Confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

Data Integrity: Assures ~~that a~~ that information and programs are changed only in a specified & authorized manner.

System Integrity :- Assures that system performs its intended function in an unimpaired manner, free from deliberate or inaadvertent unauthorized manipulation of system

Availability :- Assures that system work promptly & service is not denied to authorized users

Authentication :- The assurance that the communicating entity is the one that it claims to be

A passive attact attempts to learn or make use of information from the system but doesnt effect system resources'

An active attact attempts to alter system resources or affect their operation.

Sub Cipher

Caeser Cipher :- Involves replacing each letter of the alphabet with the letter standing 3 places further down the alphable

meet ⇒ PHHW ⇒ m+3

No of keys possible available keys = 25

Monoalphabetic Cipher:- Replace each letter with one of 26 letters. So one letter can be encrypted with 26 letters

No of keys = 26! or 4×10^{26}

PLAY FAIR : Best known multiple letter encrypton cipher - Treates Di-grams in plaintext as single units and translates those units into cipher text di-grams.

Possible keys 25!

Vigenere Cipher:- Polyalphabetic cipher — best
In this scheme the set of related mono alphabetic sub-rules consists of 26 Caeser ciphers with shifts of 0 through 25
Each cipher is denoted by a key letter which is the cipher text letter that substitutes for plain text letter a

key DeC
PT WEA

Cipher ⇒ D=3 W=22 Cipher ⇒ 22+3 = 25 = Z
E=4 E=4 ciphr = 4+4 = 8 = I
C=2 A=0 CP' = 0+2 = C

Brute Force = InVolves trying every possible keys until an intelligible translation of cipher text into plain text is obotained

Cryptanalyses : Techniques used for de-ciphering a message with out any knowlede of en-crypting Attack relies on nature of algorithm and some knowledge of general charactiristics of plain text

MONO	POLY
one letter is mapped to unique alphabet	One letter mapped to m alphabets of a cipher text
one to one	one to many
stream	
Caeser Monoalphabetic	playfair, Vigeneae.

Substitution	Transposition
It is easy	It is hard.
A sub techique is one in which PT letters are replaced with other letter	~~A~~ In the position of letters are changed with one another

ONE TIME PAD

Use a random key that is as long as the message so that the key need not be repeated

Key is used to encrypt and decrypt a single message & then it is discarded. Each new message requires a new key of the same length as the new message.

Scheme is very unbreakable.

-> produces random output that bears no statistical relationship to the plaintext

-> Because the cipher text contains no information whatsoever about the plain text there is simply no way to break code.

Difficulties-

There is a practical problem of making large quantities of random key

Any heavily used system might require millions of random characteristics on a regular basis.

Mammoth key key distribution problem

message length = key length