

UNIVERSIDAD DEL ISTMO

FACULTAD DE INGENIERÍA

INFORME ALGORITMO DES

SISTEMAS OPERATIVOS

 KEVIN ALEXANDER CHAMPNEY LEÓN

ELISA MARGARITA MONZÓN GODOY

Guatemala, 24 de septiembre de 2019

ÍNDICE

[INTRODUCCIÓN 1](#_Toc20066452)

[CONTENIDO 2](#_Toc20066453)

[Descripción de Algoritmo DES 2](#_Toc20066454)

[Principio de funcionamiento 2](#_Toc20066455)

[Diagrama de flujo 3](#_Toc20066456)

[Lógica descriptiva 4](#_Toc20066457)

[Código descriptivo 4](#_Toc20066458)

[Rondas de Feistel 4](#_Toc20066459)

[Variables mutex y condicionales 4](#_Toc20066460)

[Catálogo de funciones principales de programa 4](#_Toc20066461)

[CONCLUSIONES 5](#_Toc20066462)

[BIBLIOGRAFÍA 6](#_Toc20066463)

# INTRODUCCIÓN

# CONTENIDO

## Descripción de Algoritmo DES

DES, Data Encryption Estándar[[1]](#footnote-1), es un esquema de encriptación simétrico, desarrollado en 1977 por el Departamento de Comercio y la Oficina Nacional de Estándares de Estados Unidos, en colaboración con la empresa IBM. Fue creado con el objeto de proporcionar al público en general un algoritmo de cifrado normalizado para las redes de ordenadores, que contara con los siguientes requisitos:

* Ofrecer un alto nivel de seguridad relacionado con una pequeña clave utilizada para cifrado y descifrado
* Comprensible
* No depender de la confidencialidad del algoritmo
* Adaptativo y económico
* Eficaz y exportable

El algoritmo se basa en un sistema mono alfabético, con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones. Inicialmente el texto en claro a cifrar se somete a una permutación, con un bloque de entrada de 64 bits, para posteriormente ser sometido a la acción de dos funciones principales, una función de permutación con entrada de 8 bits y otra de sustitución con entrada de 5 bits, en un proceso que consta de 16 etapas de cifrado.

## Principio de funcionamiento

Se trata de un sistema de cifrado simétrico por bloques de 64 bits, de los que 8 bits se utilizan como control de paridad (para la verificación de la integridad de la clave). Cada uno de los bits de la clave de paridad se utiliza para controlar uno de los bytes de la clave por paridad impar, es decir, que cada uno de los bits de paridad se ajusta para que tenga un número impar dentro del byte al que pertenece. Por lo tanto, la clave tiene una longitud útil de 56 bites.

El algoritmo se encarga de realizar combinaciones, sustituciones y permutaciones entre el texto a cifrar y la clave, asegurándose al mismo tiempo de que las operaciones puedan realizarse en ambas direcciones (para el descifrado). La combinación entre sustituciones y permutaciones se llama cifrado del producto.

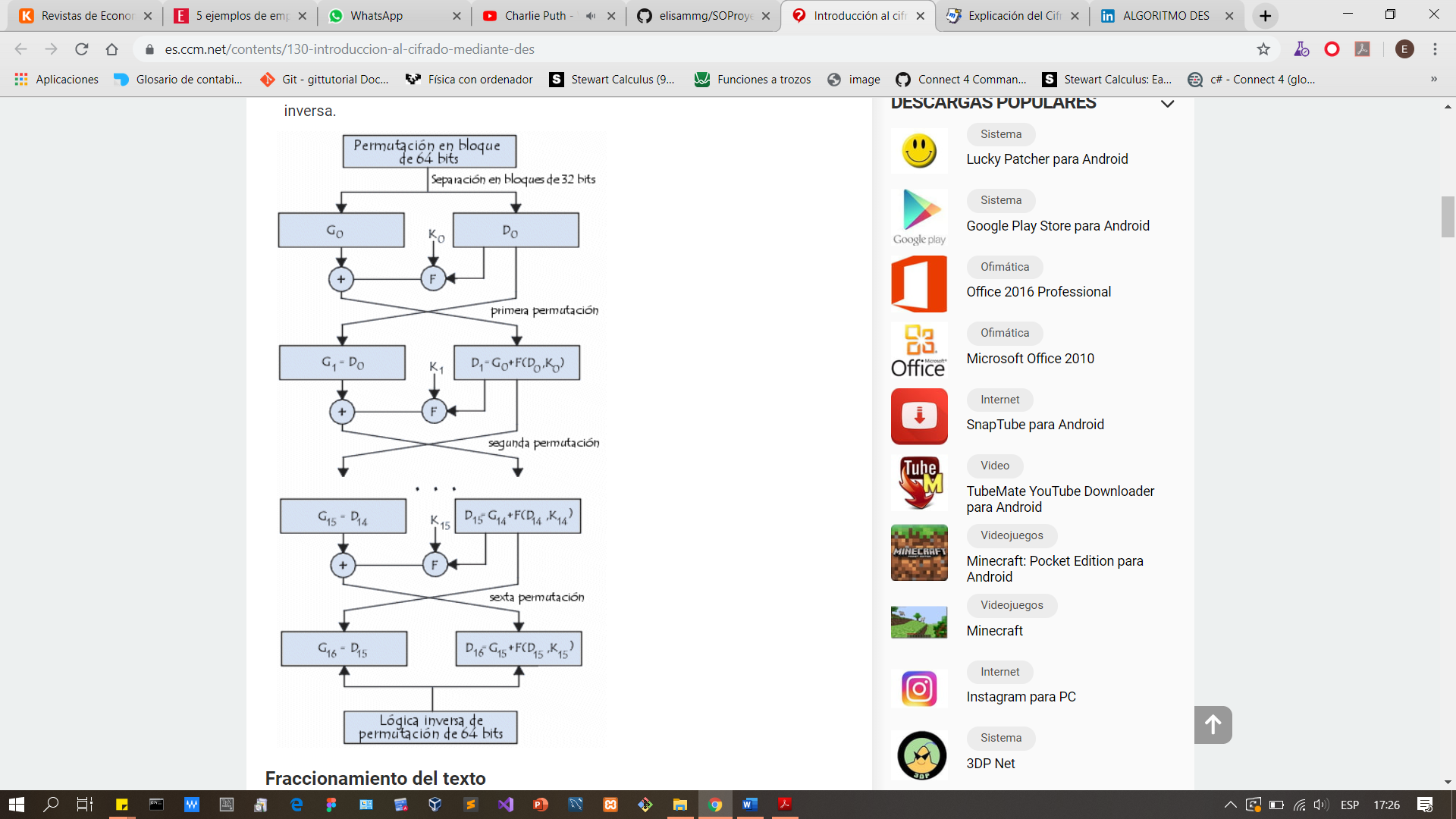
La clave es codificada en 64 bits y se compone de 16 bloques de 4 bits, generalmente anotadas de *k1* a *k16*. Dado que "solamente" 56 bits sirven para el cifrado, ¡puede haber hasta 256 (o 7.2\*1016) claves diferentes

## Diagrama de flujo

Las partes principales del algoritmo constan de:

* Fraccionamiento del texto en bloques de 64 bits
* Permutación inicial de los bloques
* Partición de los bloques en dos partes:
  + Izquierda 🡪 I
  + Derecha 🡪 D
* Fases de permutación y de sustitución repetidas 16 veces (rondas)
* Reconexión de las partes izquierda y derecha, seguida de la permutación inicial inversa.

Imagen No.1: Diagrama algoritmo DES



Fuente: CCM, 2019.

## Lógica descriptiva

<http://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm>

## Código descriptivo

<https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/>

## Rondas de Feistel

## Variables mutex y condicionales

## Catálogo de funciones principales de programa

# CONCLUSIONES

# BIBLIOGRAFÍA

<http://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/des.html>

<https://es.ccm.net/contents/130-introduccion-al-cifrado-mediante-des>

1. En castellano: Algoritmo de Cifrado de Datos [↑](#footnote-ref-1)