Semester : 1   Subject : CSS   Academic Year: 20 23- 2024 .

MECHANISMS OF SECURITY :

The different mechanisms of Security are:

* Encipherment
* One Way Hashing
* Firewall
* Intrusion Detection System
* Access Control list
* Digital Signature

Encipherment :-

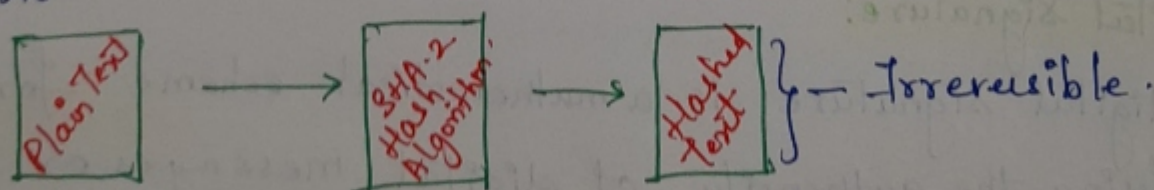The application of mathetical algorithms to transform data into a form that is difficult to understand. An algorithm or more encryption keys are used to convert the data and then recover it.

There are two types:

* Symmetric (or) Private (or) Secret key Cryptography.
* Asymmetric (or) Public Key Cryptography.

One Way Hash Function :

A fixed length output string is generated from a variable length input in which the reverse of a function is almost impossible.


Plain Text → SHA-2 Hash Algorithm → Hashed Text } — Irreversible.

PARSHWANATH CHARITABLE TRUST'S
A.P. SHAH INSTITUTE OF TECHNOLOGY
Department of Computer Science and Engineering
Data Science

CSE DATA SCIENCE

Semester : 1

Subject : CSS

Academic Year: 2023-2024

Firewall :-

Firewall is a software or firmware that enforces a set of rules about what data packets will be allowed to enter or leave a network. It uses 3 rules :
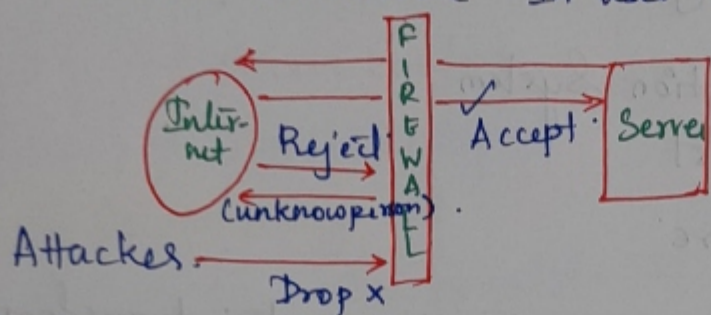
IDS : Intrusion Detection System

IDS is a type of security software designed to automatically alert administrators when someone or something is trying to compromise information through malicious activities.

Access Control List :-

Access control list refers to permissions attached to an object that specify which users are granted access to that object and its operation it is ~~called~~ allowed to perform.

Digital Signature:

A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents.