Proyecto CLCript
Cuadernos de Laboratorio de Criptografía. Entrega nº 3. Ultima actualización 06/05/19
Autor: Dr. Jorge Ramió Aguirre (@criptored)
Prácticas con el algoritmo de Vigenère: cifrado, descifrado y criptoanálisis

- Software Criptoclásicos v2.1: http://www.criptored.upm.es/software/sw_m001c.htm
- Lectura de interés: http://www.criptored.upm.es/crypt4you/temas/criptografiaclasica/leccion9.html

Objetivos:

1. Comprobar cómo se cifra y se descifra con el algoritmo por sustitución polialfabética de Vigenère en mod 27 y mod 191.
2. Realizar un criptoanálisis a la cifra de Vigenère mediante el método de Kasiski y comprobar los pasos que éste realiza.

I. Vigenère: cifrado y descifrado

Ejercicio 1)

1.1. Con el software Criptoclásicos v2.1 abre el Criptosistema Vigenère y en la ventana de Entrada pega este texto:

Me gustas cuando callas porque estás como ausente,
y me oyes desde lejos, y mi voz no te toca.
Parece que los ojos se te hubieran volado
y parece que un beso te cerrara la boca.
Como todas las cosas están llenas de mi alma,
emerges de las cosas, llena del alma mía.
Mariposa de sueño, te pareces a mi alma,
y te pareces a la palabra melancolía.

1.2. Haz clic en Clave e introduce la palabra PABLO. A continuación haz clic en la opción Cifrar y observa el criptograma en la ventana Salida.

1.3. Abre el informe que genera el programa y observa las operaciones de cifrado hechas.

1.4. Selecciona todo el texto cifrado de la ventana de Salida (doble clic) y cópialo en la ventana de Entrada. Hecho esto, haz clic en la opción Descifrar y observa el texto en claro en la ventana de Salida.

1.5. ¿Por qué sólo ves letras mayúsculas, no hay espacios ni signos de puntuación?

1.6. Cierra la ventana de Vigenère. Ahora en Opciones selecciona ASCII 191. Abre otra vez Vigenère y vuelve a cifrar el texto anterior con la misma clave. Observa el criptograma.

1.7. ¿Se podría hacer en este nuevo escenario un ataque por estadísticas o redundancia del lenguaje?

1.8. Puedes ver ese conjunto de 191 caracteres ASCII imprimibles desde Herramientas – Estadísticas del lenguaje – Tablas de caracteres – Tabla ASCII (191 caracteres). Observa que no se ha tenido en cuenta el espacio en blanco.

1.9. Cierra la ventana de Vigenère. En Opciones selecciona nuevamente Español Z27.

1.10. Abre Vigenère e introduce el siguiente criptograma en la ventana de Entrada:
BDVKQURUXALUHNJEDKÑBLHSRCWZDKMZTNHOVQBPKCFNAJDDOORCÑNRQUICOIHQK
BNWQOVONVMAORAYILZQVACSAFJDVZNORZNNIKGZODXVSXALWJOSXYMMXOKKTCSZ
DSIZTNNSCABVMZNYEÑRSQTDRSOOFZSWEXDJIDUWQZLHDXVICRWSRSSEREUHELZGZHZ
RDJEELKHLHZRNWXVWXOX

1.10 Descífralo con la clave GOLONDRINAS y observa el texto descifrado.

1.11 Usa los archivos de prueba que entrega el programa Criptoclásicos v2.1 y que verás en la pestaña Fichero para cifrado, para realizar un cifrado y un descifrado con textos distintos.

Comprueba tu trabajo:

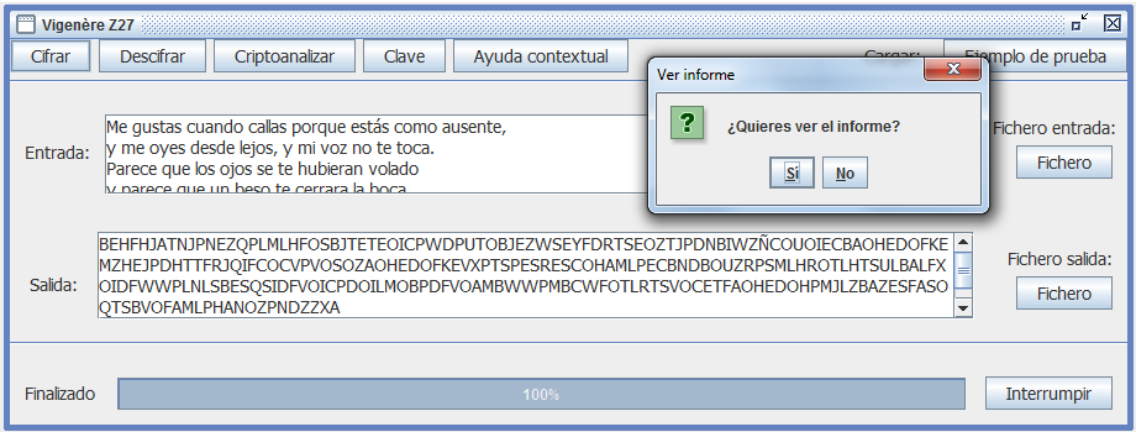

Figura 1. Operación cifrado de Vigenère mod 27.

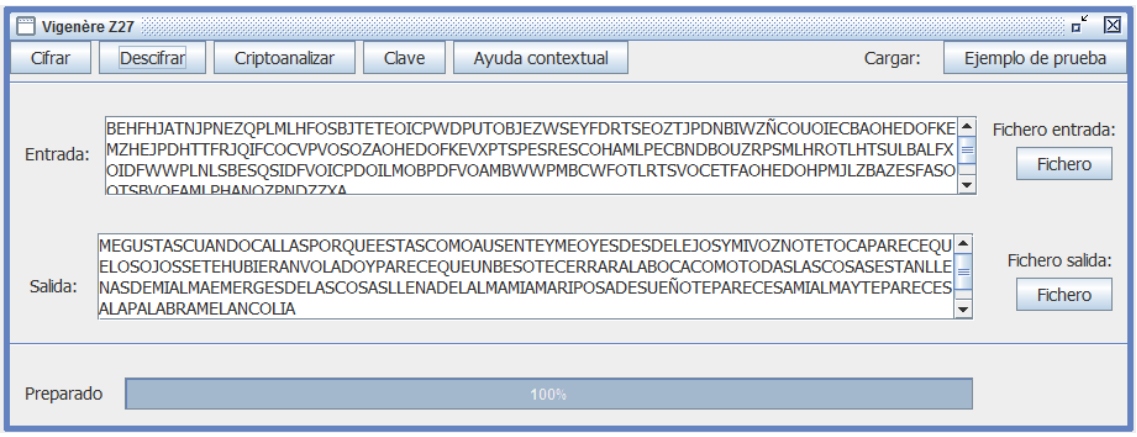

Figura 2. Operación descifrado de Vigenère mod 27.

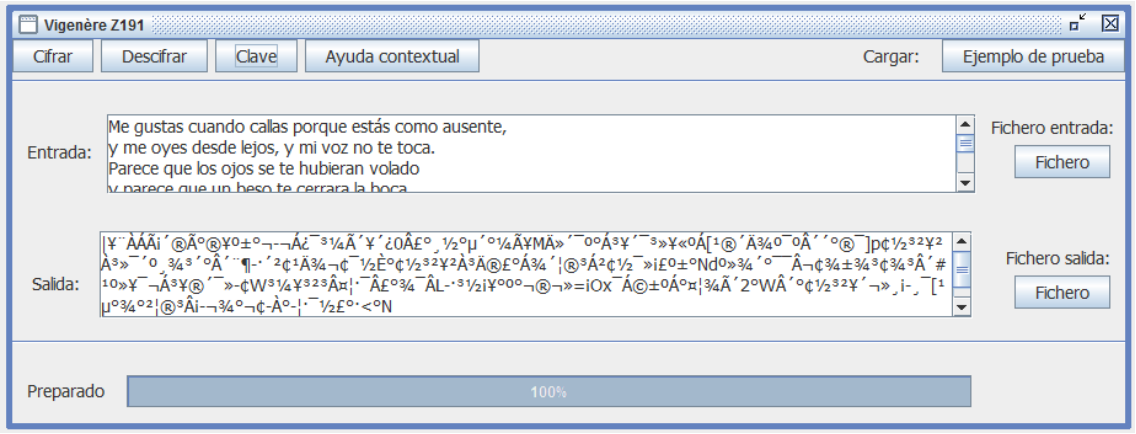

Figura 3. Operación cifrado de Vigenère mod 191.

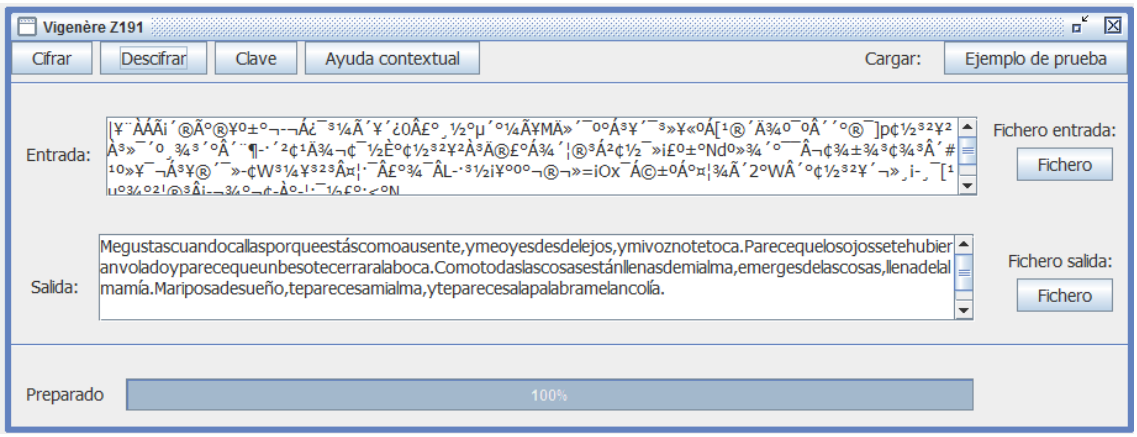

Figura 4. Operación descifrado de Vigenère mod 191.

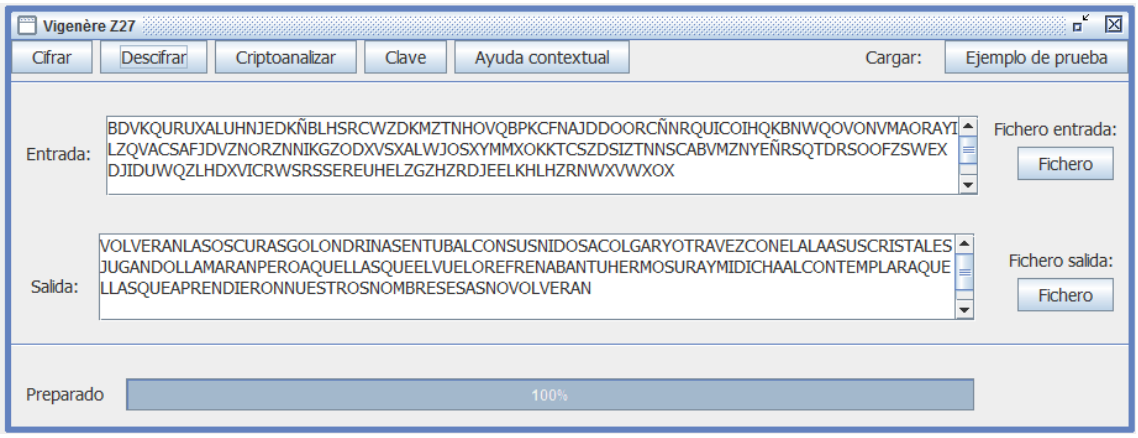

Figura 5. Operación descifrado de Vigenère mod 27 clave GOLONDRINAS.

II. Vigenère: ataque de Kasiski

Ejercicio 2)

2.1. Con el software Criptoclásicos v2.1 abre el Criptosistema Vigenère y en la ventana de Entrada pega este texto cifrado en módulo 27:
XUFMZUFPVMÑLHCPUYAKUÑIZOUHFLQSIUFAPENNDWZCAESBBTNRFPZATATLQTKATLQ
LSBBZEAVEMCZIUOCIEQNEWPYOLACPQRMODIZTSMFCZAUAÑKUOFAMWUDHYUMCOF
GPCZCNBBBNCHNVUNCHNEPOIHNRCQMWDFQQSSBJMETHEMJNLUOÑLQTNSPQBSVEHI
GADODWCOKCPUBCWRMWFSWCSMGOLDFBHDHRNPGOKIPMFAFODOQCSNUMNLIIBU
BDWLBTNNWCFZGOVONPEEIESBBRAOMWFCDIFUGELDFSÑAKUÑWNUFOTMRUWRPUY
AKCIIZDHTVANLASUMNCWRSIEYHMFLUJWCVPPAVODONVSLUMQSMATMZAEOSIZDHLV
MSOMOEWCALOEMEEIEÑBQTNDFLBEFMJMFPSLEIPITUKWHNUOSIMOFYNPYAFOMMO
OKRFACOFDJWPETAKWPEMUGIXDSCBTUNATPIXHHSUIXNHSCMFAEOTMZCSDBNNRHLB
MEANNQCQBDODWZMSRZWDUWRJIPOKMJZOOFTJÑBYMUÑWDUWRJIFDHRNPESHLB
2.2. Haz clic en Criptoanalizar y observa las repeticiones de cadenas de letras en el criptograma pinchando en dichas repeticiones.
2.3. Elige Tamaño de la repetición 3 y comprueba que la clave encontrada NW no es válida porque al descifrar no se obtiene texto en claro.
2.4. Elige Tamaño de la repetición 4 y comprueba que ahora la clave encontrada sí descifra correctamente el criptograma.
2.5. ¿Cuántas letras tiene cada uno de los subcriptogramas?
2.6. ¿Cuál es el máximo común divisor de las separaciones de cadenas iguales con 4 o más letras del criptograma: 24, 320, 294, 276, 6, 318, 120, 228, 54, 6? Comprueba que esa es la longitud de la clave propuesta.

2.7. Descifra el criptograma y comprueba pinchando en la cadena IZDH que aparece dos veces que ésta se corresponde con el texto en claro ANDO. Mira otras cadenas.

2.8. Observa cómo elige el programa las posiciones relativas de las letras A, E, O y S en cada uno de los seis subcriptogramas.

2.9. Si el texto en claro fuese más pequeño, el ataque sigue prosperando. Introduce el siguiente criptograma en la ventana de Entrada y criptoanaliza la cifra:
XUFMZUFPVMÑLHCPUYAKUÑIZOUHFLQSIUFAPENNDWZCAESBBTNRFPZATATLQTKATLQ LSBBZEAVEMCZIUOCIEQNEWPYOLACPQRMODIZTSMFCZAUAÑKUOFAMWUDHYUMCOF GPCZCNBBBNCHNVUNCHNEPOIHNRCQMWDFQQSSBJMETHEMJNLUOÑLQTNSPQBSVEHI GADODWCOKCPUBCWRMWFSWCSMGOLDFBHDHRNPGOKIPMFAFODOQCSNUMNLIIBU BDWLBTNNWCFZGOVONPEEIESBBRAO

2.10 Observa que ahora el ataque de Kasiski sigue funcionando aunque encuentra bien sólo 5 letras de la clave al elegir Tamaño de la repetición 4.

2.11 ¿Qué sucede si pinchas en Tamaño de repetición 3 y después en 2?

2.12 ¿Cuántas letras tiene ahora cada subcriptograma? ¿Qué puedes concluir al ver que un sistema con 27 letras se rompe haciendo estadísticas con tan poca cantidad de letras?

Comprueba tu trabajo:

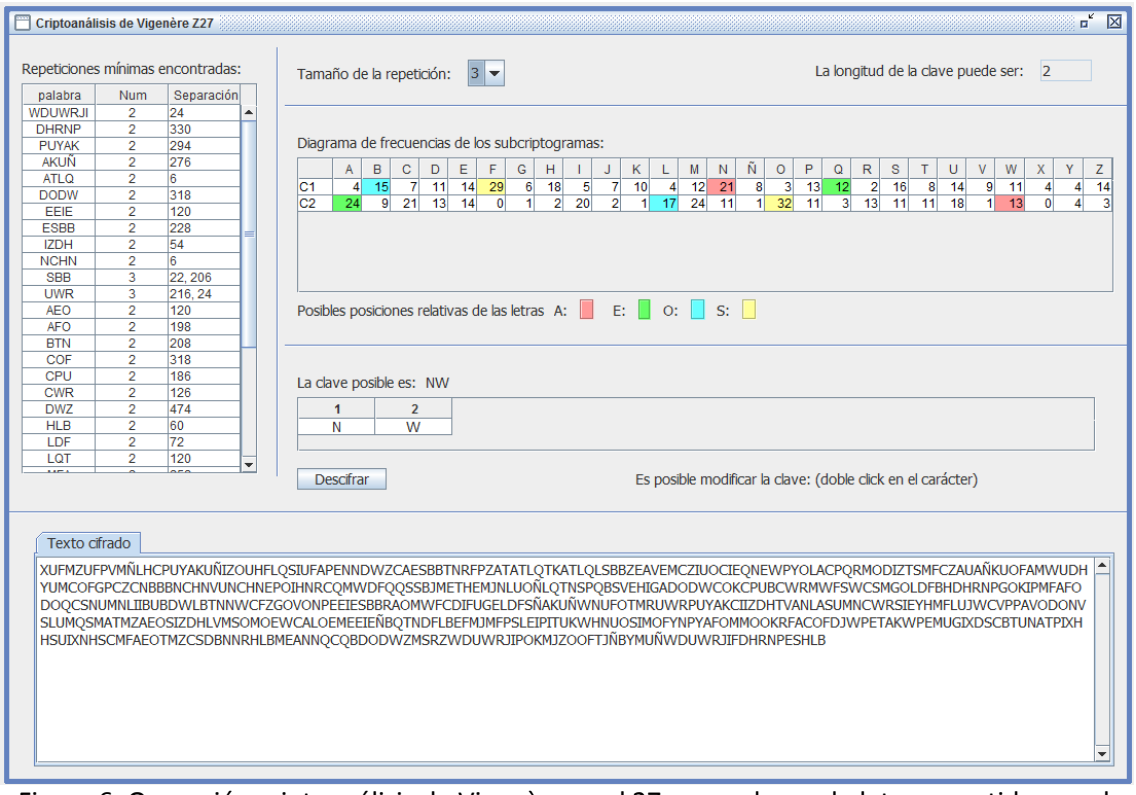

Figura 6. Operación criptoanálisis de Vigenère mod 27 con cadenas de letras repetidas en el criptograma de longitud 3 o mayor.

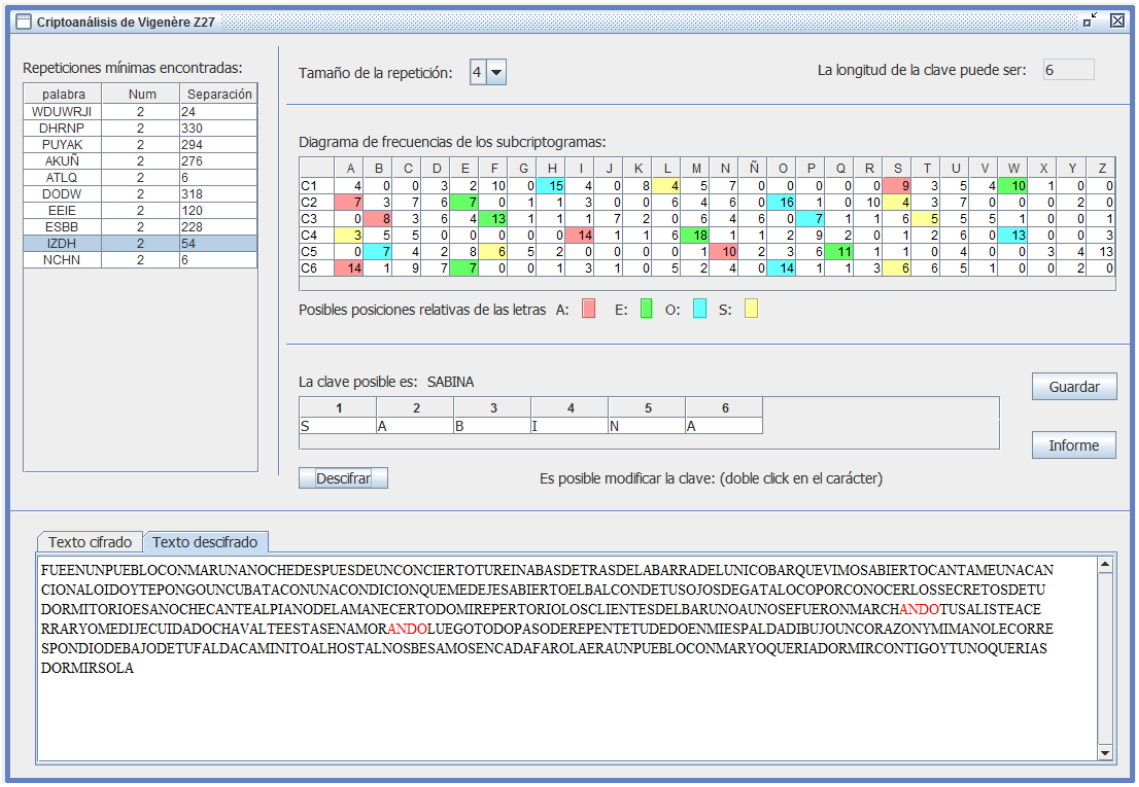

Figura 7. Operación criptoanálisis de Vigenère mod 27 con cadenas de letras repetidas en el criptograma de longitud 4 o mayor. Se muestra cadena en claro ANDO repetida.

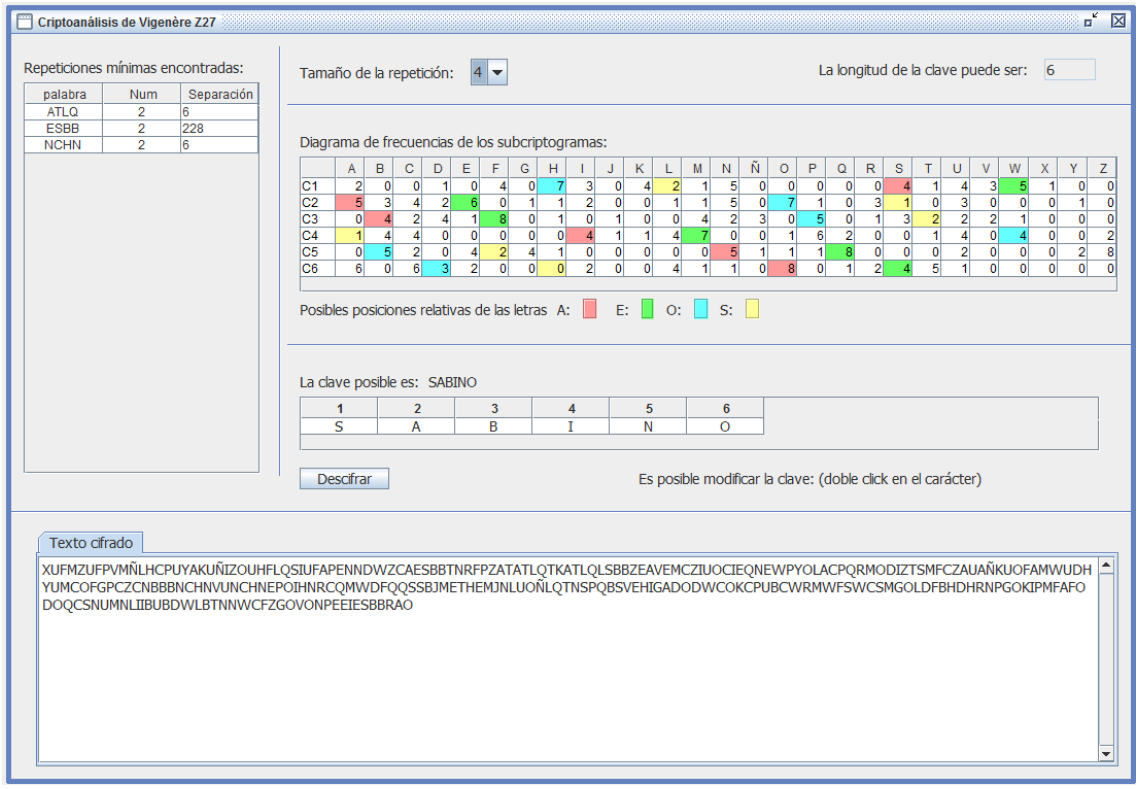

Figura 8. Operación criptoanálisis de Vigenère mod 27 con cadenas de letras repetidas en el criptograma de longitud 4 o mayor. Al tener menos texto cifrado, falla en la última letra.

Puedes utilizar esta documentación, otros libros, material multimedia y software de prácticas generados en Criptored, todos de libre distribución en Internet, para poder demostrar que entiendes y sabes cómo trabaja la criptografía, logrando la nueva certificación técnica profesional CriptoCert Certified Crypto Analyst, reconocida por el Centro Criptológico Nacional CCN de España, disponible desde el mes de abril de 2019.

Encontrarás más información sobre esta certificación y correo de contacto en el sitio web: https://www.criptocert.com

Madrid, 6 de mayo de 2019
Dr. Jorge Ramió Aguirre