiness of a key using what is called a "Web of Trust".
- ***Kerberos -*** Kerberos, a Secret Key distribution scheme, is a commonly used authentication scheme on the internet, using a Third Party.
- ***Certificates and certificate authorities -*** Public Key certificates are part of a public key infrastructure that deals with digitally sighed documents and a certificate authority is an body that acts to validate identities and bind them to cryptographic key pairs with digital certificates.

**How is encryption broken?**

First of all, the length of the key defines the number of potential keys, which makes this kind of attack feasible because key size and encryption strength are closely correlated. As a result, the resources needed to run the computation also rise along with the key size.

Side-channel attacks, which target the implementation of the cypher rather than the cypher itself, are another way to defeat encryption.

Thus, Public key cryptography, Secret Key Cryptography and Hash Function together perform a single type of Modern Cryptography. Now let's have a look on the 2nd most important part which is a little bit different and that is Quantum Cryptography.

## IIIC QUANTUM CRYPTOGRAPHY

Before developing the idea on Quantum Cryptography, we need to know that, Quantum computers process quantum-bits, a two-state quantum mechanical system, which can hold a value of one and zero simultaneously, allowing the calculation in a more complex process in a very short period of time. Quantum System with at least two states can serve as a qubit, for

example, the spin of an atom or the polarization of a light particle etc. Small scale quantum-computers already exist and inevitably after the development of full-scale quantum computer, the well-known Discrete Logarithmic Problem (*DLP*) or the integer factorization problem will no longer difficult *under Quantum-computer*. *In 1994* mathematician Shor proposed the quantum algorithm by which the integer factorization problem and DLP can be solved easily the polynomial time. Thus, *Public Key Cryptosystem* will no longer be safe.


**Quantum Cryptography**

Now, quantum physics and classical cryptography are combined to form quantum cryptography. The purpose is to provide a way for two uses in different location to securely establish a secret key which is not accessible in the Polynomial-time by an outsider who uses full—scale Quantum Computer.

Now we discuss the basic properties of quantum cryptography.

***Heisenberg's Uncertainty Principle:*** German physicist Heisenberg first proposed it in 1927. The basic contention is that it is impossible to establish a particle's position in the micro universe, and that some pairs of quantum physical qualities are interconnected in such a way that simultaneous knowledge of the values of both attributes by an observer is prohibited. The decision of which direction to measure in particularly impacts all future measurements even if it just refers to the polarisation of a photon.

***Quantum No Cloning Principle:*** Cloning is to produce a quantum state completely identical to an existing system in another system. It is proved that none of the existing machines are skilled of replicating Quantum States.

***Quantum No-deleting Principle:*** According to the theory, one cannot delete an unknown quantum state and deleting one of a pair of unknown quantum states, will make changes to the remaining one and leave traces.

***Quantum Entanglement:*** In Quantum Physics, the entanglement of particles describes a relationship between their fundamental properties that occurs when two particles become inextricably linked and whatever happens to one immediately affects the other, regardless hoe far apart they are. They can share information in such a way that it cannot be accessed in any experiment performed only on either of the particles alone.

***Quantum Teleportation:*** Even in the lack of quantum communication routes between two parties, quantum teleportation enables remote parties to exchange unknown qubits. Teleportation on servers as an ingredient in several Computation and communication tastes.

## QUANTUM KEY DISTRIBUTION

A shared random secret key that will both encrypt and decode the message quantum is needed for this kind of secure communication between two participants. A quantum mechanics-based cryptography technique is implemented using Key Distribution.

***Key Distribution***

1. *R* sends a sequence of photons to *J*.
   Each photon in a state with polarization corresponding to 1 or 0, but with randomly chosen property of the photons or basis.
2. *J* measures the state of the photons received, with each state measured with respect to randomly chosen basis.
3. *R* and *J* communicate via an open channel. For each photon they reveal which basis was used for encoding and decoding respectively. All photons that have been encoded and decoded using the same basis are retained, whereas any that have different bases are thrown away.

***Eavesdropping***

- *E* has to randomly select basis for the measurement.
- The basis will be wrong in *50%* of the time.
- Then *E* will measure *0* or *1* with whatever basis is chosen by *E*.

**Problem Faced by E**

- In this process *E* has to resend all the photons to *J*.
- It will present an error as *E* does not know the correct basis used by *R*.
- *J* will detect an increased error rate.
- Still *E* is able to listen in on a few photons and has some understanding of the key.

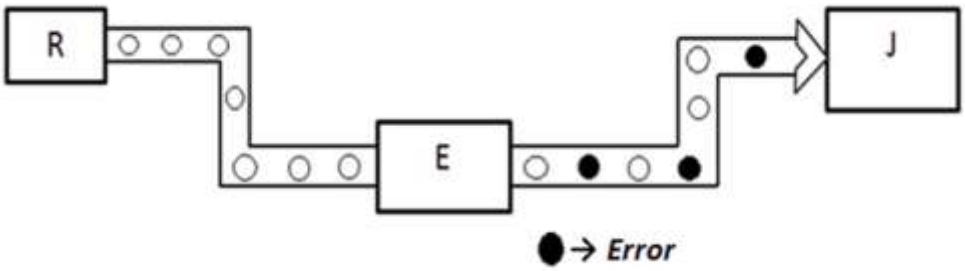
| R's Basis | R's Bit | R's Photon | E's Basis | Correct | E's Photon | E's Bit | Correct |
|---|---|---|---|---|---|---|---|
| {↑,→} | 1 | ↑ | {↑,→} | Yes | ↑ | 1 | Yes |
| | | | | | → | 0 | No |
| | | | {↗,↖} | No | ↗ | 1 | Yes |
| | | | | | ↖ | 0 | No |
| | 0 | → | {↑,→} | Yes | → | 0 | Yes |
| | | | | | ↑ | 1 | No |
| | | | {↗,↖} | No | ↗ | 1 | No |
| | | | | | ↖ | 0 | Yes |
| {↗,↖} | 1 | ↗ | {↑,→} | No | ↑ | 1 | Yes |
| | | | | | → | 0 | No |
| | | | {↗,↖} | Yes | ↗ | 1 | Yes |
| | | | | | ↖ | 0 | No |
| | 0 | ↖ | {↑,→} | No | ↑ | 1 | No |
| | | | | | → | 0 | Yes |
| | | | {↗,↖} | Yes | ↖ | 0 | Yes |
| | | | | | ↗ | 1 | No |

***Detecting Eavesdropping:***

Randomly choosing a number of bits from the key and computer error.

(Error rate < $E_{max}$ =) Assume no eavesdropping.

(Error rate > $E_{max}$ =) Assume no Eavesdropping and discard the whole key and start over.




**Benefits of quantum cryptography**

1. Maintenance requires fewer resources.
2. It is almost impossible to hack.
3. In QKD (Quantum Key Distribution), it is utilised to identify eavesdropping.

**Disadvantage of Quantum Cryptography**

1. There will likely be a rise in unemployment as a result of this being implemented globally.
2. Many essential functions, including digital signatures and certified mail, are missing from quantum cryptography.
3. A photon's polarisation may vary as it passes through the channel (such as an optical fibre or the air) for a variety of reasons.

**More application of Quantum Cryptography**

Beside Quantum Key Distribution, it may play role in various crypto-tasks.

1. ***Quantum random number generation:*** Apart key distribution, Quantum random number generators are aspiring to be a new standard of random ness generators, and current level of quantum technology suffice are providing not only a good source of genuine randomness but also gaining importance in algorithms for simulation.
2. ***Quantum Secret sharing:*** Quantum Secret Sharing is a fundamental primitive in Quantum Cryptography. It is used widely to design schemes for digital signature, key management, secure multi party computation etc. Basically, it splits a secret into two or several shares and distribute among multiple agents.
3. ***Quantum Private Query:*** Private information retrieval, often known as a private query, is a crypto-task that enables a user to access a database item from the server without knowing which item the other party has previously retrieved.
4. ***Quantum Finger printing:*** Quantum Finger printing protocol is the ability to distinguish between any two strings of quantum information just by knowing their fingerprints. To do this, finger prints were transmitted in the form of single-photon pluses to two detectors. If pluses are different, both detectors click, if not then only one of them clicks.

***Benefits and Drawbacks***

| | |
|---|---|
| ■ **Confidentiality -** Encryption technique can guard the information and communication from unauthorized revelation and access of information. | ■ **High availability**, one of the fundamental aspects of information security, cannot be ensured through the use of cryptography. Other methods are needed to guard against the threats such as denial of service or complete breakdown of information system. |
| ■**Data Integrity** - The cryptographic Hash functions are playing vital role in assuring the users about the data integrity. | ■ A strongly encrypted, authentic and digitally signed information can be **difficult to access even for a legitimate user** at a curcial time of decision-making. The network or computer system can be attacked and rendered non-functional by an intruder. |

**Differences between Classical and Modern Cryptography**

| *Classical Cryptography* | *Modern Cryptography* |
|---|---|
| It is mainly based on '**security through obscurity**'. The Techniques employed for coding were kept secret and only the parties involved in communication knew about them. | It relies on publicly known mathematical algorithms for coding the information. Secrecy is obtained through a secret key which is used as the seed for the algorithms. The computational difficulty of algorithms, absence of secret information even if he knows the algorithm used for coding. |
| It requires the entire **Cryptosystem** for communicating confidentially. | **Modern Cryptography** requires parties Interested in Secure communication to process the secret key only. |

## IV CRYPTANALYSIS

Cryptanalysis is the study over cryptology that follows all its functions and instructs how to break or attack the algorithms, encryption technique. Its main target is finding the secret key which helps to decrypt the data.

Cryptanalysis Techniques and Attacks can be classified into the followings:

- ***Cipher-text only attack:*** During this attack, attacker knows only the **cipher text.** We are not giving any extra facility to the attacker. They only have the access to this cipher text and have out of knowledge about the plain-text. The goal of the attacker is to recover as much as plain text data is recover as much as plain text data as possible to guess *the Secret Key*. While designing encryption algorithms, it is most important to secure them against cipher text only attack.

- ***Known Plain-text attack:*** In this attack knows some pair of plain text and cipher text. That's mean they has an access to the plain text and its corresponding cipher text. Their goal is to get the secret key such that it helps to decrypt this process they are not able to crack the secret key actively. Its use in simple substitution cipher is significant.
- ***Chosen Plain text attack:*** In this attack adversary can choose the plain text and can get the corresponding cipher text from the sender without knowing the key. The attacker may get much encryption machinery. They try to crack the Secret key or guess the encryption algorithm to decrypt any cipher text using the secret key (It should be noted that the attacker does not have a secret key but he can get that key through this chosen Plain text attack).
  - ***Chosen Cipher text attack:*** An attack paradigm for cryptanalysis known as a "chosen cypher text attack" allows the cryptanalyst to get data by acquiring the decryptions of the chosen Cypher texts. The adversary might try to discover the hidden secret key used for decryption using these bits of information. Like previous assaults, the chosen cypher text attack may be adoptive or non-adoptive. In an adopted selected cypher text attack, the attacker can make decisions about which cypher texts to decode based on the outcomes of previous decryptions. The attacker in a non-adoptive attack selects the cypher texts to be decoded without viewing any of the resultant plain texts. The attacker is no longer able to decipher subsequent cypher texts after reading the plain texts.
  - ***Brute Force Attack:*** In this attack, the adversary tries to break the key property. He alters any possible key or passwords to decrypt the cipher text and to get the correct plain text. It's too much time-consuming process than other attacks. For breaking cipher using Brute Force Attacks, very fast specially designed super computer are used.

Cryptanalysis can be further divided into three parts.

- ***Differential Cryptanalysis:*** A differential cryptanalysis attack is a type of chosen plaintext attack on block ciphers that analyses pairs of plaintexts rather than single plain-texts, so the analyst can determine how the targeted algorithm works when it encounters different types of data.
- ***Integral Cryptanalysis:*** Comparable to differential cryptanalysis assaults, integral cryptanalysis employs sets of plaintexts instead of pairs of plaintexts where part of the plaintext is maintained while the remainder is changed. This attack is particularly effective when used against block cyphers built on substitution-permutation networks.
- ***Linear Cryptanalysis:*** Every primitive internally uses non-linear transformations (otherwise it would be a linear function and hence can easily be distinguished). The idea of linear cryptanalysis is to approximate the non-linear transformations with linear equivalents in order to build equations involving only plain-text, cipher-text and key bits.

The whole cryptanalysis process depends on the mathematical base. Some mathematical oriented tools are used for cryptanalysis. They are

- ***CrypTool:*** This is an open source project. It creates web portals for learning about cryptanalysis and encryption algorithm.
- ***Cryptol:*** The National Security Agency originates a specific language centred cryptographic algorithm, which is known as cryptol.

- ***Crypto Bench:*** This is a type of program. It can be used to decrypt cipher-text created using many simple algorithms.

**Cryptanalysis** doesn't mean hackers are associated with it. These are many responsibilities of *Cryptanalysis behind cryptography.*

- The responsibilities of *Cryptanalyst* are as follows:

i. Cryptanalysts are employed to strengthen and improve encryption algorithms so that the sensitive information, hidden messages etc. is not easily leaked. They also concern about the protection of cipher-text, encrypted data and telecommunications protocols.
ii. Business companies, government agencies use Cryptanalysis to make the information sent through their computer networks more secure, to make the algorithms more complex.
iii. They search the weakness in communication lines.
iv. Developing the models with the help of mathematics and statistics.

**Difference between Cryptography and Cryptanalysis**

| ***Topics*** | ***Cryptography*** | ***Cryptanalysis*** |
|---|---|---|
| ***1) Definition*** | 1) The art of encrypting i.e. changing Plain-text to Cipher-text to secure when messages are sent. | 1) The art of decrypting i.e. changing Cipher-text to it's Plain- text without any key. |
| ***2) Goal*** | 2) Securing the data from the adversaries. | 2) Breaking the secured data and finding the Encryption Key. |
| **3) Characteristic** | 3) It uses the functions encryption, Decryption, substitution, Transposition and product system. Also it was the key as Public Key And private key. | 3) Basically decryption is the main operation. It works over the Cipher-text with the help of Encryption algorithm. |
| **4)Expert** | 4) Cryptographer. | 4) Cryptanalyst. |

**APPLICATIONS**

- ***Digital Signatures / Authentication:*** Digital Signature of a document is a piece of information based on both the document and the signer's private key. This digital signature may be used for verification if someone wishes to check the sender, time, and date of any document. It is created through the use of hash function and a private signing function.
- ***Time Stamping:*** Time stamping basically uses an encryption model named blind signature scheme. This scheme allows the sender to receive a message receipted by another party without revealing it to the other party. In a nutshell it verifies that an electronic document, communication, or delivery was made at a specific moment.

- ***Encryption and decryption in Email:*** Email encryption is a technique for protecting email content from prying eyes during email conversations. After encryption, the only thing that can still be read by humans is the private email key. Everybody who has an email account has two keys, one of which is a "public key" that anybody connected to your name or email address may access, and the other is a "public key" that is not disclosed publicly. There are other forms of email encryption, including Open PGP, S/MIME, etc. PGP uses a decentralised, distributed trust model, but S/MIME, which is incorporated into Apple devices, uses a centralised authority to choose the encryption technique and key size. In addition, the link that email offers allow for encryption of both email content and stored messages to deter hackers.
- ***Cryptocurrency:*** A cryptocurrency is a type of currency which uses digital files as money and basically an internet based medium of exchanging normal currencies like USD etc. but later designed for the purpose of exchanging digital information, uses cryptographic functions to conduct financial transactions. Bitcoin, XRP, and Ethereum are the cryptocurrencies, mostly used.

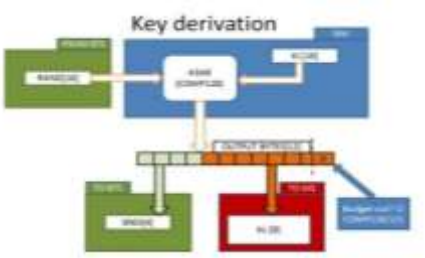
Without a single administration or central bank, *bitcoin* is a decentralised digital money. It is a computer file that is kept in a computer or phone app as a "Digital Wallet." The second-largest cryptocurrency is called Ethereum. The cryptocurrency created by Ethereum miners is called Ether. The Ripple Network (a platform that serves as both a cryptocurrency and a digital payment network for financial transactions) uses XRP to symbolise the movement of value across the network. *For example,* a person can send Bitcoins to another person and that person can send it to another person too and this continuous process of transactions are recorded into *Blockchain* (*a chain block which contains information*). A bitcoin block includes sender and recipient details. The first block is known as Genesis Block.

*Blockchain* is a publicly accessible ledger where users may add data and verify that they agree with the transaction using an elliptic curve digital signature technique. This algorithm combines an elliptic Curve and a Finite Field to 'sign' data with bitcoin, and the data represents the transaction that transfers ownership.

Now Zero-knowledge proof is a scheme and it’s agreement is a method by which certifying party can prove that something is true to the verifying party.

Both Bitcoin and Ethereum networks use public addresses to replace the true identity of the party, making transaction partially anonymous except the sending and receiving address and the amount is there to be known. Zero knowledge proof can remain it anonymous while guaranteeing the transactions are valid. Z cash may be the Blockchain project, implement zero known ledge proof & Z cash implements modified version of ZKP called ZK-SNARKS. Reduces the size of the proofs and the amount of computation. It makes valid transactions without revealing any crucial information by the proof of two polynomial products are equal along with homomorphic encryption and other techs.

- ***Encryption in WhatsApp:*** Previously we have told that WhatsApp uses ‘end-to-end’ encryption process to hide the messages from a third party. It employs the "signal" encryption protocol, which combines symmetric and asymmetric cryptographic algorithms to ensure confidentiality and integrity while asymmetric algorithms are used to achieve other security objectives like authentication and non-repudiation.




- ***Sim Card Authentication:*** Authentication is required in order to determine if the SIM may access the network. The number (random) passes through A3 algorithms with the secret key KI, then the operator produces a random number and sends it to the device, where it runs through A8 algorithms with KI to generate a session key KC. To encrypt or decrypt data, KC is used in conjunction with the A5 algorithm.
- ***Encryption in Instagram:*** When our phone asks data from Instagram, it utilises SSL/TLS over port 443 to encrypt the request from Instagram servers and will deliver data over the same encrypted data stream. This encryption keeps third parties from listening in on the discussion.

# V CONCLUSIONS

we have had knowledge on how the whole cryptosystem is entirely connected with our daily routine where cryptography is providing us the way to secure our private data like name, address etc. on the basis of several mathematical applications and algorithms and beside this cryptanalysis is having importance in strengthening encryption algorithms, searching for weakness in communication system to serve us a modified version of it to communicate more securely. last but not the least, quantum cryptography is going raise its importance in this field day by day.

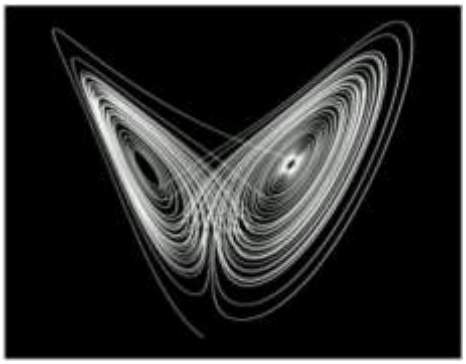
Nowadays cryptosystem is a subject that will make many improvements in the future. MIT, which has been developed using Number Theory and other mathematical concepts will use new applications from encryption method and will try trying to get 100% free from adversaries. Neutral networks are now able to secure data. As we can see in most of the cell phones fingerprint lock which is an important example in encryption method. Thus, the crypto currency is becoming more technologically advanced. Now let us see how different fields of cryptosystem can be further developed in the future.

**Quantum and post-quantum Cryptography:** Quantum cryptography covers a wide area of our progress. In the era of quantum computing, there are similar terms of this field for data protection and communication, such as quantum-cryptography, quantum-encryption, quantum-proof encryption, quantum security, post-quantum cryptography. *Post-quantum* cryptography, also termed as quantum-proof cryptography, is a way of ensuring secure communication in future by upgrading mathematical-based algorithms and standards, which is indeed different from the quantum-physics based quantum-cryptography.

**Multivariate Cryptography:** Communication security can be guaranteed in the presence of quantum computer using multivariate cryptography. Encryption and decryption algorithms can be made much stronger based on multivariate mapping.

**DNA Cryptography:** DNA cryptography is also rapidly processing. A DNA-based implementation of YAEA encryption algorithm could easily be improved using a larger DNA strand. Now, in technical world, DNA sequences are used in secret data writing. In steganography and authentication, DNA computing can lead to a brighter future possibility.

**Chaos-based Cryptography:** Chaos-based Cryptography has drawn the interest of academics in two fields: nonlinear dynamic systems and cryptography. The study of a certain form of system that arose from some beginning conditions is known as chaos theory. A little change in the initial configuration of a chaotic system might result in significantly different behaviours. The unpredictability and ergodicity qualities of a chaotic system are helpful for creating data protection solutions. Numerous examples of chaos-based algorithms have been proven to be insecure while being in their early stages. However, the significant research being conducted in this subject cannot be overlooked when considering the future prospects of cryptography.



**Homomorphic Cryptography:** Even when data is encrypted and sent over the internet or secured, some vulnerabilities exist. Homomorphic encryption is a novel idea that will aid us in solving this challenge. This is the type of process that will allow data to be processed without being decrypted.

# REFERENCES


1. Xiaoqing Tan (July 17th 2013). Introduction to Quantum Cryptography, Theory and Practice of Cryptography and Network Security Protocols and Technologies, Jaydip Sen, IntechOpen, DOI: 10.5772/56092.
2. Tianqi Zhou, Jian Shen, Xiong Li, Chen Wang, Jun Shen, "Quantum Cryptography for the Future Internet and the Security Analysis", Security and Communication Networks, vol. 2018, Article ID 8214619, 7 pages, 2018.
3. J Aditya, PS Rao, Quantum Cryptography - Proceedings of computer society of India, 2005
4. https://www.garykessler.net/library/crypto.html
5. https://searchsecurity.techtarget.com/definition/encryption
6. https://medium.com/searchencrypt/what-is-encryption-how-does-it-work-e8f20e340537
7. https://www.cis.upenn.edu/~nadiah/courses/cis800-02-f13/
8. https://resources.infosecinstitute.com/top-30-cryptographer-interview-questions-and-answers-for-2019/
9. https://www.eng.tau.ac.il/~yash/crypto-netsec/classical.htm
10. https://www.coindesk.com/math-behind-bitcoin
11. https://medium.com/hackernoon/wtf-is-zero-knowledge-proof-be5b49735f27
12. https://medium.com/dataseries/explaining-the-math-behind-blockchain-algorithms-98d06e06c2e3#:~:text=Blockchain%20is%20a%20publicly%20available,%2B%207%20(see%20graph)
13. https://searchsecurity.techtarget.com/
14. https://www.cloudflare.com/learning/ssl
15. https://reverus.com/
16. https://www.popularmechanics.com/science/a25699/how-quantum-teleportation-works/
17. https://www.sciencealert.com/entanglement