

# Laboratorio B de Seguridad en la Computación, Informe Práctica 01

ESTUDIANTE: García Cáceres Uberto

GRUPO: B

## ACTIVIDADES

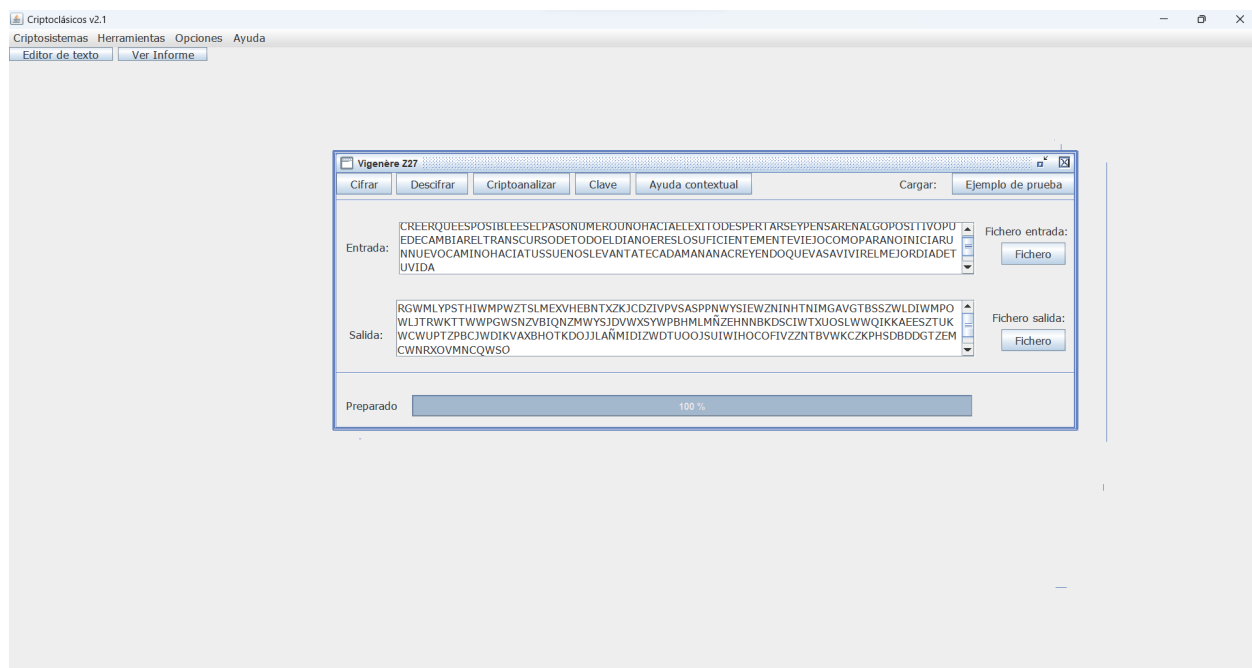
1)

```
string Vignere(string texto, string palabra, int n_mod = 26){  
    int j=0;  
    string traducido = "";  
    for (int i = 0; i < texto.size(); i++){  
        if(j == palabra.size()){  
            j = 0;  
        }  
        int de_texto = int(texto[i]) - 'A';  
        int de_palabra = int(palabra[j]) - 'A';  
        int data = MOD(de_texto + de_palabra, n_mod);  
        traducido += char(data + 'A');  
        j++;  
    }  
    return traducido;  
}
```

2)

RGWMLYPSTHIWMPWZTSLMEXVHEBNTXZKJCDZIVPVSASPPNWYSIEWZNINHTNIMGA  
VGTBSSZWLDIWMPOWLJTRWKTTWWPGWSNZVBIQNZMWYSJDVWXSYPBHMMLMÑZE  
HNNBKDCIWTXUOSLWWQIKKAESZTUKWCWUPTZPBCJWDIKVAXBHOKDOJJLAÑMI  
DIZWDTUOOJSUIWIHOCOFIVZZNTBVWKCZKPHSDBDDGTZEMCWNRXOVMNCQWSO

3)



4)

The screenshot shows the Visual Studio Code interface. The editor window displays a C++ file named `codigo.cpp` with the following code:

```
183 int main(){
184     setlocale(LC_ALL, "");
185     string original = "CREERQUEESPIBLEEELPASONUMEROUNOHAIELEXITODESPERTARSEYPENSARENALGOPOSITIVOPUEDECAMBIAR
186     cout<<"Cifrado con POSITIVO"<<endl;
187     string cifrado1 = Vignere(original, "POSITIVO");
188     cout<<cifrado1<<endl;
189 }
```

The terminal window shows the execution of the program:

```
PS C:\Users\Ubert.CHUBERT> cd "c:\Users\Ubert.CHUBERT\Documents\Uberto\UNSA\4to\2do_semestre\Seguridad en la Computación\Práctica 02\"
; if ($?) { g++ codigo.cpp -o codigo } ; if ($?) { .\codigo }
Cifrado con POSITIVO
RGMMLYPSTHIWMPWZTSLMEXVHEBNTXZKJCDZIVPVASPPNMYISIEWZINHTNIMGAVGTBSSZWLDIWMPOWLJTRWKTWMPGWSNZVBIONZMWSJDVWXSYPBHLMLÑZEHNBNBKDSCIWTXUO
SLWQIKKAEESZTUKWCWUPTZPBCJWDIKVAXBHOKDOJLLAÑMIDIZWDTUOJSUIWIHOCOFIVZZNTBVWKCZKPHSDBDDGTZEMCWNRXOVMMNCQWSO
Repeticion con clave POSITIVO
W : 26
S : 16
Z : 15
T : 15
I : 15
N : 12
D : 11
M : 11
P : 11
V : 10
K : 10
O : 10
```

5)

Repeticion con clave POSITIVO

Ñ : 2  
A : 5  
B : 9  
C : 8  
D : 11  
E : 7  
F : 1  
G : 5  
H : 8  
I : 15  
J : 7  
K : 10  
L : 7  
M : 11  
N : 12  
O : 10  
P : 11  
Q : 3  
R : 3  
S : 16  
T : 15  
U : 5  
V : 10  
W : 26  
X : 6  
Y : 4

#### Repeticion con clave HIELO

Ñ : 0

A : 6

B : 9

C : 10

D : 14

E : 6

F : 3

G : 8

H : 7

I : 23

J : 5

K : 6

L : 20

M : 11

N : 2

O : 16

P : 7

Q : 8

R : 6

S : 16

T : 9

U : 1

V : 10

W : 15

X : 9

Y : 5

#### Repeticion con clave MAR

Ñ : 5

A : 21

B : 2

C : 5

D : 12

E : 31

F : 2

G : 13

H : 2

I : 10

J : 6

K : 4

L : 11

M : 13

N : 7

O : 9

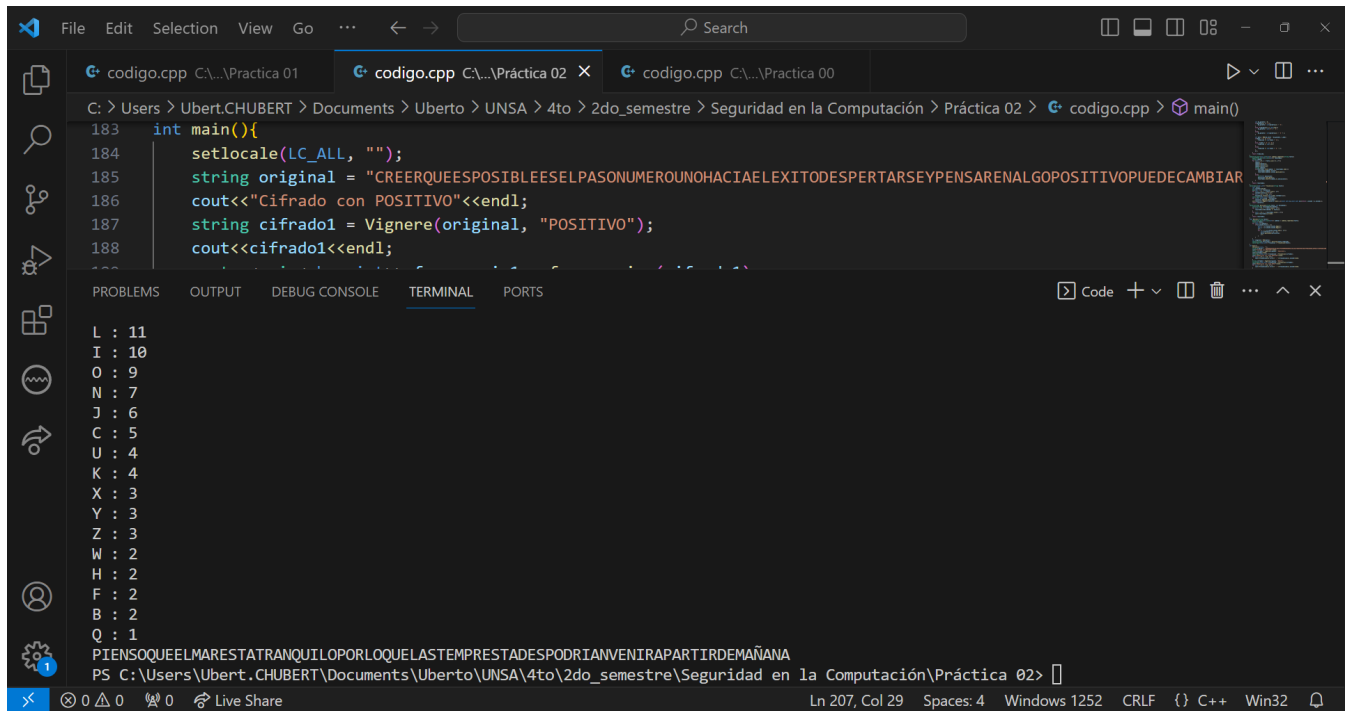
P : 15

Q : 1

R : 16

S : 11  
T : 14  
U : 4  
V : 17  
W : 2  
X : 3  
Y : 3

6)

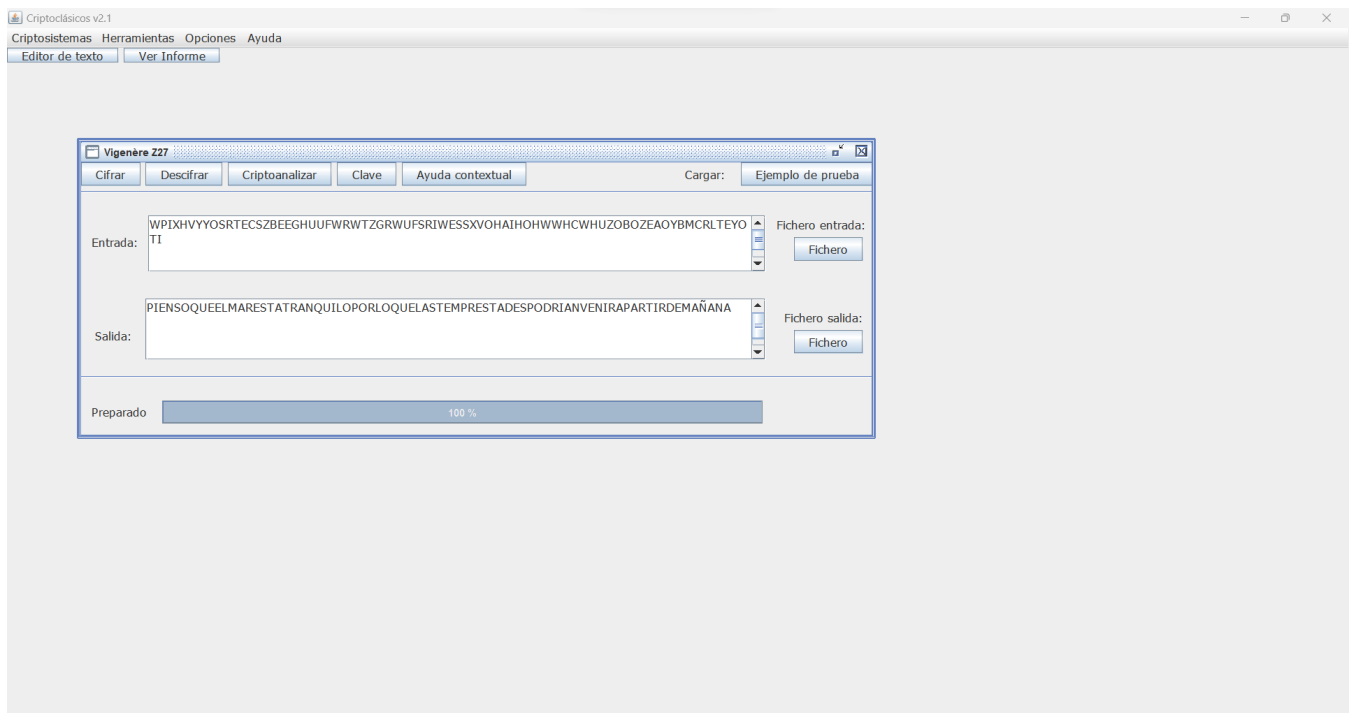


```
183 int main(){
184     setlocale(LC_ALL, "");
185     string original = "CREERQUEESPOSIBLEESEL PASONUMERO UNO HACIA EL EXITO DESPERTARSE PENSARENALGO POSITIVO PUEDE CAMBIAR
186     cout<<"Cifrado con POSITIVO"<<endl;
187     string cifrado1 = Vignere(original, "POSITIVO");
188     cout<<cifrado1<<endl;
189 }
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

L : 11  
I : 10  
O : 9  
N : 7  
J : 6  
C : 5  
U : 4  
K : 4  
X : 3  
Y : 3  
Z : 3  
W : 2  
H : 2  
F : 2  
B : 2  
Q : 1  
PIENSO QUE EL MARESTA TRANQUILO POR LO QUE LASTEMPRESADESPODRIAN VENIR A PARTIR DE MAÑANA  
PS C:\Users\Ubert.CHUBERT\Documents\Uberto\UNSA\4to\2do\_semestre\Seguridad en la Computación\Práctica 02>

7)



8)

## TRESSIGLOS

### CIFRADO CON AUTOCLAVE

DURANTE LAPRIMERAGUERRAMUNDIALWQSÑFJUUKSSDT CGOCTKGDVLFYODDDLGC  
CKLYAÑYDFWPPDNXWAXFMHÑXGTLWOUJFIQDGEMGWPPULROYTEQXVZAMIXOELÑ  
TWMTGELXHEPLIKÑTYHLCWIBJSMLERRIHFICULBBSWBZUUDUWHNSEOVBOSSHQLIS  
CSUÑMHEFCDKHSAYZAWGWHKVFHWFNIAÑNNTYUWÑOÑTKHVRKXCFKYCVSDQQJIAW  
EYNAKVWQÑAVBSÑWXOAZAU

### ATAQUE DE KASISKI

JACQUESSAUNIEREELRENOMBRADOCONRERVADORAVANZABATAMBALEANDOSEBA  
JOKABOVEDADELAGRANGALERIADELLUSEOARREMETIOCONTRALAPRIMERAPINTUR  
AQUEVIOUNCARAVAFGIOAGARRANDOELMARCODORADOAQUELHOMBREDESETENT  
AYSEISAÑOSTIRODELAOBRADARTEHASTAQUELAARRANCODEKAPAREDYSEDESPK  
OMOCAYENDOAOCAARRIBACONELLIENZOENCIMATALCOMOHABIAPREVISTOCERCAS  
EOYOELCHASQUIDODEUNAREJADEHIERROQUEALCERRARREALOQUEAAAEKACCES  
OALASALAE LRUELODEMADERATEMALOKEJOSSEDIRPAROUNAALARMAELCONSERVA  
DORSEQUEDOAHITENDIDOUNMOMENTOJADEANDOEVALUANDOLASITUACIONTODAVI  
AESTOYVIVOSEDIOLAVUELTA SEDESEMBARAZODELLIENZOYBUSCOCONLALIRADAAL  
FUNRITIODONDEESCONDERSEENAQUEKERPACIOCAVERNOSO

### CUESTIONARIO FINAL

- 1) Trabajando en módulo 191 (un subconjunto imprimible del código ASCII del software Criptoclásicos), cifra el siguiente texto en claro con la clave: El ingenioso hidalgo.

En un lugar de la Mancha, de cuyo nombre no quiero acordarme, no ha mucho tiempo que vivía un hidalgo de los de lanza en astillero, adarga antigua, rocin flaco y galgo corredor. Una olla de algo mas vaca que carnero, salpicon las más noches, duelos y quebrantos los sábados, lentejas los viernes, algun palomino de añadidura los domingos, consumían las tres partes de su hacienda. El resto della concluían sayo de velarte, calzas de velludo para las fiestas con sus pantuflos de lo mismo, los días de entre semana se honraba con su vellori de lo más fino. Tenía en su casa una ama que pasaba de los cuarenta, y una sobrina que no llegaba a los veinte, y un mozo de campo y plaza, que así ensillaba el rocin como tomaba la podadera.

IXCZQYSIGVSRIOAXIVEÑMOACBUDEPYMPOBAWICWNISELOKALURHLRJGRWGNİYXDJJLDLVS  
GJQRPPGOSWRWZVAGEVGBDLMZGWGPZDSYWDDLXUELUGÑKHIGHQOUIILLDCQIXMSOWGK  
SKWUUXGDOVIPKEXÑDEOZDDCLWJINIESIEWHSZWPFOXQOWWIFSSOOSLRBMÑODEFYOJEG  
QGWHDDZADBLJDWVMZZIVIHDDZDLECSSLSSAQCIZHAOURDOGCENPPAVNSDLRVTLNQUH  
GZUFAPUIBDOZBUEDVOVEMFJIFCVSQOMPD LKZVOAGUHQSZSQVUFLFÑOQDILUHQDSDOYB  
HCLQÑEDLQBIXSJVDWIUAVGHJSMFZEFKDFHBASAXZJJVWFJIXWAAHSWÑODJWEDLQKQGZS  
LSSIPADKVSXZNHEOWBLJCMÑLZXWHOSBREFNWF DAMPILKBWFKNYEHUOSAHYXEAGHEMIP  
KOB AQNOYMP TLEJQLABHVUUOJJLURLVKUEMINQSFD SABAMBUXRDDZLQIEYXDQERICABAS  
EDPQSWUSZSPHMÑRZI WQN WYUXBTOTORISOÑGRICI

- 2) Descifre el criptograma en el mismo software ¿Por qué crees que el software no permite hacer un criptoanálisis?

Porque el MCD es 1.

- 3) Si el cifrado de Vigenere es IZLQOD y la clave SOL, ¿cuál era el mensaje en claro?

PLAYAS

- 4) ¿Cuál será la cifra con autoclave del texto HABIA UNA VEZ, con la clave CIRCO?

JISKO WUR XSB

- 5) En el ataque a Vigenere por Kasiski ¿Qué buscamos preferentemente?

Saber la longitud de la palabra mediante cadenas que se repiten.

- 6) Encontradas las cadenas repetidas en el criptograma, con separación d1, d2, d3 y d4 ¿Cuál sería la longitud L de la clave?

Será el MCD entre d1, d2, d3 y d4.

- 7) Si las distancias entre repeticiones de cadenas en un criptograma son 35, 112, 70. ¿Cuál sería la longitud L de la clave?

Será 7.

- 8) ¿Qué diferencia la regla AEOS de AEO en Kasiski?

La regla AEO es fundamental para el ataque de Kasiski, por otro lado, la regla AEOS es una variante y no puede hacer gran impacto como AEO.

**Repositorio de Github usado:**

<https://github.com/UbertoGC/Laboratorio-B-Seguridad-en-la-Computacion>