密碼工程Quiz2

學號:112550090 姓名:曾士珍

Problem1

程式碼按執行即可

a) 用python內建的sha1解密函式解密

一張含有 文字, 螢幕擷取畫面, 字型, 行 的圖片

自動產生的描述

b) 用python內建的sha1解密函式解密

一張含有 文字, 螢幕擷取畫面, 字型, 行 的圖片

自動產生的描述

c) 用python內建的sha1解密出前半部的密碼，在枚舉後半部的密碼，合起來在用python內建的sha1解密函式解密

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述

d)將password檔案顛倒(想從文件檔最後面開始試)並複製兩份分別為dict1及dict2，將dict2中的每個字串前都加一個空格，再利用hashcat跑出答案

指令：hashcat -m 100 -a 1 ${hash} dict1.txt dict2.txt

一張含有 文字, 螢幕擷取畫面, 字型, 黑與白 的圖片

自動產生的描述

Problem2

a)程式碼按執行即可，以下為output

一張含有 文字, 字型, 螢幕擷取畫面, 印刷術 的圖片

自動產生的描述

b)由上圖可以看出最快的是sha1

c)由快到慢排序依序是：

sha1 md5 sha512 sha224 sha256 sha3\_224 sha3\_256 sha3\_512

Problem3

有98個字母，先用程式過不同組合的difference，由拆的行數跟列數來看，最有可能的拆法是14\*7跟7\*14，由下圖difference的平均可以看出14\*7比7\*14好

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述

嘗試拆成14\*7依照英文字母的拼法觀察每行的排序順序

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| U | H | S | E | T | E | Q |
| O | I | W | F | T | O | N |
| N | G | P | D | A | E | A |
| C | I | N | O | R | C | E |
| S | R | I | W | T | O | L |
| V | I | T | E | L | H | A |
| A | B | E | C | O | E | F |
| I | I | T | X | D | N | S |
| H | E | I | T | Y | I | G |
| G | C | E | R | F | O | N |
| E | S | N | S | S | D | O |
| P | T | O | R | O | A | P |
| A | E | I | X | V | A | T |
| A | C | E | S | N | R | E |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |

重排後如下：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| T | H | E | Q | U | E | S |
| T | I | O | N | O | F | W |
| A | G | E | A | N | D | P |
| R | I | C | E | C | O | N |
| T | R | O | L | S | W | I |
| L | L | H | A | V | E | T |
| O | B | E | F | A | C | E |
| D | I | N | S | I | X | T |
| Y | E | I | G | H | T | I |
| F | C | O | N | G | R | E |
| S | S | D | O | E | S | N |
| O | T | A | P | P | R | O |
| V | E | A | T | A | X | I |
| N | C | R | E | A | S | E |
| 5 | 2 | 6 | 7 | 1 | 4 | 3 |

解得Key為：5267143

明文如下：

THE QUESTION OF WAGE AND PRICE CONTROLS WILL HAVE TO BE FACED IN SIXTY EIGHT IF CONGRESS DOES NOT APPROVE A TAX INCREASE