

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO FACULTAD DE INGENIERÍA

Criptografía

Practica #4

MD2

Elaborada por: : Carvente Velasco Carlos Alberto

Miramontes Sarabia Luis Enrique

Grupo: 2

Semestre: 2020-1

Fecha de entrega: 16 de Septiembre del 2019



Práctica 4

Práctica 4 MD2

Objetivo

- 1. Utilizando la descripción proporcionada y el pseudocódigo, en los equipos se discute cómo se debe implementar este algoritmo, cuál sería el mejor lenguaje de programación para hacerlo y crear un borrador de dicho código.
- 2.Haga su presentación individual en Alphagrader su implementación MD2 en el lenguaje de programación que elija. Los casos de prueba son los que se presentan en la tabla anterior.

Desarrollo

1. Después de platicar sobre el algoritmo y sus requerimientos el equipo decidió utilizar Python para implementarlo, a continuación se hablará del porqué de nuestra decisión.

Python ya incluye métodos específicos para tratar con binarios y conversiones a hexadecimal, en éste caso pensamos que la implementación se podría facilitar mucho usando los métodos format() y list().

Format() pasa de un entero a una representación binaria (ya sea en binario o hexadecimal) del número proporcionado. En este caso planeamos usarlo para las salidas, transformando los valores que usemos a través de todo el código en hexadecimal, que se piensa utilizar en la función **Hash**.

List() Lo importante de este método es que los elementos de una lista no necesitan ser del mismo tipo. Este método puede ser de gran ayuda a la hora de convertir una string a una lista de bytes que en el algoritmo es de suma utilidad a la hora del manejo de bytes.

A la hora de combinar estos dos métodos que Python nos ofrece podemos convertir una lista con bytes a un string en formato hexadecimal.

Las razones listadas anteriormente, la facilidad del lenguaje y nuestra experiencia programando en programando el Python hacen de éste nuestra mejor opción.