**Module 20**

**Cryptography**

Cryptography means encrypting the data or information.

Encryption use algorithm of cipher and a secret value of key. Cipher is the method in which we write a letter in another form.

**Objective of Cryptography**

**Confidentiality** :- Confidentiality is the assurance that the information is accessible to authorize person .

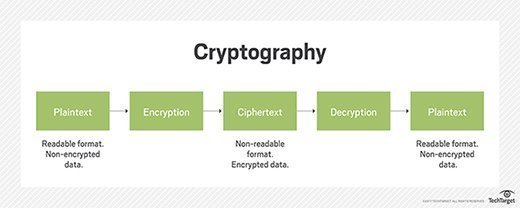
**Integrity** :- in this term, protect the data from deletion or modification by intruder .

After keeping the data confidential and integrity , than also data is useless unless it is not accessible , so here our third term come

**Availability** :- Data must be available to authorize user only

**Cryptography Process**

In this process plain text is encrypted than converted to the cipher than it sent. On reaching the destination is decrypted in the form of plain text with the help of key which is having both end.



**Encryption Algorithm**

**Algorithm-** step by step process through which plain text convert into encryption.

**Two general form of Cryptography-**

* **Substitution:-** In this process of encryption, bit are replaced by bits to encrypt the data.
* **Transposition:-** In this process bits doesn’t replace, it change the order of sequence. It use swapping method.

**Encryption Algorithm:-** Mathematical operation, methodology, formulas are used to encrypt or decrypt the data or information.

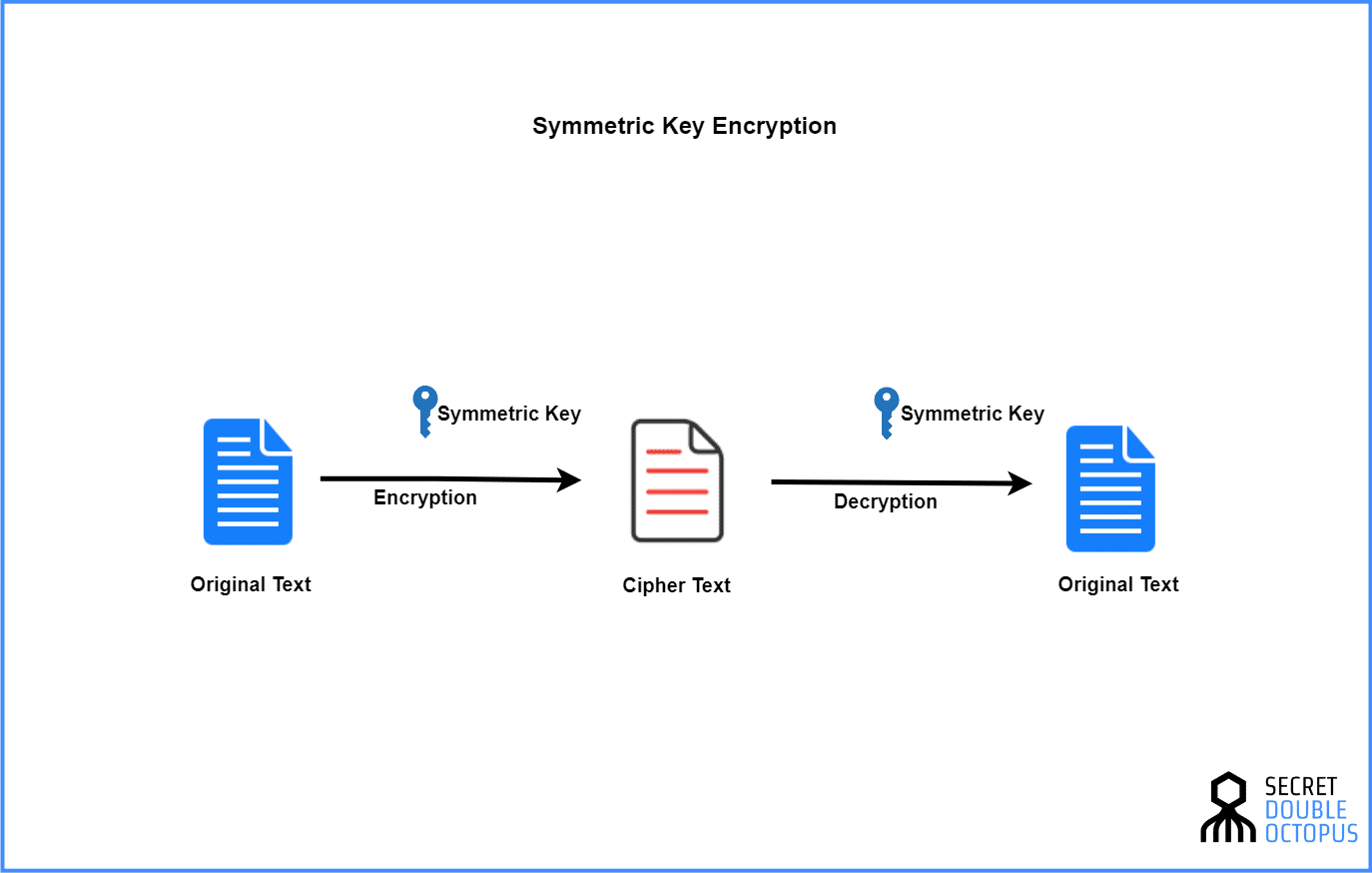
**What is cipher ?**

Cipher is an algorithm of encrypting or decrypting the sensitive data. It is used to convert plain text into specific pattern and reverse of this process is known as decipherment. Encrypted message has key, without this key it is hard to decrypt it.

**Steam cipher:-** In stream cipher one byte is encode at a time . It make key long so it is difficult to perform brute force attack.

**Block cipher:-** In block cipher all bits (128-bit) are encrypted at a time. It has draw back it is simple to analyze and slower than stream cipher.

**Three types of cryptographic techniques used in general*.***  
  
1. Symmetric-key cryptography  
2. Hash functions.  
3. Public-key cryptography  
  
**Symmetric-key Cryptography:** Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.



**TYPES of Symmetric-key cryptography**

**Data encryption standard**

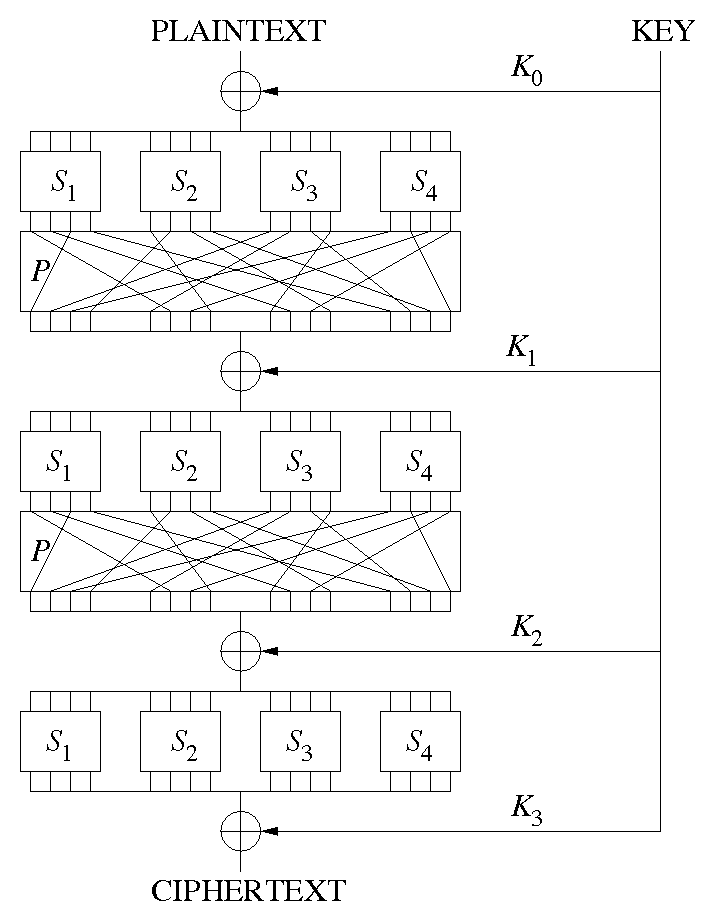
DES is adopted in 1977 for protecting sensitive data. DES is method of encryption in which it use 64 bit code encryption. It use 56 bit encryption for encrypting and 8 bit used for error checking. It design allow us to implement it on hardware and use it for single use.

It was outdated method of data encryption and officially retired in 2005.

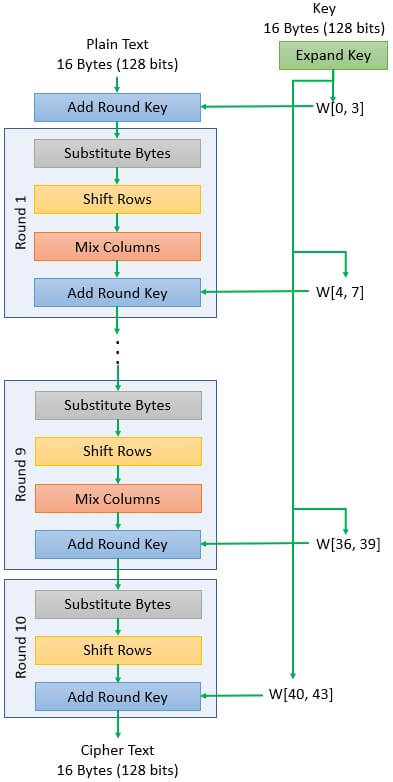
**3DES or TRIPLE DES**

It is upgraded version of DES. It provide high security of 112-bit security. It provide high security but it is not efficient because it is very slow in software. For 112- bit security it required 168 bits longer key which itself is highly encrypted that’s why it is slow, it take time in decryption.

**Advance Encryption System**  
AES is most used cipher in universe. NIST standardized AES in 2000 as a replacement of DES. It use 128 bit of encryption input and output of substitution-permutation.



Working of permutation here each step 4word of key is added(one word = 4 byte & 1 byte = 8 bit). Like this 10 round take place in AES.



**RC4( Rivest cipher 4)**

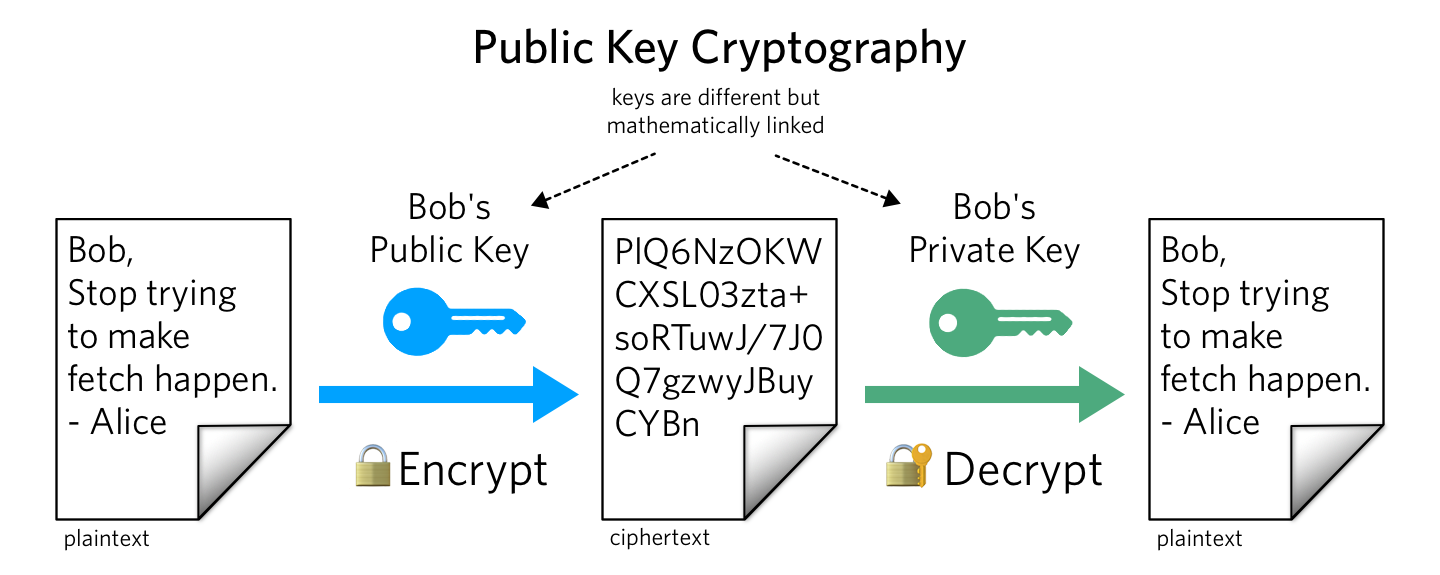
Rivest cipher is invented by Ron Rivest in 1987. It is one of the most used cipher because of its simplicity and speed of operation. It use either 64-bit or 128-bit key size while encrypting the data. It work in WEP, TLS etc.

RC4 cipher is secretly used for long time until Ron Rivest the RC4 algorithm in Wikipedia at 2014, where he describe history of RC4.

Ron Rivest work in RSA. RSA is a organization which help us to reduce the risk like fraud, threat detection, access management etc.

**Asymmetric-Key Cryptography**

This is the most revolutionary concept. In Public-Key Cryptography two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key, remains a secret. The public key is used for encryption and for decryption private key is used.

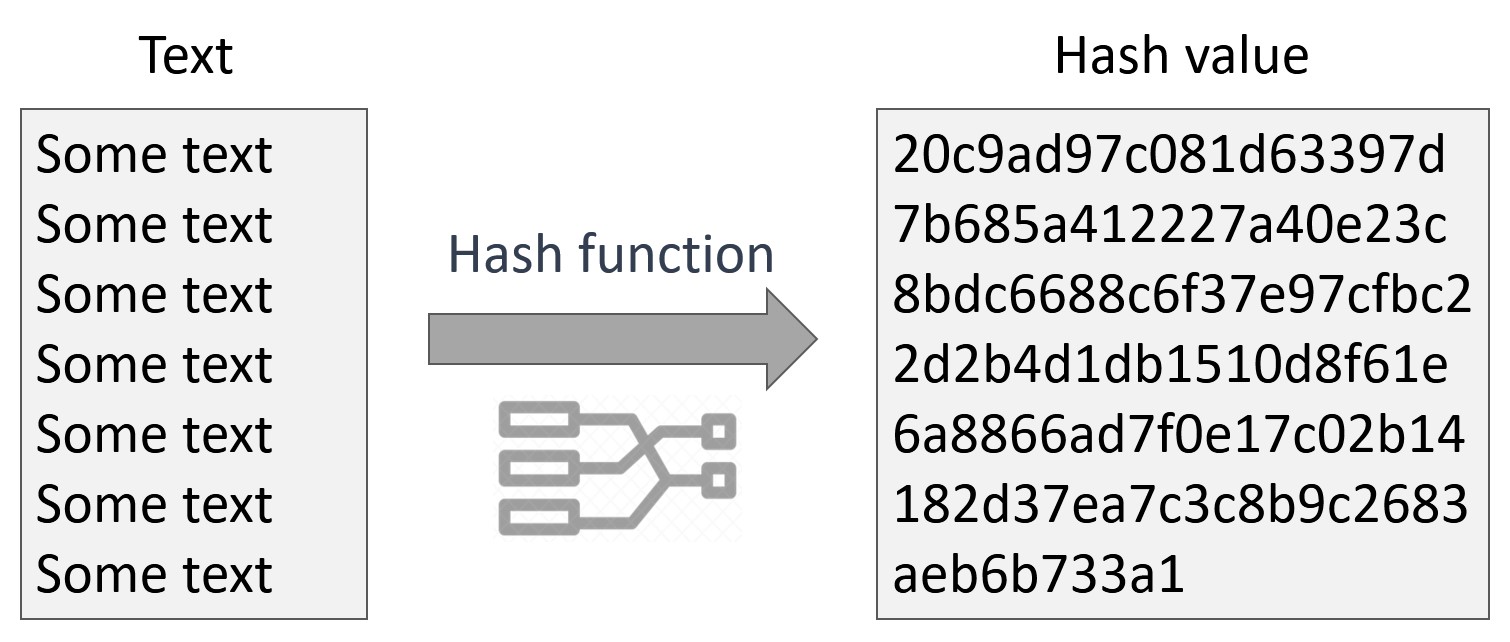
Example:- whats app, Facebook messenger, etc use this crypto graphy.  


**Hash Functions**

No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.

As encryption hash cannot be reverted its original position, even with unlimited computing value hash cannot be revert into its original value.

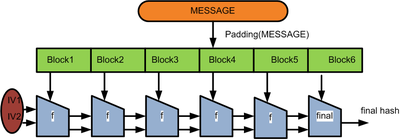
After creating hash it act as a check sum. This means it check the value with the created hash whether the input value is correct or not.



**Merkel-Damgard construction**

Hash Function is introduce in 1980 and production goes to 2010 on the basis of Merkle-Damgard(M-D) construction: MD4, MD5, SHA-1, SHA-2 Family.

M-D construction split the message into identical block and size. In internal mixes these block using compression function.

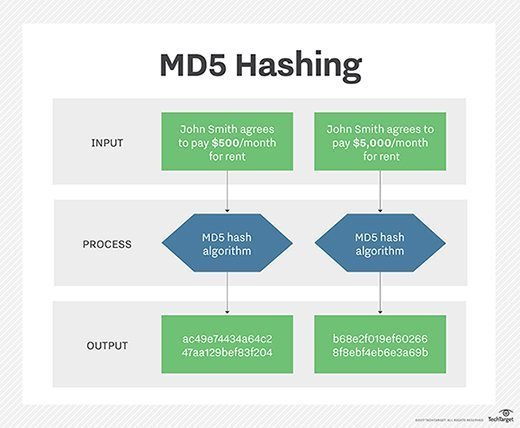


**The Devies-Mayer Construction**

In this construction, real hash are compressed such as SHA-256, which are based on block cipher.

**Type of hashing**

**MD5** - An MD5 hash function encodes a string of information and encodes it into a 128-bit fingerprint. It is used for data verification in transmission protocol. It’s one of the most widely used algorithms in the world.



**SHA1** – It stand for Secure Hash Algorithm. It is developed by the National Security Agency (NSA), is a cryptographic hash function. Results from SHA1 are expressed as a 160-bit hexadecimal number. This hash function is widely considered the successor to MD5.

SHA1 use merkle-Damgard function for splitting the value into identical block and size than it use devise-mayer function to compressed the hash together.

**SHA2**- It is a successor of SHA1 and designed by NSA.

Goal was to make the SHA2 to enhance the security and generate longer hash.

It is a cryptographical hash function. Cryptographical hash function is a mathematical algorithm, it is very quick to compute hash value for any message. SHA2 family consist of six hash function **SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256.**

MD5 Hash: FC3FF98E8C6A0D3087D515C0473F8677

SHA-1 Hash: 430CE34D020724ED75A196DFC2AD67C77772D169

SHA256 Hash: 7509E5BDA0C762D2BAC7F90D758B5B2263FA01CCBC542AB5E3DF163BE08E6CA9

**CRC32** – A cyclic redundancy check (CRC) is an error-detecting code often used for detection of accidental changes to data. Encoding the same data string using CRC32 will always result in the same hash output, thus CRC32 is sometimes used as a hash algorithm for file integrity checks.