NATIONAL SKILL TRAINING INSTITUTE (W)

SEC-V, KOLKATA

A PROJECT ON-CRYPTOGRAPHY

SUBMITTED BY:

TRADE NAME : ADV.DIPLOMA IN CLOUD COMPUTING AND NETWORKING(IBM).

SESSION:2019-2021

TRAINING INCHARGE: ABHISHEK RAMAN

1.SOMA SANTRA(GROUP LEADER).

2.SANJUKTA DUTTA.

3.RUPAMA MAJEE.

4.NIHARIKA SINGH

AKNOWLWDGEMENT

- We have taken efforts in this project. However,it would not have been possible without the kind support and help of many individuals and organizations. We would like to extend our sincere thanks to all of them.

- We are highly indebted to the teacher in charge "MR. Abhishek Raman"(Edunet Foundation)For his able guidance and constant supervision as well as providing necessary information regarding the project & also for his support in completing the project.

- We would also like to extend our gratitude to our principal sir of NSTI (W)Saltlake kolkata "SRI G.C RAMAMURTHY " & trade in charge of adv. Diploma in cloud computing and networking "MR. SARBOJIT NEOGI " for providing golden opportunity of this project.

- We are really thankful to our peer group and our team members ,who helped us a lot in finalizing the project within the limited time frame.

CONTENT OF THE PROJECT:

INTRODUCTION OF CRYPTOGRAPHY:

What is Cryptography?

- Science of writing Secret Code.

Historical background of cryptography:

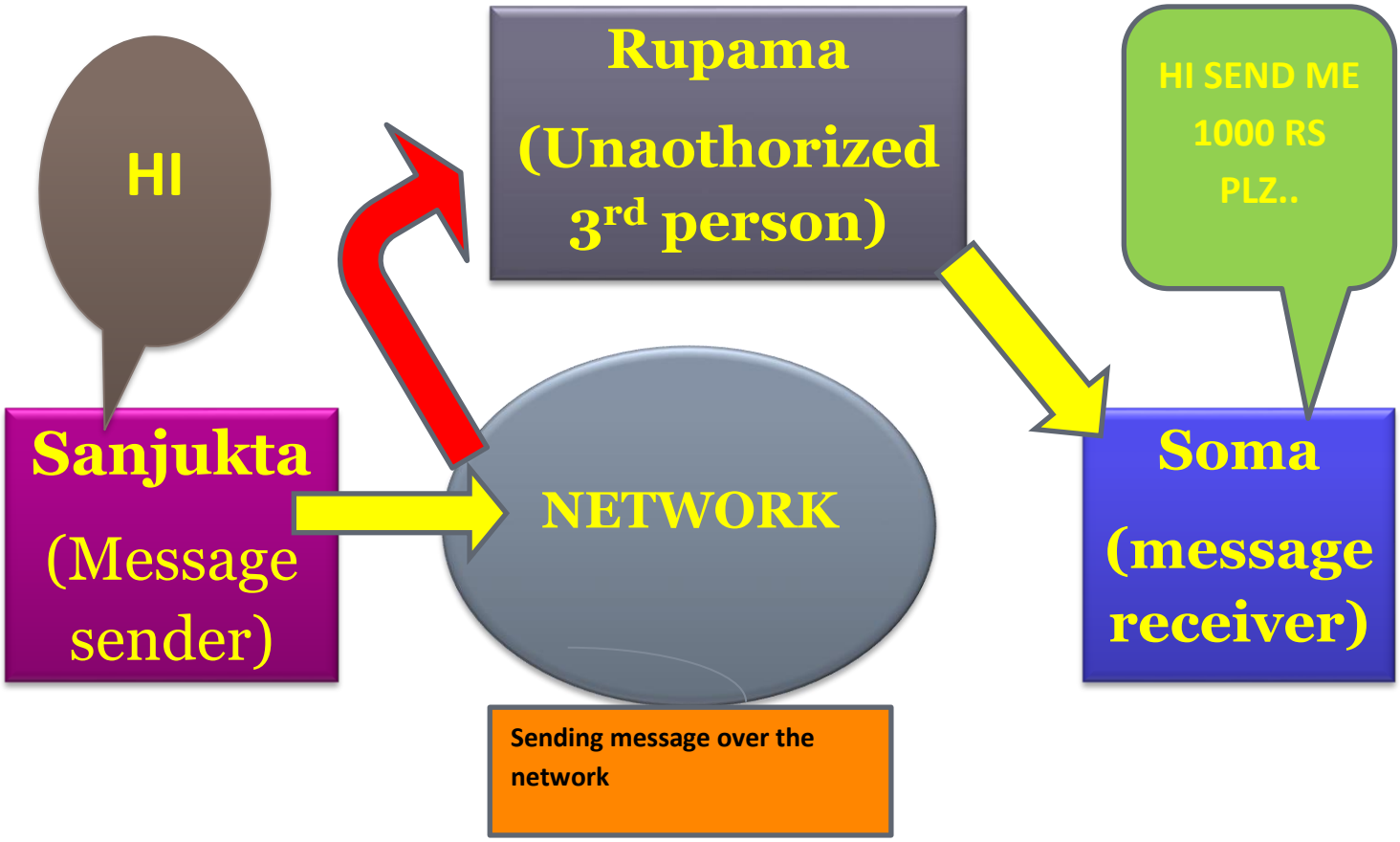
- The First use of Cryptography in 1900 B.C. Used by Egyptian Scribe.
- Some experts say it appeared right after writing was invented

- Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans.

- Crypto means hidden secret and graphien means to write. Cryptography is a process of converting a plain text into an encrypted message and then decrypting it again to plain text by intended users. This is mostly done to avoid adversaries or so that it can be protected by an unintended user.

Simple example on cryptography:

- Let's say there's a lady named *Sanjukta*. Now suppose *sanjukta* sends a message to her friend *soma* who is on the other side of the world. Now obviously she wants this message to be private and nobody else should have access to the message. She uses a public forum, for example, WhatsApp for sending this message. The main goal is to secure this communication.

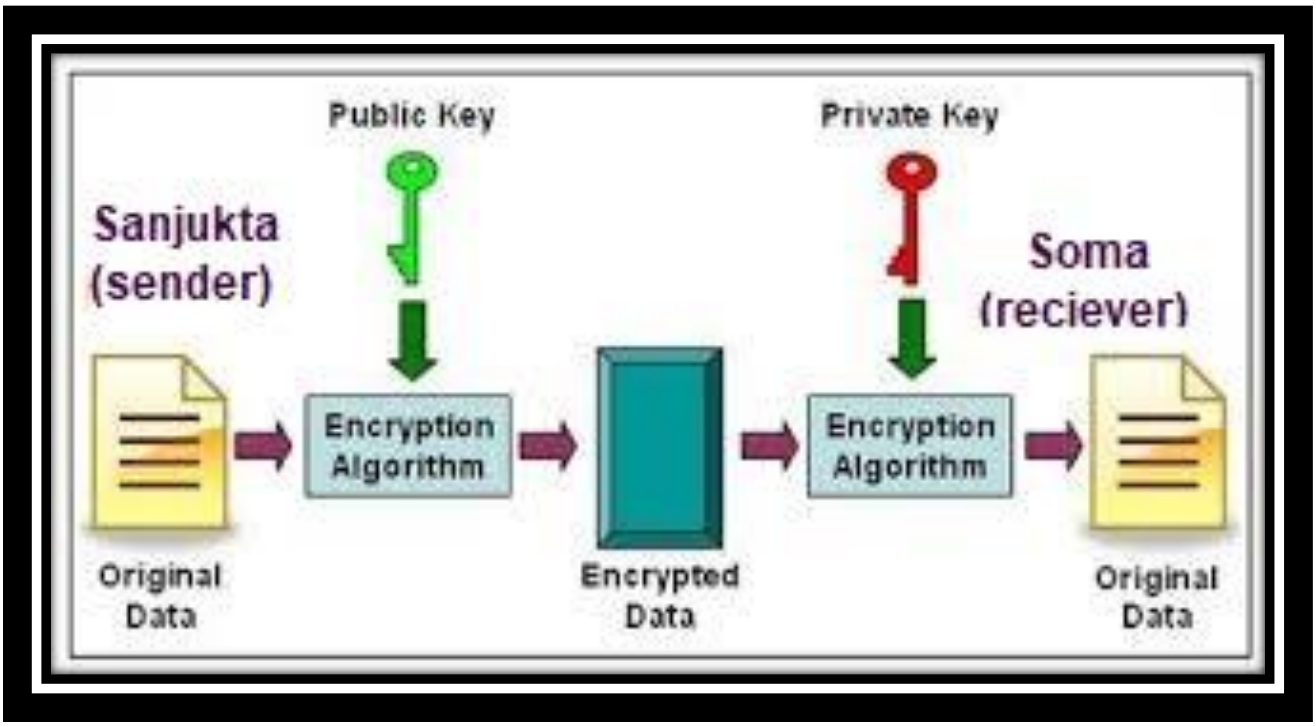


Let's say there is a smart lady called *Rupama* who secretly got access to your communication channel. Since this lady has access to their communication, she can do much more than just eavesdropping, for example, she can try to change the message. Now, this is just a small example. What if *Rupama* gets access to your private information?The result could be catastrophic.

- So how can *Sanjukta* be sure that nobody in the middle could access the message sent to soma?Now the answer will be Cryptography.

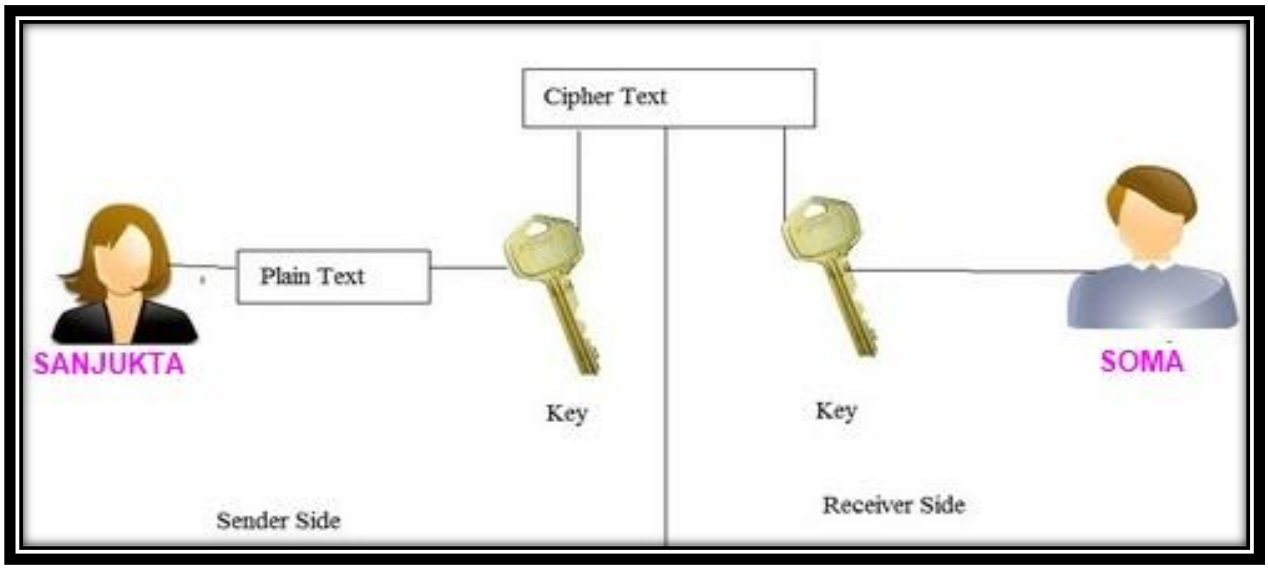
So in a simple word Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

Lets have a look on this picture:



now that you know " what is cryptography " let's see how cryptography can help secure the connection between Sanjukta and Soma.

So, to protect his message, *Sanjukta* first convert his readable message to unreadable form. Here, he converts the message to some random numbers. After that, she uses a key to encrypt his message, in Cryptography, we call this *ciphertext***.**



Sanjukta sends this *ciphertext* or encrypted message over the communication channel, she won't have to worry about somebody in the middle of discovering his private messages. Suppose, *rupma* here discover the message and she somehow manages to alter it before it reaches *Soma*.

After using the key for decryption what will come out is the original *plaintext* message, is an *error*. Now, this error is very important. It is the way *Soma* knows that message sent by *Sanjukta* not the same as the message that she received. Thus, we can say that encryption is important to communicate or share information over the network.

Why cryptography used for?

- Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. The prefix "crypt-" means "hidden" or "vault" -- and the suffix "-graphy" stands for "writing."

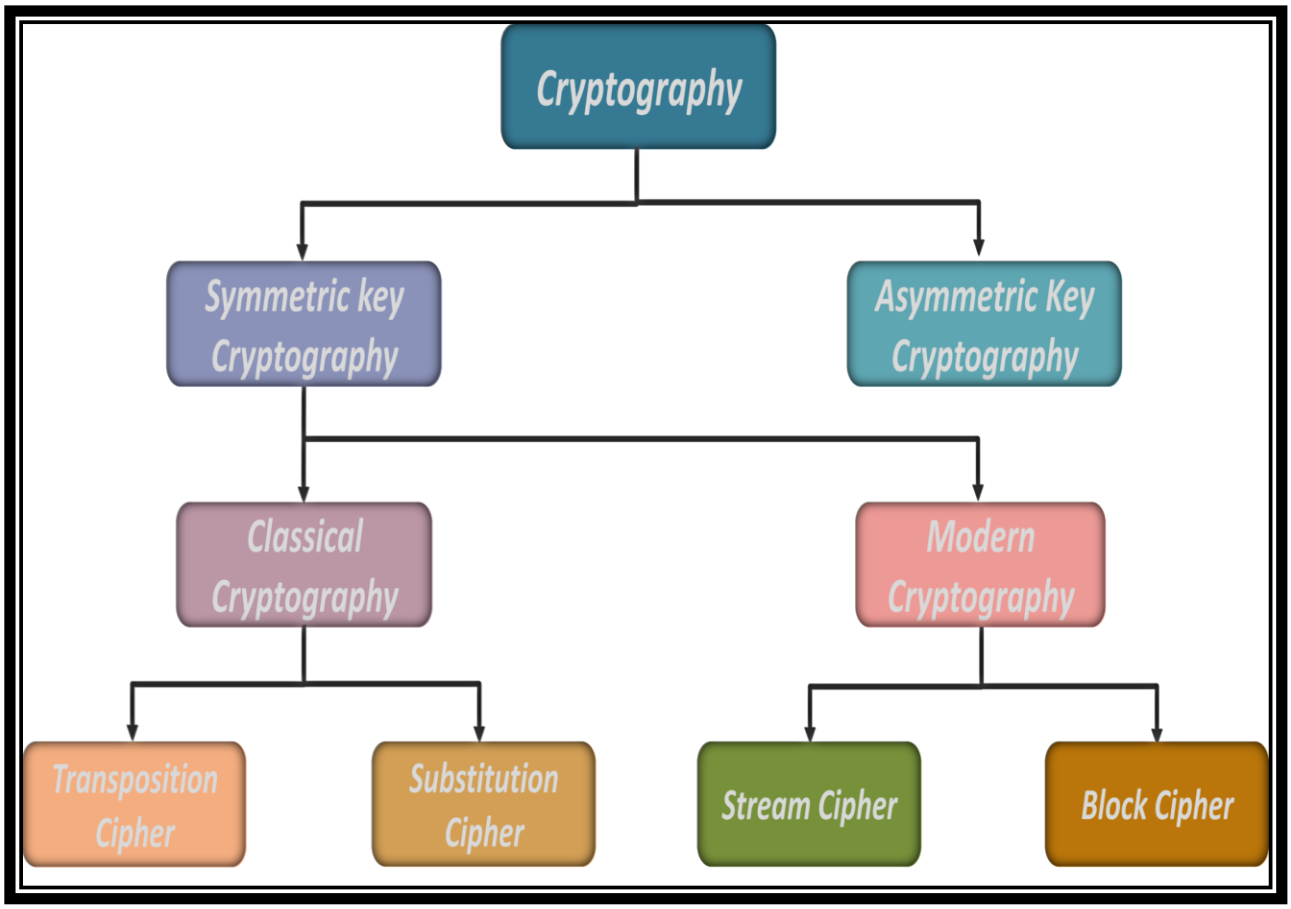
- In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet, and confidential communications such as credit card transactions and email.

- It is said that most deadly war that can happen on internet will be caused by a hacker. By attacking our personal, professional and confidential data. But still how can we make secure online payments? How the websites on which we create our account ensures that our data is safe and secure with them? How businesses and government agencies protect their data from these hackers? Well, the answer to all of these questions **is** CRYPTOGRAPHY**.**
- Modern cryptography uses sophisticated mathematical equations (algorithms) and secret keys to encrypt and decrypt .data.Today, cryptography is used to provide secrecy and integrity to our data, and both authentication and anonymity to our communications.

TYPES OF CRYPTOGRAPHIC FUNCTIONS

1. Decryption is the reverse of encryption, and Hash functions-it involves the use of zero keys.
2. Secret key functions-it involves the use of one key.
3. Public key functions-it involves the use of two keys.

TYPES OF CRYPTOGRAPHY:

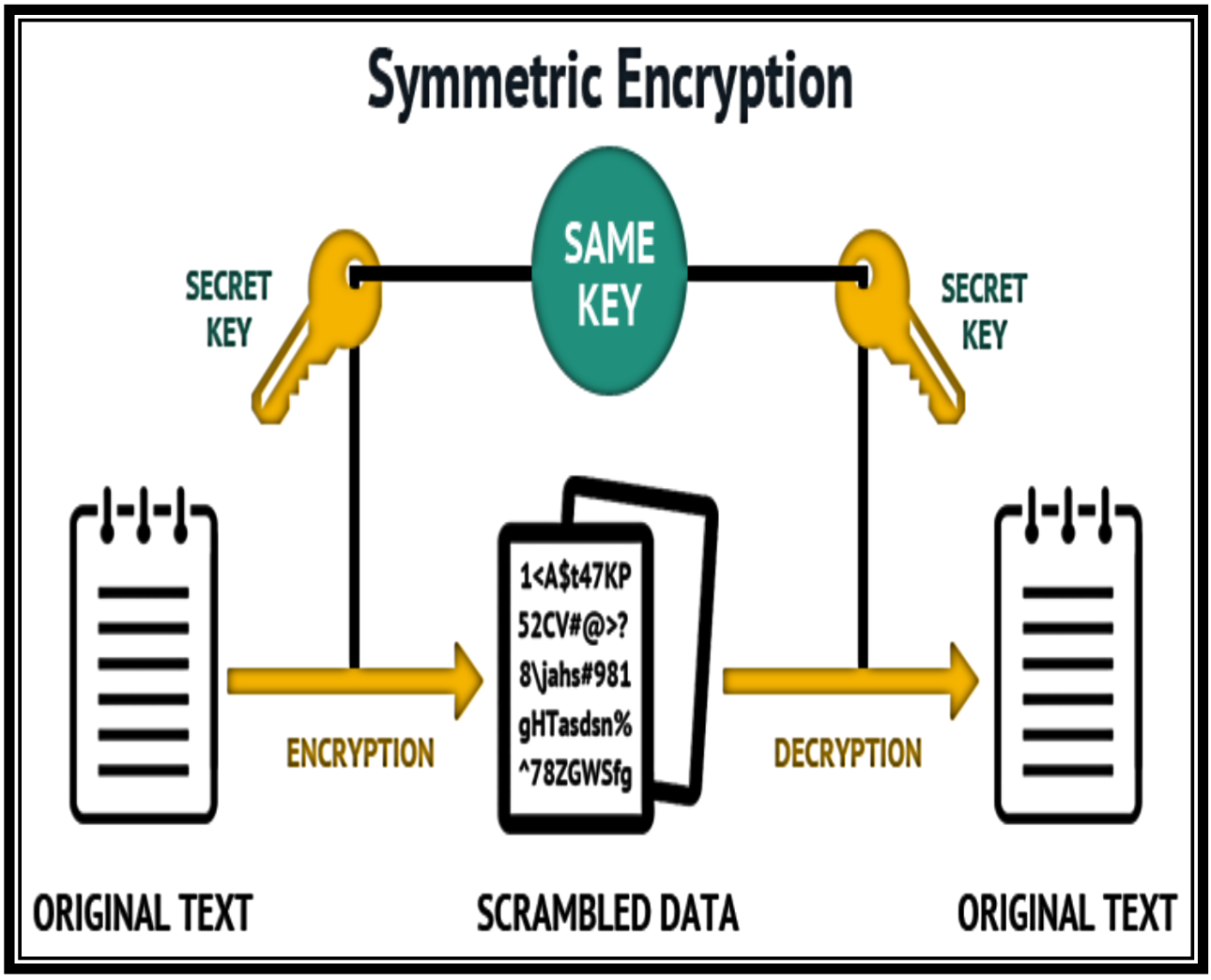


♦ **What are the two main types of cryptography?**

There are two main types of cryptography systems : symmetric (" private key ") and asymmetric (" public key ")

Symmetric Key Cryptography:

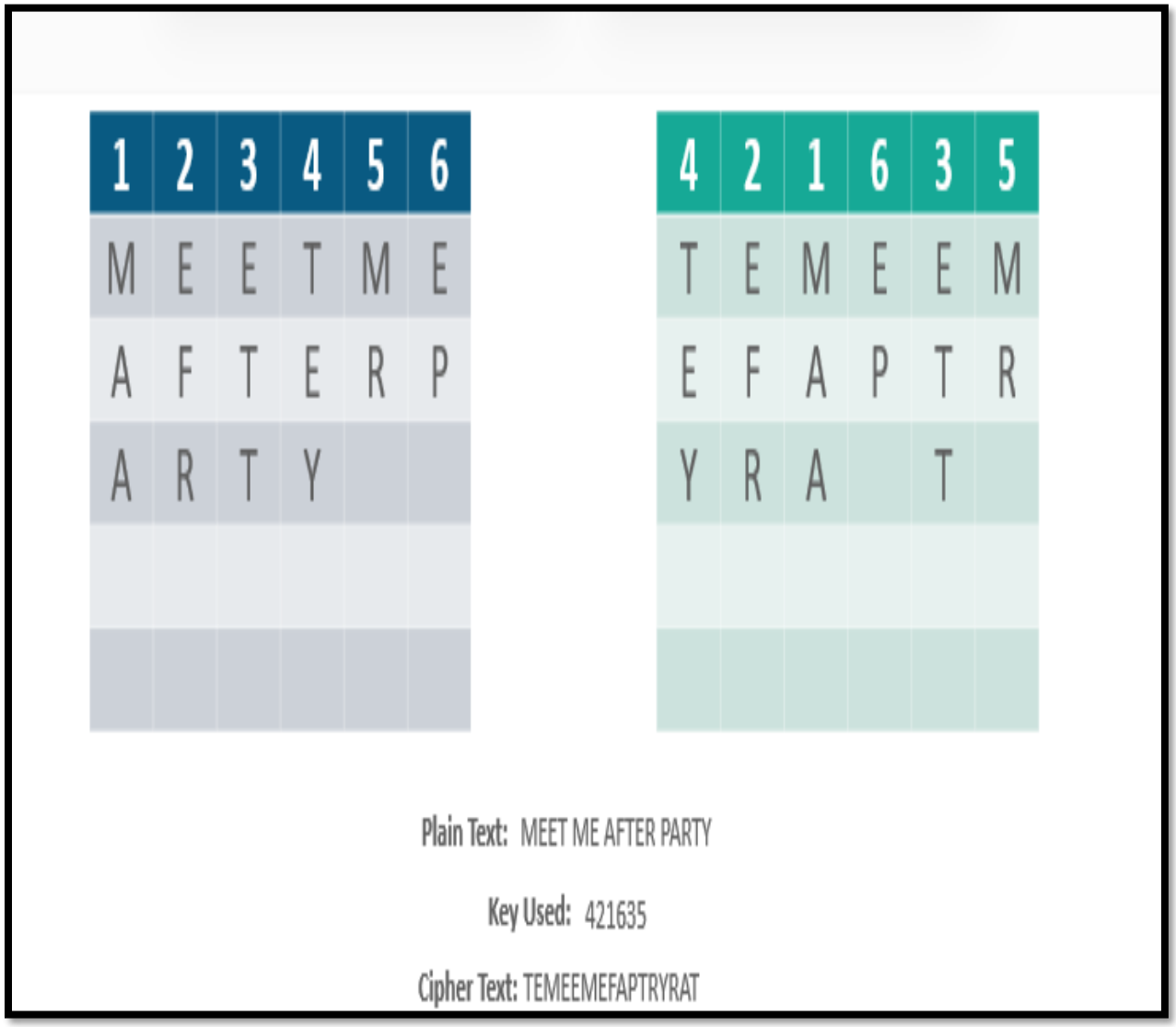
It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography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



Transposition Ciphers:

In Cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext.

Example:

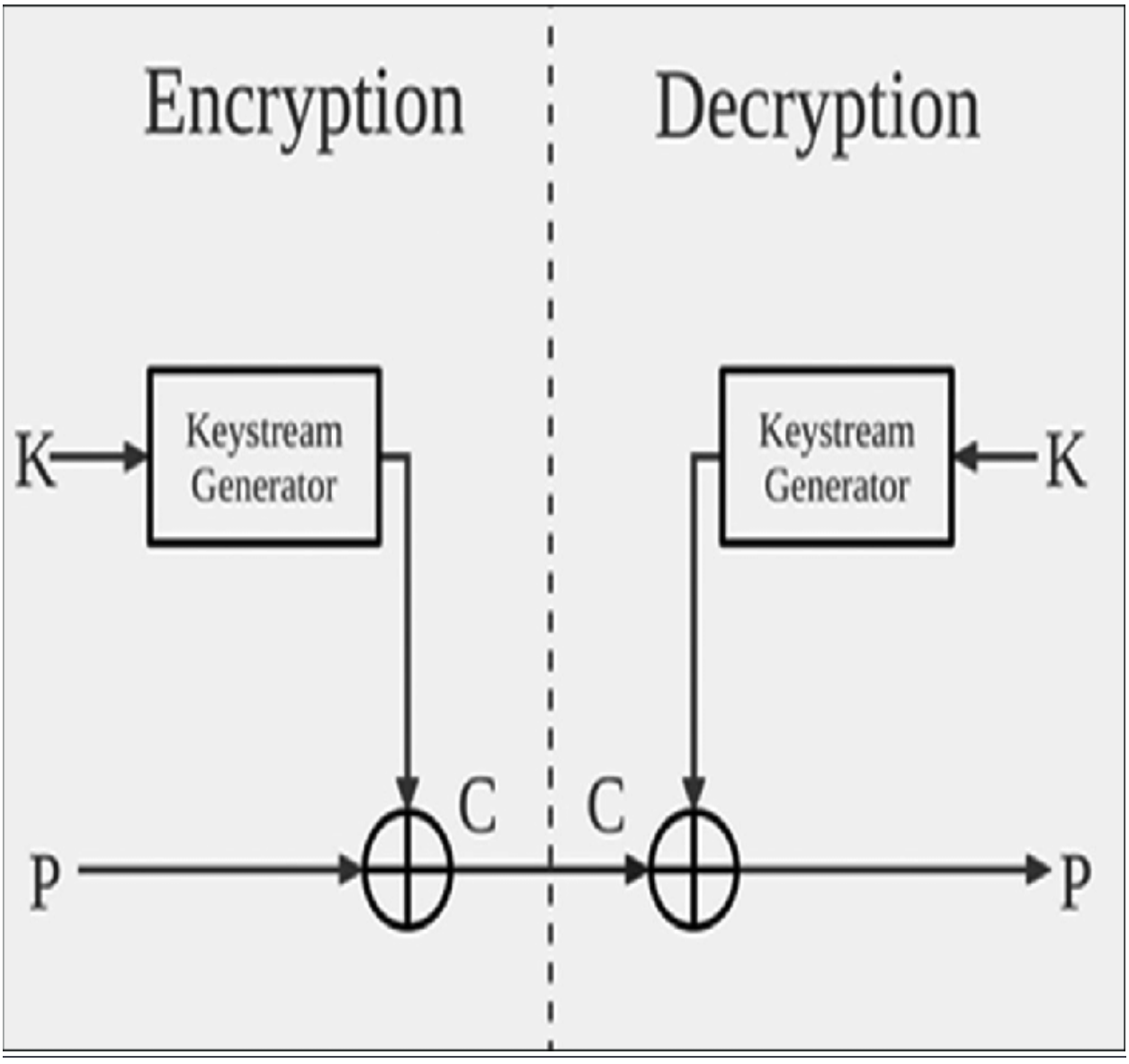


That is, the order of the units is changed (the plaintext is reordered). Mathematically, a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt.

Stream Cipher:

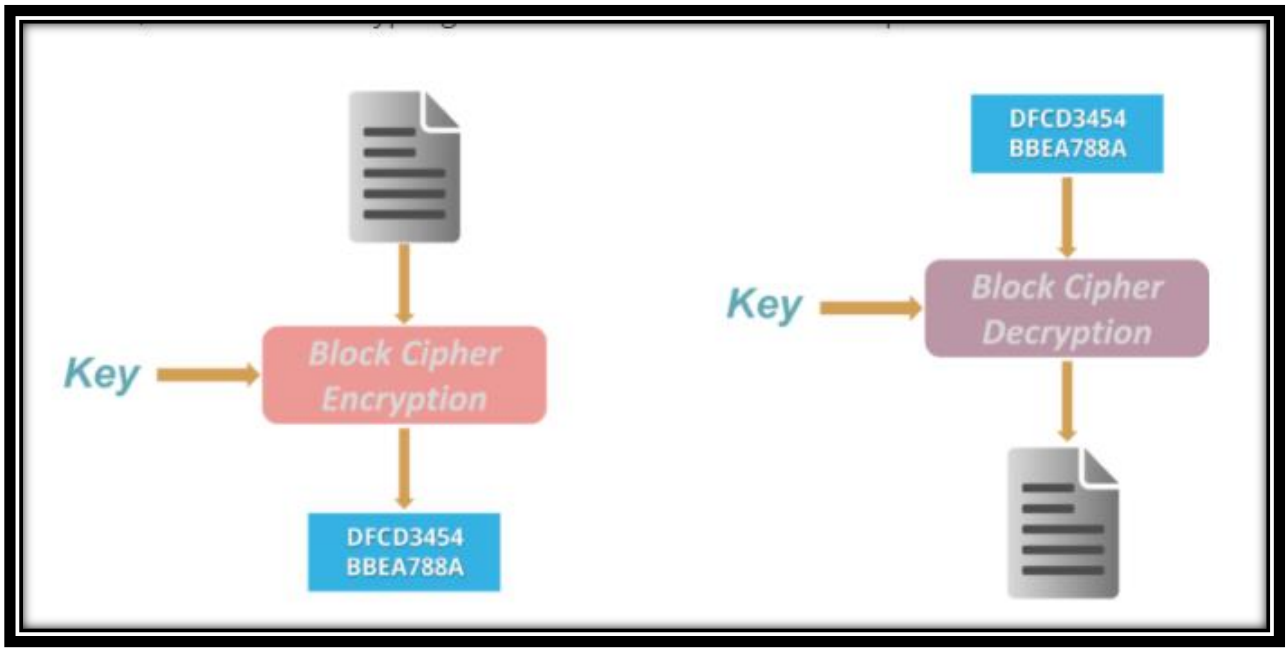
symmetric or secret-key encryption algorithm that encrypts a single bit at a time. With a Stream Cipher, the same plaintext bit or byte will encrypt to a different bit or byte every time it is encrypted.

Example:



Block Cipher:

A block cipher is an encryption method that applies a deterministic algorithm along with a symmetric key to encrypt a block of text, rather than encrypting one bit at a time as in stream ciphers. For example, a common block cipher, AES, encrypts 128 bit blocks with a key of predetermined length: 128, 192, or 256 bits. Block ciphers are pseudorandom permutation (PRP) families that operate on the fixed size block of bits. PRPs are functions that cannot be differentiated from completely random permutations and thus, are considered reliable, until proven unreliable.

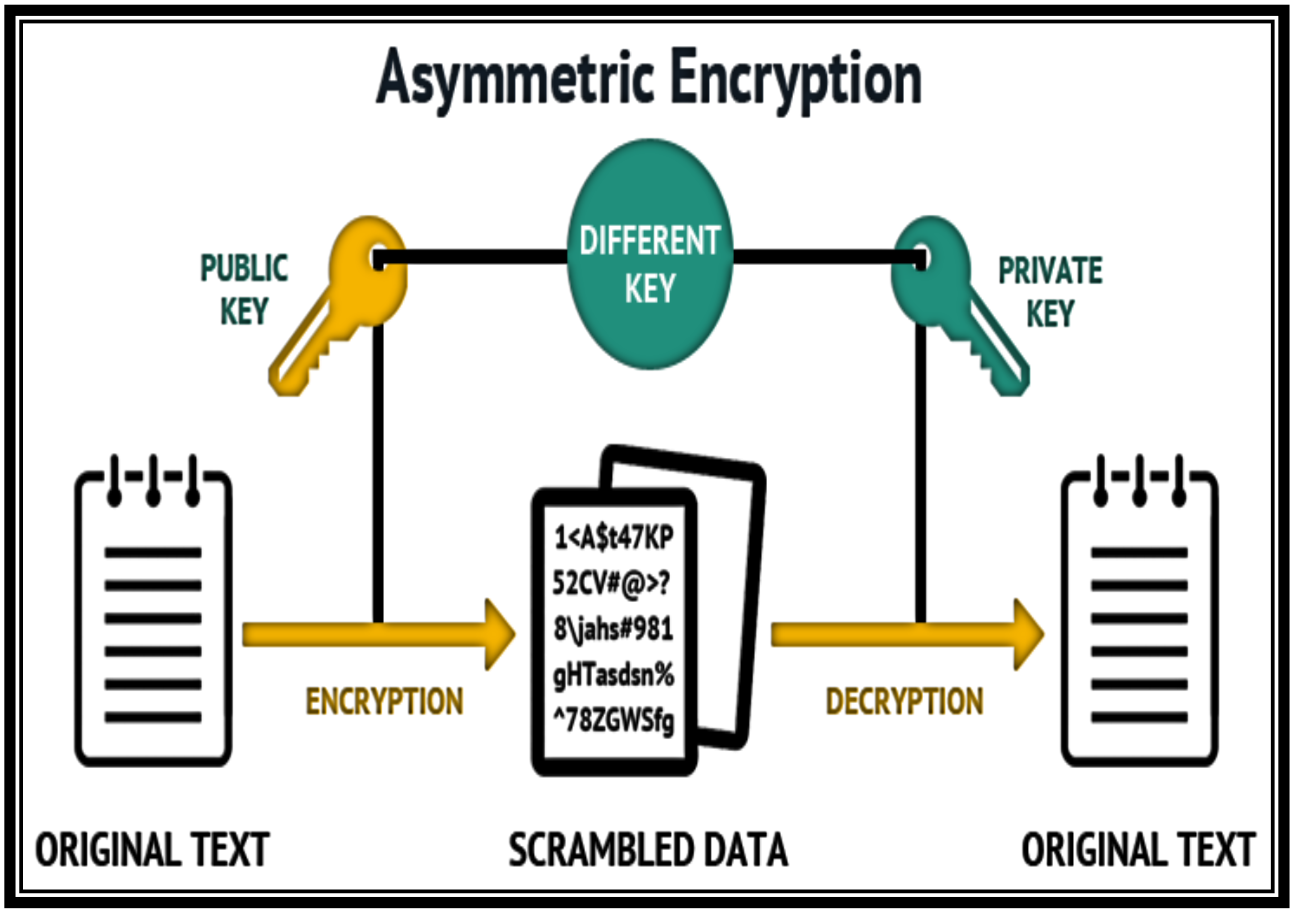


Block cipher modes of operation have been developed to eliminate the chance of encrypting identical blocks of text the same way, the ciphertext formed from the previous encrypted block is applied to the next block. A block of bits called an initialization vector (IV) is also used by modes of operation to ensure ciphertexts remain distinct even when the same plaintext message is encrypted a number of times.

Note: 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.

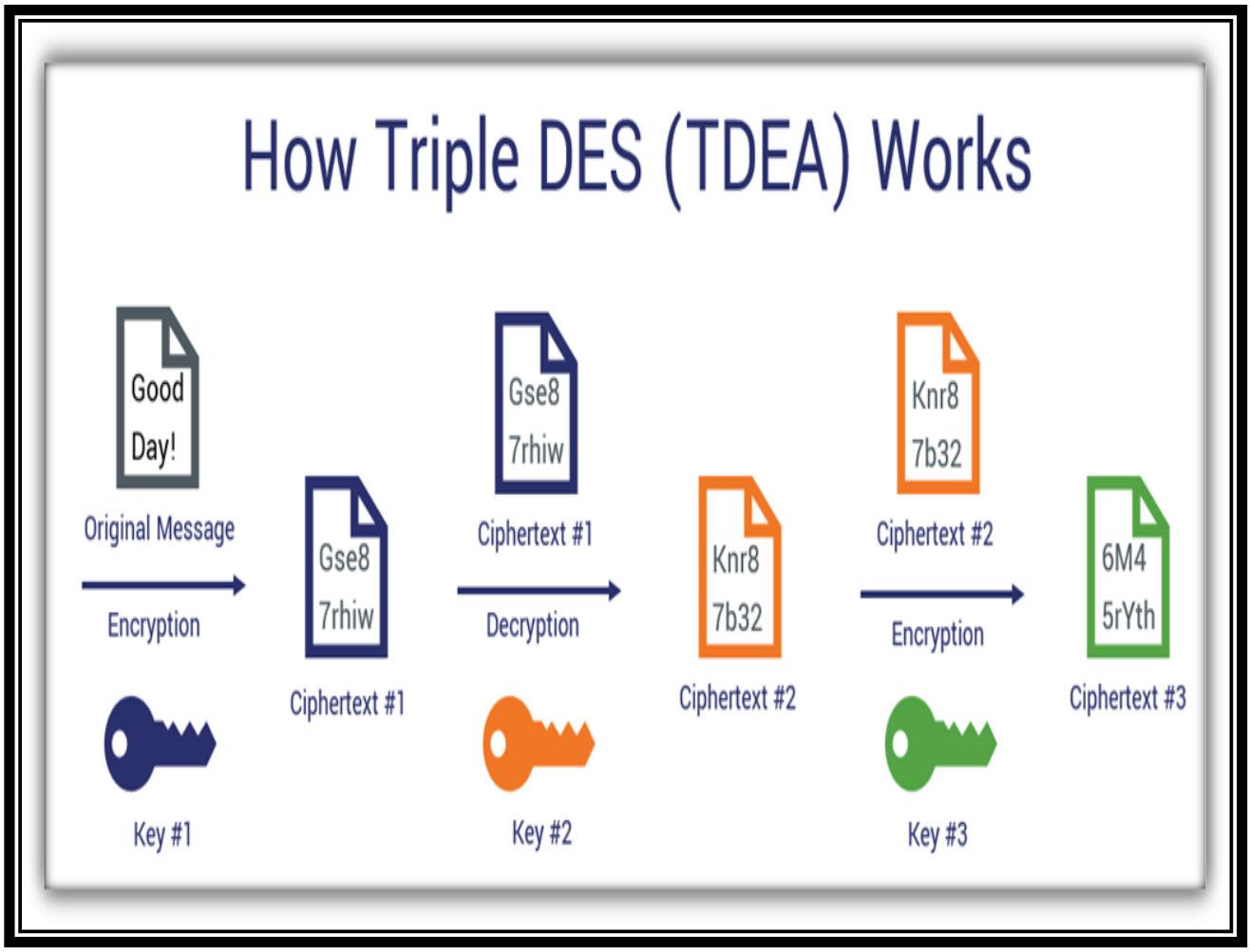


The encryption process where different keys are used for encrypting and decrypting the information. Keys are different but are mathematically related, such that retrieving the plain text by decrypting ciphertext is feasible.

Algorithms used in cryptography

Triple DES:-

Triple DES is an encryption technique which uses three instance of DES on same plain text. It uses there different types of key choosing technique in first all used keys are different and in second two keys are same and one is different and in third all keys are same. 3DES is an improvement over des, but each has their benefits and opportunities for improvements.



The encryption-decryption process is as follows –

· Encrypt the plaintext blocks using single DES with key K1.

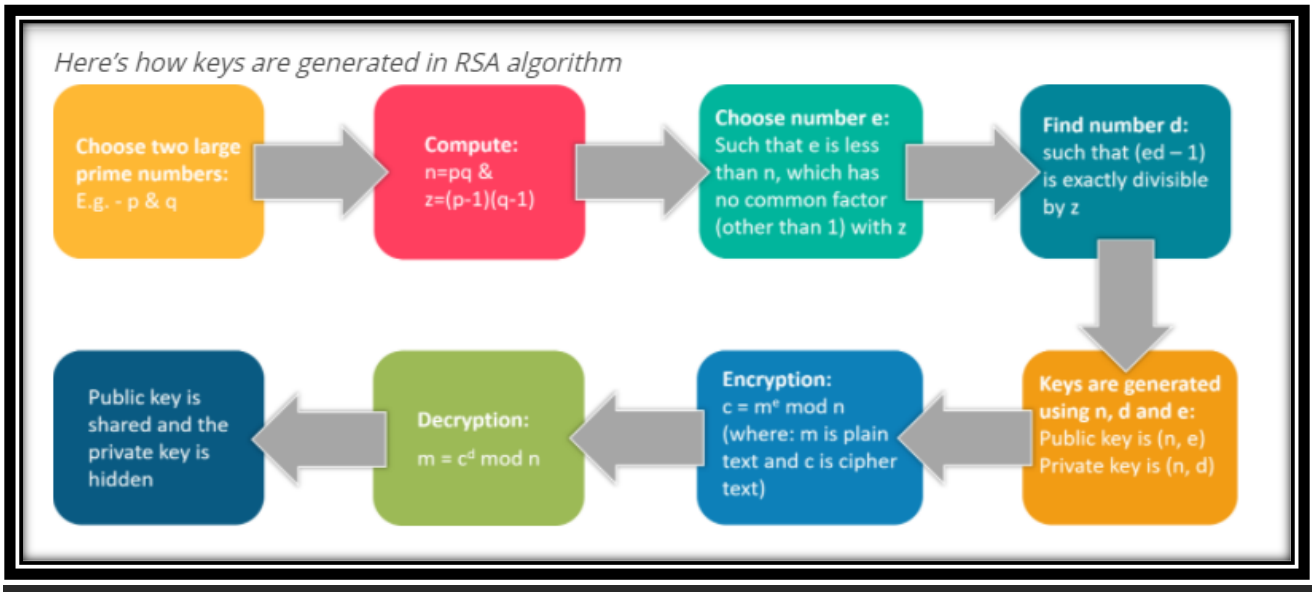
· Now decrypt the output of step 1 using single DES with key K2.

· Finally, encrypt the output of step 2 using single DES with key K3.

The output of step 3 is the cipher text. Decryption of a ciphertext is a reverse process. User first decrypt using K3, then encrypt with K2, and finally decrypt with K1.

RSA

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private.



RSA Component Features

- Public/private key generation.
- Encrypt with either public or private key.
- Decrypt with matching public or private key.
- Create digital signatures.
- Verify digital signatures.
- Encrypt and decrypt in-memory strings or byte arrays of any size.

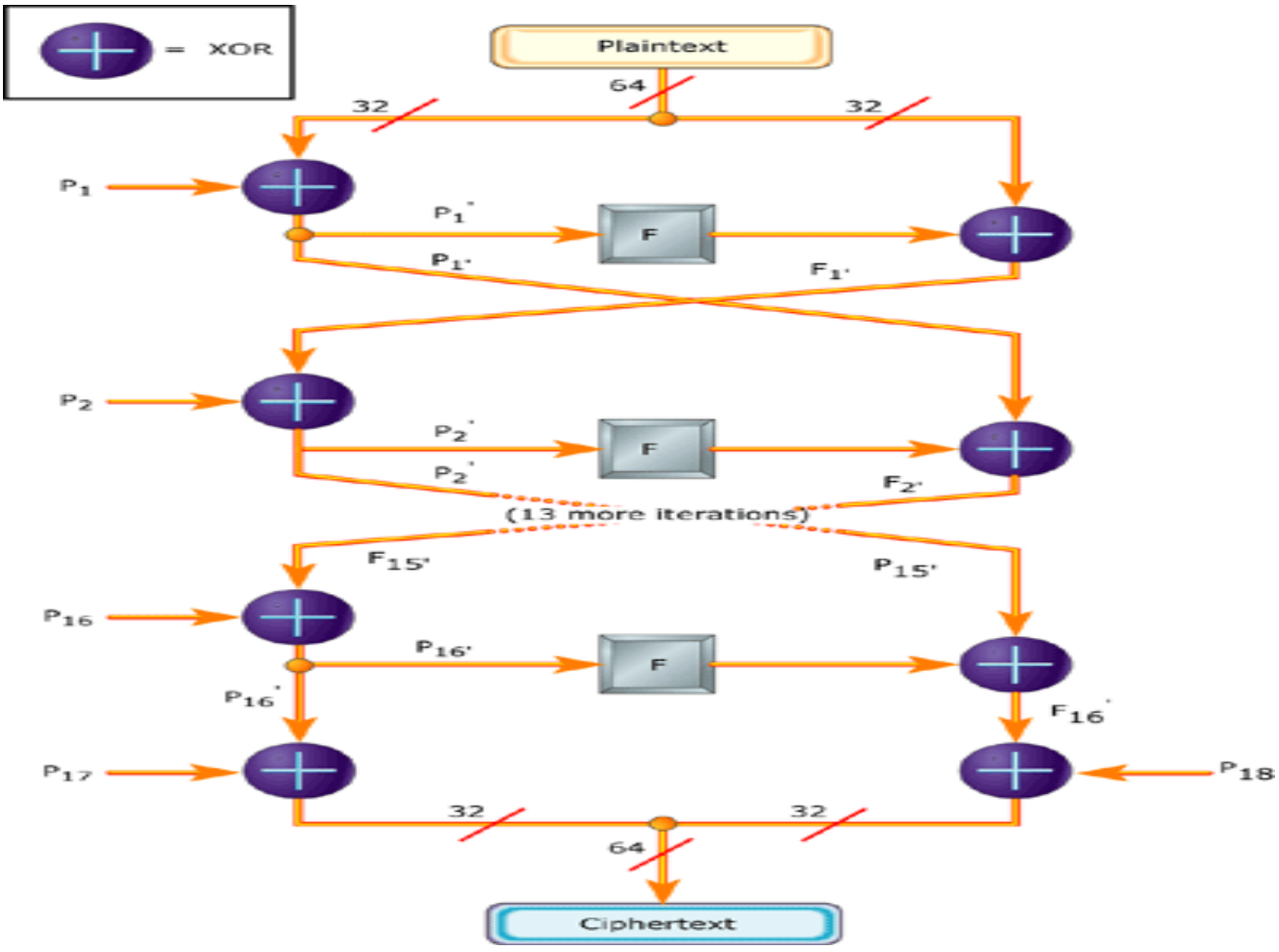
- Encode encrypted output to Base64, Hex, Quoted-Printable, or URL-encoding
- Export public/private key pairs to XML.
- Import key pair from .snk file.
  - Import public/private key pairs from XML.
  - Import/Export only public-part or private-part of key pair.
  - PKCS v1.5 padding for encryption and signatures.
  - OAEP Padding Scheme for Encryption/Decryption
  - RSASSA-PSS (RSA Signature Scheme with Appendix — Probabilistic Signature Scheme)
  - Create/verify signatures with little-endian or big-endian byte ordering.
  - Supports key sizes ranging from 512 bits to 4096 bits.
  - Supports hash algorithms: MD5, SHA-1, SHA-2 (SHA-256, SHA-384, SHA-512), and more…
  - Thread safe.

How RSA works:

- The intention is that messages encrypted with the public key can only be decrypted in a reasonable amount of time by using the private key. The public key is represented by the integers n and e; and, the private key, by the integer d (although n is also used during the decryption process. Thus, it might be considered to be a part of the private key, too.
-

Blowfish:

Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. Blowfish is an alternative to DES Encryption Technique.



Why is Blowfish used for?

Blowfish is an encryption algorithm that can be **used as** a replacement for the DES or IDEA algorithms. It is a symmetric (that is, a secret or private key) block cipher that **uses** a variable-length key, from 32 bits to 448 bits, making it useful for both domestic and exportable use

What does block size mean?

Block size can refer to: Block (data storage), the size of a block in data storage and file systems. Block size (cryptography), the minimal unit of data for block ciphers. Block (telecommunications) Block size (mathematics).

What is keySize of 32 bits or 448 bits?

Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. In structure it resemblesCAST-128, which uses fixed S-boxes.

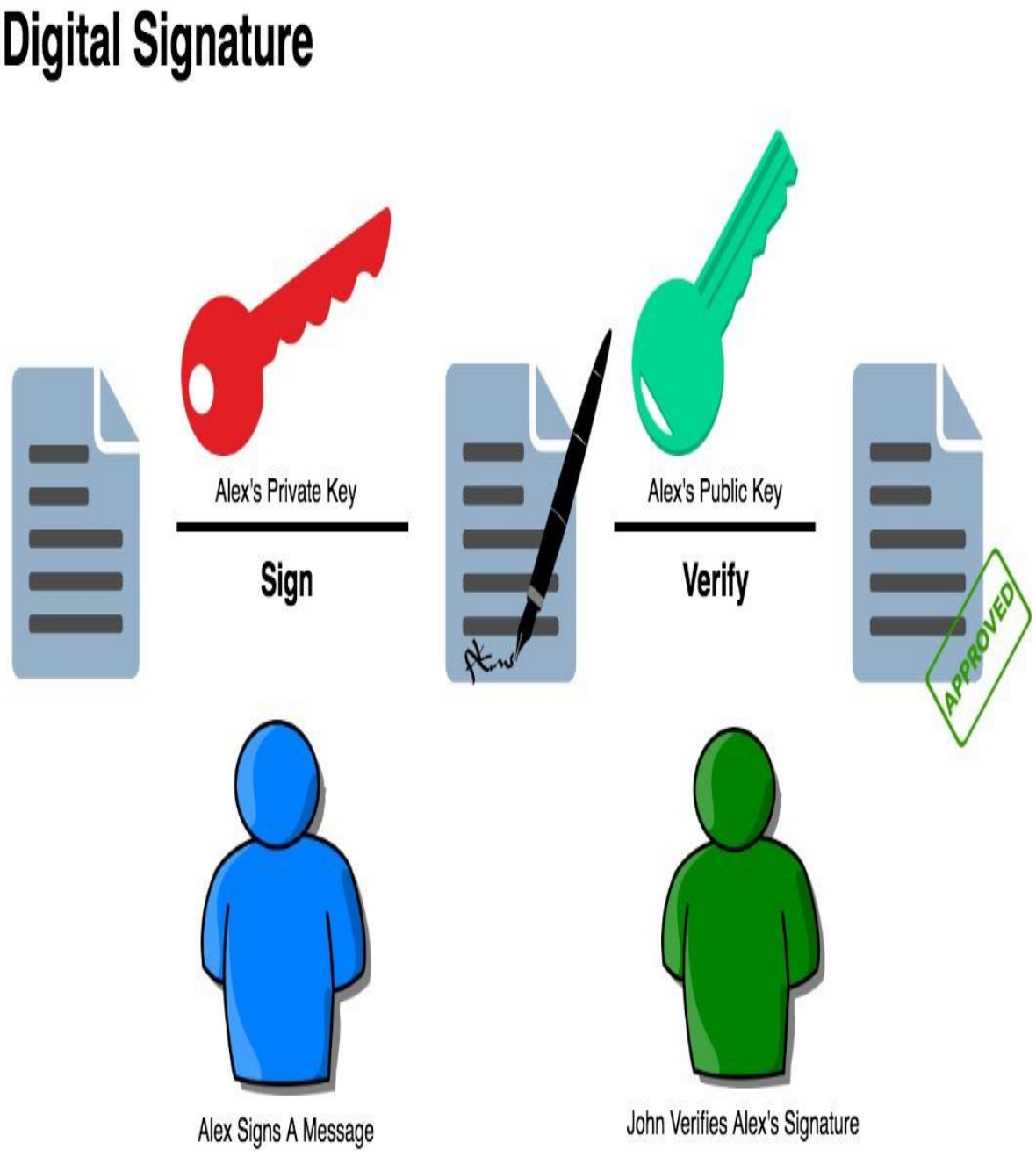
Features:-

Block cipher: 64-bit block

Variable key length: 32 bits to 448 bits

Much faster than DES and IDEA

Unpatented and royalty-free and No license required.

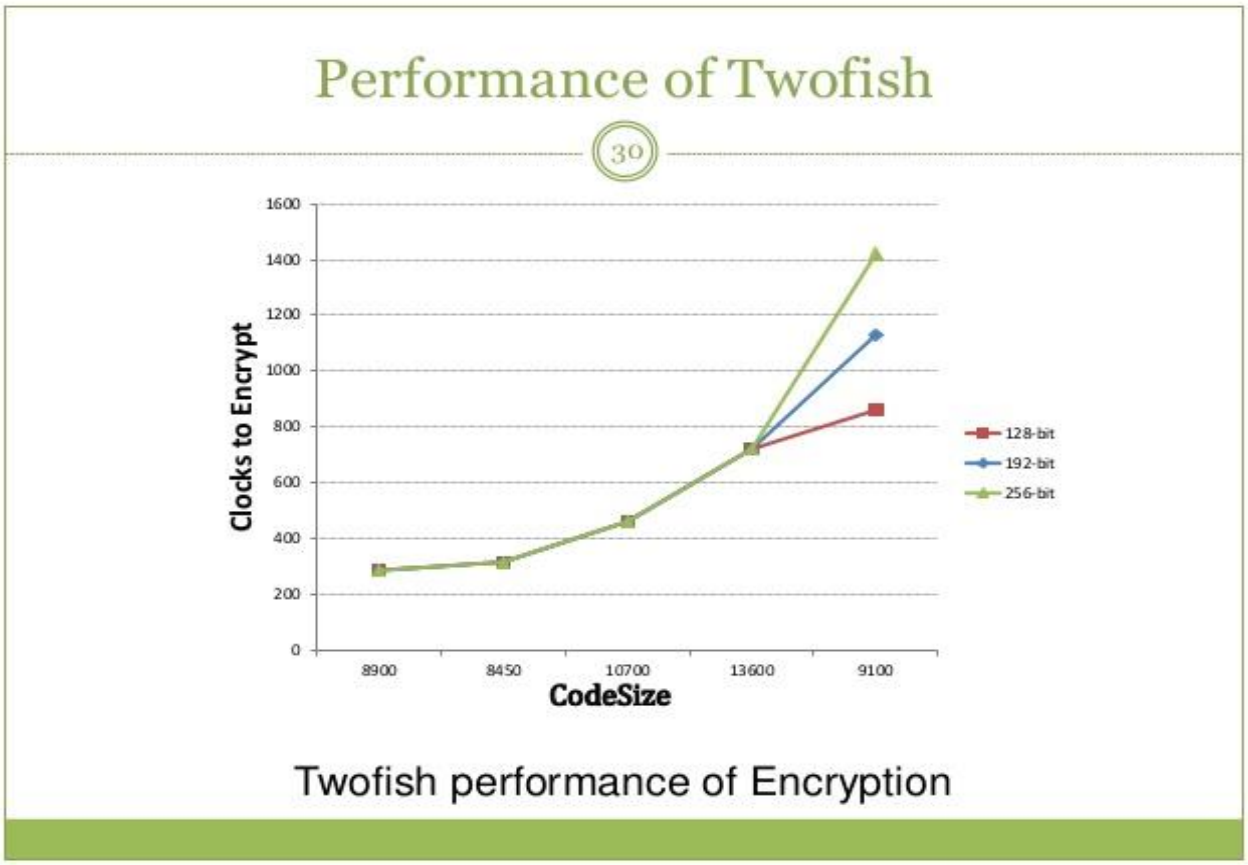


The diagram to the right shows Blowfish's F-function. The function splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The outputs are added modulo232 and XORed to produce the final 32-bit output.

Twofish

Twofish is a symmetric block cipher; a single key is used for encryption and decryption.

It has a block size of 128 bits, and accepts a key of any length up to 256 bits.



Features:

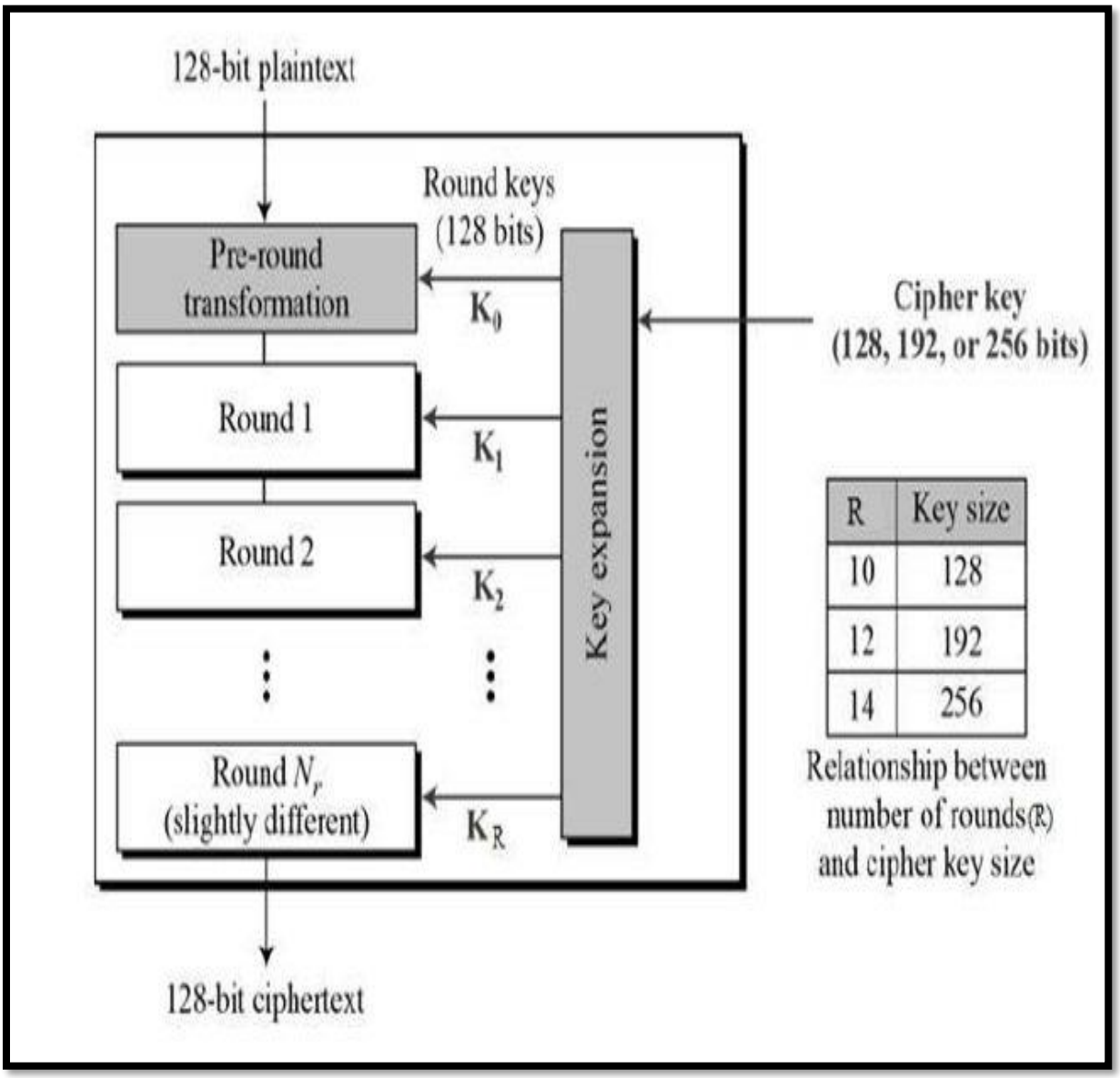
1.128 bit block cipher

2.Uses 16 rounds of Feistel network and key length of 128 bit,192 bits and 256 bits No weak keys.

3.Key length of 128 bit,192 bits and 256 bits No weak keys.

AES

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data AES is six times faster than Triple DES.AES is much faster than RSA.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

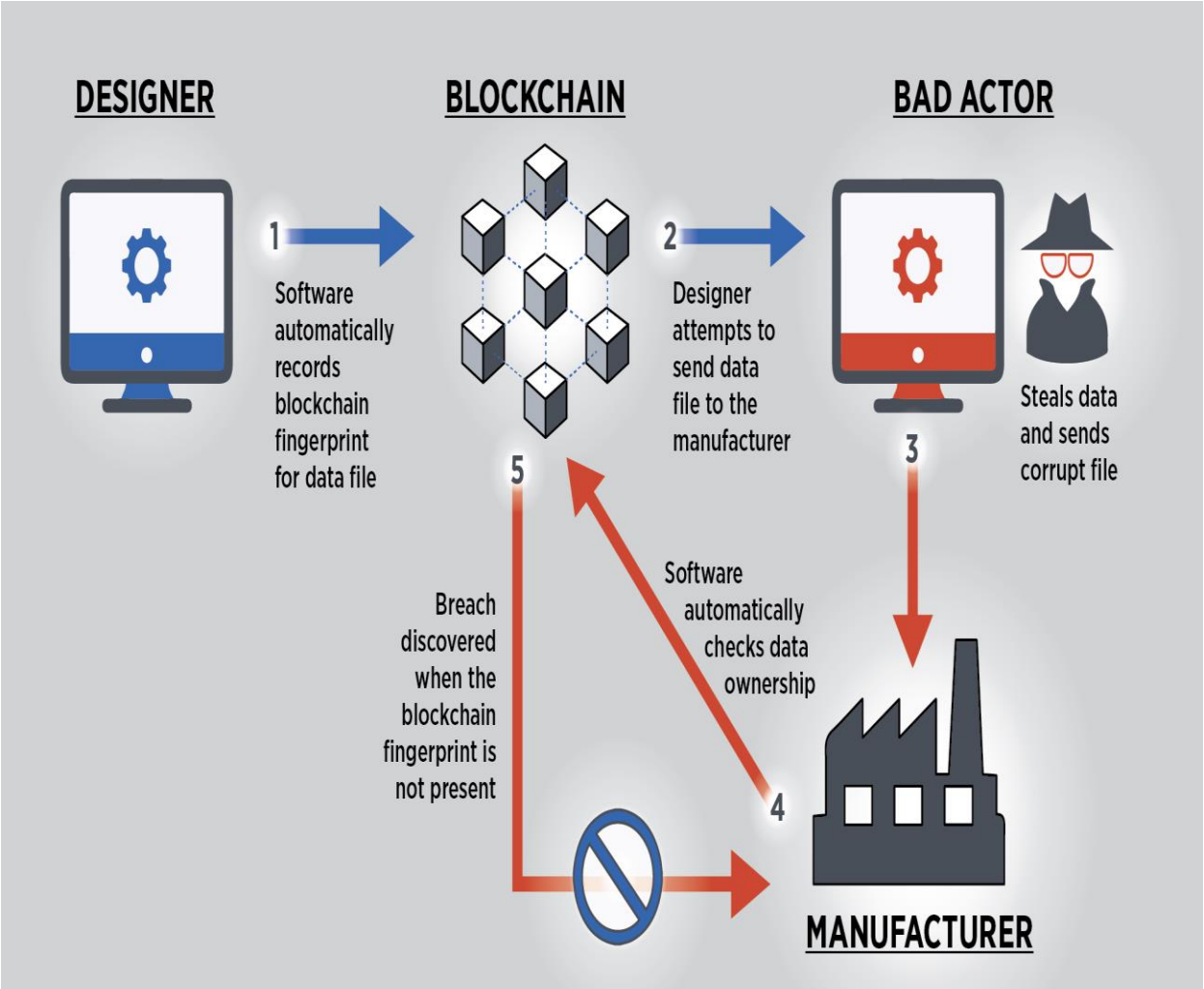
The features of AES are as follows :

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

- AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix he number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

Blockchain

It's decentralized nature and cryptographic algorithm make it immune to attack. In fact, **hacking** a **Blockchain** is close to impossible. In a world where cyber security has become a key issue for personal, corporate, and national security, **Block chain** is a potentially revolutionary technology.



Features:

1. Cannot be Corrupted
2. Decentralized Technology
3. Enhanced Security
4. Distributed Ledgers
5. Consensus
6. Faster Settlement.

One of the application of block chain is bit-coin.

What Bit-coin means?

virtual currency,Bit-coin, often described as a cryptocurrency, a virtual currency or a digital currency - is a type of money that is completely virtual. It's like an online version of cash. ... People can send Bit-coins (or part of one) to your digital wallet, and you can send Bit-coins to other people.

What is Blockchain in cryptography ?

Blockchains make use of two types of cryptographic algorithms, asymmetric-key algorithms, and hash functions. Hash functions are used to provide the functionality of a single view of blockchain to every participant. Blockchains generally use the SHA-256 hashing algorithm as their hash function.

What is Bit-coin used for?

Bit-coin is a new currency that was created in 2009 by an unknown person using the alias Satoshi Nakamoto. Transactions are made with no middle men – meaning, no banks! **Bit-coin** can be **used** to book hotels on Expedia, shop for furniture on Overstock and buy Xbox games.

Visual cryptography

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption can be done just by sight reading.

Features:-

1) The independence of pixel's encryption
2) Easy matrix generation
3) Simple operations

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images and layers are required to reveal the information.

BENEFITS OF CRYPTOGRAPHY

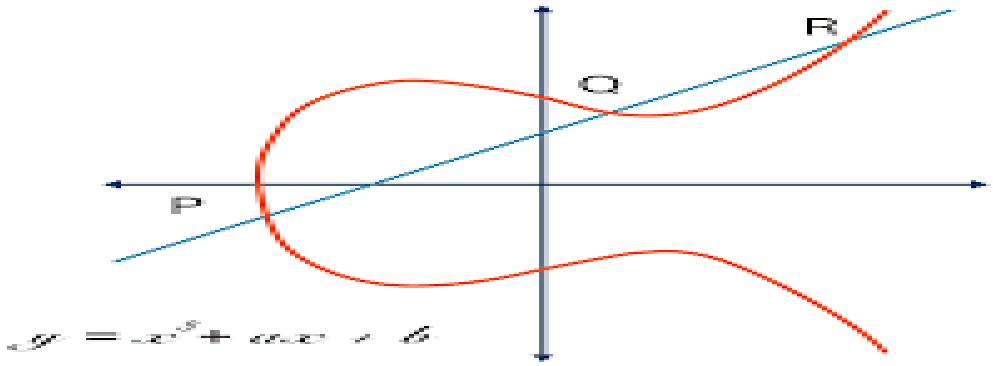
- Cryptography is an essential information security tool. It provides the four most basic services of information security –
- **Confidentiality** – Encryption technique can guard the information and communication from unauthorized revelation and access of information.
- **Authentication** – The cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries.
- **Data Integrity** – The cryptographic hash functions are playing vital role in assuring the users about the data integrity.
- **Non-repudiation** – The digital signature provides the non-repudiation service to guard against the dispute that may arise due to denial of passing message by the sender.

APPLICATIONS OF CRYPTOGRAPHY:

- To safe user's websites.
- Secure online transactions which is very important for now a days.
- For encryption of files it gives user more security.
- Military communications.
- Encryption in your social mediaaccount like facebook,whatsapp.
- Sim card Authentication.
- Electronic Money.
- Device authentication.

Future of Cryptography

Elliptic Curve Cryptography (ECC) has already been invented but its advantages and disadvantages are not yet fully understood. ECC allows to perform encryption and decryption in a drastically lesser time, thus allowing a higher amount of data to be passed with equal security. However, as other methods of encryption, ECC must also be tested and proven secure before it is accepted for governmental, commercial, and private use.



Quantum computation is the new phenomenon. While modern computers store data using a binary format called a "bit" in which a "1" or a "0" can be stored; a quantum computer stores data using a quantum superposition of multiple states. These multiple valued states are stored in "quantum bits" or "qubits". This allows the computation of numbers to be several orders of magnitude faster than traditional transistor processors.

To comprehend the power of quantum computer, consider RSA-640, a number with 193 digits, which can be factored by eighty 2.2GHz computers over the span of 5 months, one quantum computer would factor in less than 17 seconds. Numbers that would typically take billions of years to compute could only take a matter of hours or even minutes with a fully developed quantum computer.

In view of these facts, modern cryptography will have to look for computationally harder problems or devise completely new techniques of archiving the goals presently served by modern cryptography.

Aims and objective of the project

Our objective to execute of this project is to learn and aquire deeper knowledge about cryptography because In our day-to-day lives, the use of cryptography is everywhere. For example, we use it to securely send passwords over vast networks for online purchases. Bank servers and e-mail clients save your passwords using cryptography as well. Cryptography is used to secure all transmitted information in our IoT-connected world, to authenticate people and devices, and devices to other devices.

If all of the cryptographic engines/functions stopped working for a day, modern life as we know it would stop. Bank transactions wouldn't go through, internet traffic would come to a halt, and cell phones would no longer function. At this point, all of our important information would be exposed, and it then could be exploited to do unimaginable harm to us all.

Cryptography is an essential way of preventing that from happening. It secures information and communications using a set of rules that allows only those intended—and no one else—to receive the information to access and process it.

CHALLENGES:

Challenges are everywhere so we have also faced a bit of challenge to complete this project . This project is given by our class techer after commencing our physical classes so we have to complete our day to day study and have to perform our practical task ,but side by side we continued our project work to meet the deadline of the project. And second most thing is cryptography is a huge subject and trending topic so it is not possible to cover all the aspects in one project book but we have tried our best from our teams end. Everyone wants to make their project innovative these days. But applying your innovation in your traditional project framework can get confusing. So it is important to discuss your project ideas and way of implementation with your team members first.

Whenever we face any problem to complete our project our team members aree always ready to resolve the problems effectively.

CONCLUSION

2020 was a transformative year ,a year of adaptability and tackling new challenges,all the payment or confidential work done by virtualy so cryptography is very important aspects for today. The cloud will play a bigger role, especially in financial services .

The movement toward broad acceptance of cloud-based encryption and key management will accelerate as more of the pieces come together. Organizations have become more aggressive with the cloud, especially financial services organizations that are moving toward payment processing in the cloud.

Cloud providers are offering more robust and flexible security to meet the demands of organizations who want to retain control of the keys and avoid being vendor locked. Cloud providers have been listening to enterprises about their concerns around data security practices and are making forward strides with data access, key management, and data retention policies.

so being a trainee of cloud computing and networking this project is very relevant and helpful to us to meet our future scope**.**

Bibliography

- **search?rlz=1C1RLNS_enIN913IN913&sxsrf=ALeKk01pq55CTDJCHSlA5GKNve14Ufohfw:1616688546589&q=final+year+projects+on+cryptography+and+network+s**
- **http://www.123seminarsonly.com/**

https://www.edureka.co/blog/what-is-cryptography/