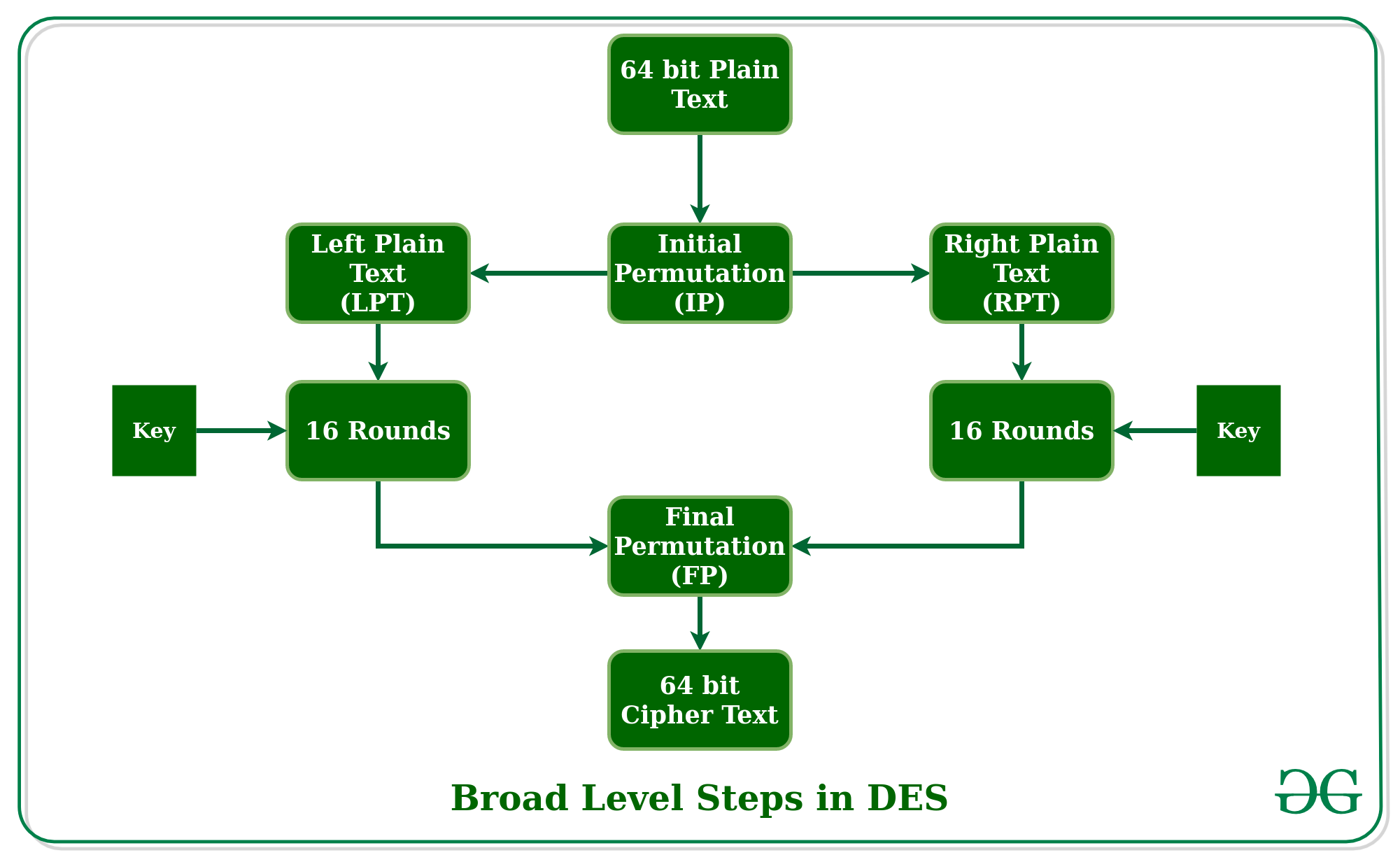
DES is based on the two fundamental attributes of [cryptography](https://www.geeksforgeeks.org/cryptography-and-its-types/): substitution (also called confusion) and transposition (also called diffusion). DES consists of 16 steps, each of which is called a round. Each round performs the steps of substitution and transposition. Let us now discuss the broad-level steps in DES.

* In the first step, the 64-bit plain text block is handed over to an initial [Permutation](https://www.geeksforgeeks.org/permutation/) (IP) function.
* The initial permutation is performed on plain text.
* Next, the initial permutation (IP) produces two halves of the permuted block; saying Left Plain Text (LPT) and Right Plain Text (RPT).
* Now each LPT and RPT go through 16 rounds of the encryption process.
* In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block
* The result of this process produces 64-bit ciphertext.

****

**What is SSL?**

SSL, or Secure Sockets Layer, is an [encryption](https://www.cloudflare.com/learning/ssl/what-is-encryption/)-based Internet security [protocol](https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/). It was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern [TLS](https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/) encryption used today.

A website that implements SSL/TLS has "[HTTPS](https://www.cloudflare.com/learning/ssl/what-is-https/)" in its URL instead of "[HTTP](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/)."

**How does SSL/TLS work?**

* In order to provide a high degree of [privacy](https://www.cloudflare.com/learning/privacy/what-is-data-privacy/), SSL encrypts data that is transmitted across the web. This means that anyone who tries to intercept this data will only see a garbled mix of characters that is nearly impossible to decrypt.
* SSL initiates an **authentication** process called a [handshake](https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/) between two communicating devices to ensure that both devices are really who they claim to be.
* SSL also digitally signs data in order to provide **data integrity**, verifying that the data is not tampered with before reaching its intended recipient.

## Why is SSL/TLS important?

Originally, data on the Web was transmitted in plaintext that anyone could read if they intercepted the message. For example, if a consumer visited a shopping website, placed an order, and entered their credit card number on the website, that credit card number would travel across the Internet unconcealed.

SSL was created to correct this problem and protect user privacy. By encrypting any data that goes between a user and a web server, SSL ensures that anyone who intercepts the data can only see a scrambled mess of characters. The consumer's credit card number is now safe, only visible to the shopping website where they entered it.

SSL also stops certain kinds of cyber attacks: It authenticates web servers, which is important because attackers will often try to set up fake websites to trick users and steal data. It also prevents attackers from tampering with data in transit, like a tamper-proof seal on a medicine container.

**Are SSL and TLS the same thing?**

SSL is the direct predecessor of another protocol called TLS (Transport Layer Security). In 1999 the Internet Engineering Task Force (IETF) proposed an update to SSL. Since this update was being developed by the IETF and Netscape was no longer involved, the name was changed to TLS. The differences between the final version of SSL (3.0) and the first version of TLS are not drastic; the name change was applied to signify the change in ownership.

Since they are so closely related, the two terms are often used interchangeably and confused. Some people still use SSL to refer to TLS, others use the term "SSL/TLS encryption" because SSL still has so much name recognition.

**Is SSL still up to date?**

SSL has not been updated since SSL 3.0 in 1996 and is now considered to be deprecated. There are several known vulnerabilities in the SSL protocol, and security experts recommend discontinuing its use. In fact, most modern web browsers no longer support SSL at all.

TLS is the up-to-date encryption protocol that is still being implemented online, even though many people still refer to it as "SSL encryption." This can be a source of confusion for someone shopping for security solutions. The truth is that any vendor offering "SSL" these days is almost certainly providing TLS protection, which has been an industry standard for over 20 years. But since many folks are still searching for "SSL protection," the term is still featured prominently on many product pages.

**What is an SSL certificate?**

SSL can only be implemented by websites that have an [SSL certificate](https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/) (technically a "TLS certificate"). An SSL certificate is like an ID card or a badge that proves someone is who they say they are. SSL certificates are stored and displayed on the Web by a website's or application's server.

One of the most important pieces of information in an SSL certificate is the website's public [key](https://www.cloudflare.com/learning/ssl/what-is-a-cryptographic-key/). The [public key](https://www.cloudflare.com/learning/ssl/how-does-public-key-encryption-work/) makes encryption and authentication possible. A user's device views the public key and uses it to establish secure encryption keys with the web server. Meanwhile the web server also has a private key that is kept secret; the private key decrypts data encrypted with the public key.

Certificate authorities (CA) are responsible for issuing SSL certificates.

**What are the types of SSL certificates?**

There are several different [types of SSL certificates](https://www.cloudflare.com/learning/ssl/types-of-ssl-certificates/). One certificate can apply to a single website or several websites, depending on the type:

* **Single-domain:** A single-domain SSL certificate applies to only one domain (a "domain" is the name of a website, like www.cloudflare.com).
* **Wildcard:** Like a single-domain certificate, a wildcard SSL certificate applies to only one domain. However, it also includes that domain's subdomains. For example, a wildcard certificate could cover www.cloudflare.com, blog.cloudflare.com, and developers.cloudflare.com, while a single-domain certificate could only cover the first.
* **Multi-domain:** As the name indicates, multi-domain SSL certificates can apply to multiple unrelated domains.

SSL certificates also come with different validation levels. A validation level is like a background check, and the level changes depending on the thoroughness of the check.

* **Domain Validation:** This is the least-stringent level of validation, and the cheapest. All a business has to do is prove they control the domain.
* **Organization Validation:** This is a more hands-on process: The CA directly contacts the person or business requesting the certificate. These certificates are more trustworthy for users.
* **Extended Validation:** This requires a full background check of an organization before the SSL certificate can be issued.

**How can a business obtain an SSL certificate?**

Cloudflare offers [free SSL certificates](https://www.cloudflare.com/application-services/products/ssl/) for any business. A website protected by Cloudflare can activate SSL with a few clicks. Websites may need to set up an SSL certificate on their [origin server](https://www.cloudflare.com/learning/cdn/glossary/origin-server/) as well: [this article](https://support.cloudflare.com/hc/en-us/articles/360024787372-How-do-I-add-SSL-to-my-site-) has further instructions.

**What is SSL/TLS Encryption?**

**TLDR: SSL/TLS encrypts communications between a client and server, primarily web browsers and web sites/applications.**

SSL (Secure Sockets Layer) encryption, and its more modern and secure replacement, TLS (Transport Layer Security) encryption, protect data sent over the internet or a computer network. This prevents attackers (and Internet Service Providers) from viewing or tampering with data exchanged between two nodes—typically a user’s web browser and a web/app server. Most website owners and operators have an obligation to implement SSL/TLS to protect the exchange of sensitive data such as passwords, payment information, and other personal information considered private.

**How Does SSL/TLS Encryption Work?**

SSL/TLS uses both asymmetric and symmetric encryption to protect the confidentiality and integrity of data-in-transit. Asymmetric encryption is used to establish a secure session between a client and a server, and symmetric encryption is used to exchange data within the secured session.

A website must have an SSL/TLS certificate for their web server/domain name to use SSL/TLS encryption. Once installed, the certificate enables the client and server to securely negotiate the level of encryption in the following steps:

1. The client contacts the server using a secure URL (HTTPS…).
2. The server sends the client its certificate and public key.
3. The client verifies this with a Trusted Root Certification Authority to ensure the certificate is legitimate.
4. The client and server negotiate the strongest type of encryption that each can support.
5. The client encrypts a session (secret) key with the server’s public key, and sends it back to the server.
6. The server decrypts the client communication with its private key, and the session is established.
7. The session key (symmetric encryption) is now used to encrypt and decrypt data transmitted between the client and server.

Both the client and server are now using HTTPS (SSL/TLS + HTTP) for their communication. Web browsers validate this with a lock icon in the browser address bar. HTTPS functions over Port 443.

Once you leave the website, those keys are discarded. On your next visit, a new handshake is negotiated, and a new set of keys are generated.