**ASSIGNMENT 04**

**Hash Function:**

A hash function takes a group of characters (called a key) and maps it to a value of a certain length (called a hash value or hash). The hash value is representative of the original string of characters, but is normally smaller than the original.

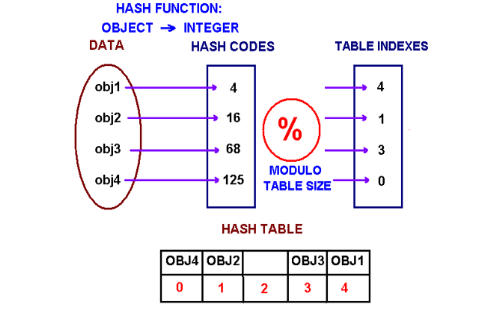
Hashing is done for indexing and locating items in databases because it is easier to find the shorter hash value than the longer string. Hashing is also used in encryption.

A function is basically something that takes an input and from that input derives an output.

undefined

A hash function is therefore something that takes an input (which can be any data - numbers, files, etc) and outputs a hash. A hash is usually displayed as a hexadecimal number.

undefined



Basic Use of Hash Function:

Hashing is a technique that is used to uniquely identify a specific object from a group of similar objects. Some examples of how hashing is used in our lives include:

* In universities, each student is assigned a unique roll number that can be used to retrieve information about them.
* In libraries, each book is assigned a unique number that can be used to determine information about the book, such as its exact position in the library or the users it has been issued to etc.

**Firewall:**

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

**Types of Firewalls:**

### **Proxy firewall**

An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.

### **Stateful inspection firewall**

Now thought of as a “traditional” firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

### **Unified threat management (UTM) firewall**

A UTM device typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and [antivirus](https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/best-antivirus-strategy.html). It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use.

**Data Encryption Standard:**

The Data Encryption Standard, usually referred to by the [acronym](https://www.sciencedirect.com/topics/engineering/acronyms" \o "Learn more about Acronyms from ScienceDirect's AI-generated Topic Pages)DES, is a well-established [encryption](https://www.sciencedirect.com/topics/engineering/cryptography) [algorithm](https://www.sciencedirect.com/topics/engineering/algorithm) which was first standardized by NIST in the 1980s. **Data encryption standard (DES)** has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on decline.

DES is a block cipher, and encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences.

# **SSL (Secure Sockets Layer)**

Secure Sockets Layer (SSL) is a networking [protocol](https://searchnetworking.techtarget.com/definition/protocol) designed for securing connections between web [clients](https://searchenterprisedesktop.techtarget.com/definition/client) and web [servers](https://whatis.techtarget.com/definition/server) over an insecure network, such as the [internet](https://searchwindevelopment.techtarget.com/definition/Internet). SSL uses a combination of [public key encryption](https://searchsecurity.techtarget.com/definition/asymmetric-cryptography) and [private key encryption](https://searchsecurity.techtarget.com/definition/secret-key-algorithm) and other cryptographic functions to secure a connection between two machines, typically a web server or [mail server](https://searchmicroservices.techtarget.com/definition/mail-server-mail-transfer-transport-agent-MTA-mail-router-Internet-mailer) and a client system, communicating over the internet or another [TCP/IP](https://searchnetworking.techtarget.com/definition/TCP-IP)network.

SSL runs above the transport layer and the [network layer](https://searchnetworking.techtarget.com/definition/Network-layer), which are responsible for the transport of data between processes and the routing of network traffic over a network between client and server, respectively, and below [application layer](https://searchnetworking.techtarget.com/definition/Application-layer) protocols, such as HTTP and the Simple Mail Transport Protocol ([SMTP](https://whatis.techtarget.com/definition/SMTP-Simple-Mail-Transfer-Protocol)).