Laboratorio B de Seguridad en la Computación, Informe Práctica 01

ESTUDIANTE: García Cáceres Uberto
GRUPO: B

ACTIVIDADES

```cpp
#include <iostream>
#include <fstream>
#include <map>
#include <list>
#include <algorithm>
#include <vector>
#include <Windows.h>
#include <cstdio>
#include <string>
#include <io.h>
#include <fcntl.h>
using namespace std;
int MCD(list<int> numeros){
    int mcd, residuo;
    for (auto it:numeros){
        if(it == *(numeros.begin())){
            mcd = it;
        }
        else{
            do
            {
                residuo = mcd % it;
                mcd = it;
                it = residuo;
            } while (residuo != 0);
        }
    }
    return mcd;
}
map<char, int> frecuencias(string archivo){
    ifstream documento(archivo);
    char letra;
    int contador[26]{0};
    map<char, int> frecuencia;
    while (!documento.eof()){
        documento>>letra;
        contador[letra-'A']++;
    }
    documento.close();
```

```
    for (int i = 0; i < 26; i++)
        frecuencia.insert({char(i+65),contador[i]});
    return frecuencia;
}
map<string,pair<int,list<int>>> cadenas_repetidas(string texto){
    map<string,pair<int,list<int>>> resultados;
    string cadena;
    for (int i = 0; i < texto.size()-2; i++){
        cadena="";
        cadena+=texto[i];
        cadena+=texto[i+1];
        cadena+=texto[i+2];
        string cadena2;
        if(resultados.find(cadena) != resultados.end()){
            resultados[cadena].first++;
            resultados[cadena].second.push_back(i);
        }
        else{
            list<int> ubicacion1;
            ubicacion1.push_back(i);
            resultados.insert({cadena,{1,ubicacion1}});
        }
    }
    return resultados;
}
void kasiski(string texto){
    map<string,pair<int,list<int>>> cadenas = cadenas_repetidas(texto);
    list<int> datos;
    for (auto it:cadenas){
        if(it.second.first > 1){
            cout<<it.first<<" --- "<<it.second.first<<endl;
            auto i = it.second.second.begin();
            auto j = it.second.second.begin();
            i++;
            cout<<"|";
            for (; i != it.second.second.end(); i++){
                int diferencia = *i - *j;
                cout<<diferencia<<"|";
                datos.push_back(diferencia);
                j++;
            }
            cout<<endl;
        }
    }
}
string hexadecimal(int n){
    string r="";
```

```
    int resultado, residuo;
    int digitos[20];
    int i=0;
    do{
        residuo = n%16;
        resultado = n / 16;
        digitos[i] = residuo;
        n = resultado;
        i++;
    }while(resultado > 15);
    digitos[i] = resultado;
    for (int j = i; j >= 0; j--){
        if(digitos[j] > 9){
            r += char('A' + digitos[j] - 10);
        }
        else{
            r += to_string(digitos[j]);
        }
    }
    return r;
}
void UNICODE_8(string texto){
    ofstream documento("unicode8_traduccion.txt");
    for (int i = 0; i < texto.size(); i++){
        int ascii = int(texto[i]);
        string conversion = hexadecimal(ascii);
        documento<<conversion;
    }
    documento.close();
}
string ANADIENDO_AQUI(string texto){
    ofstream documento("anadiendoaqui.txt");
    string nuevo_texto="";
    for (int i = 0; i < texto.size(); i++){
        if(i%20 == 19){
            nuevo_texto+="AQUI";
        }
        nuevo_texto+=texto[i];
    }
    while (nuevo_texto.size() % 4){
        int aleatorio = rand()%26 + 'A';
        nuevo_texto+=char(aleatorio);
    }
    documento<<nuevo_texto;
    documento.close();
    return nuevo_texto;
}
```

```
int main(){
    string archivo = "HERALDOSNEGROS_pre.txt";
    map<char, int> contador;
    contador = frecuencias(archivo);
    vector<pair<char,int>> convertir;
    for (const auto &item : contador) {
        convertir.emplace_back(item);
    }
    sort(convertir.begin(),convertir.end(),[](const auto &x,const auto &y){return
x.second > y.second;});
    /**/
    cout<<"CARACTERES CON MAYOR FRECUENCIA: "<<endl;
    for (int i = 0; i < 5; i++){
        cout<<convertir[i].first<<": "<<convertir[i].second<<endl;
    }
    string texto = "";
    char letra;
    ifstream documento(archivo);
    while (!documento.eof()){
        documento>>letra;
        texto+=letra;
    }
    documento.close();
    /**/
    cout<<endl<<"METODO KASISKI: "<<endl;
    kasiski(texto);
    /**/
    cout<<endl<<"CIFRADO UNICODE-8: "<<endl;
    UNICODE_8(texto);
    convertir.clear();
    contador.clear();
    contador = frecuencias("unicode8_traduccion.txt");
    for (const auto &item : contador) {
        convertir.emplace_back(item);
    }
    sort(convertir.begin(),convertir.end(),[](const auto &x,const auto &y){return
x.second > y.second;});
    cout<<"CARACTERES CON MAYOR FRECUENCIA: "<<endl;
    for (int i = 0; i < 5; i++){
        cout<<convertir[i].first<<": "<<convertir[i].second<<endl;
    }
    string texto2 = "";
    documento.open("unicode8_traduccion.txt");
    while (!documento.eof()){
        documento>>letra;
        texto2+=letra;
    }
```

```
    documento.close();
    cout<<"METODO KASISKI: "<<endl;
    kasiski(texto2);
    /**/
    cout<<endl<<"ANADIENDO LA CADENA AQUI: "<<endl;
    string texto3 = ANADIENDO_AQUI(texto);
    convertir.clear();
    contador.clear();
    contador = frecuencias("anadiendoaqui.txt");
    for (const auto &item : contador) {
        convertir.emplace_back(item);
    }
    sort(convertir.begin(),convertir.end(),[](const auto &x,const auto &y){return
x.second > y.second;});
    cout<<"CARACTERES CON MAYOR FRECUENCIA: "<<endl;
    for (int i = 0; i < 5; i++){
        cout<<convertir[i].first<<": "<<convertir[i].second<<endl;
    }
    cout<<"METODO KASISKI: "<<endl;
    kasiski(texto3);
    return 0;
}
```

CUESTIONARIO FINAL

1) **Describa los siguientes términos (áreas de la seguridad informática)**
   - **Protección y seguridad de los datos**
   - **Criptografía**
   - **Seguridad y fortificación de redes**
   - **Seguridad en aplicaciones informáticas,programas y bases de datos**
   - **Gestión de seguridad en equipos y sistemas informáticos**
   - **Informática forense**
   - **Ciberdelito, ciberseguridad**

Respuestas:

- **Protección y seguridad de los datos: medidas que se llevan a cabo con el fin de asegurar que los datos no sean vulnerados.**
- **Criptografía: método de protección de la información usando códigos.**
- **Seguridad y fortificación de redes: medidas enfocadas en proteger y fortalecer las redes de una organización.**
- **Seguridad en aplicaciones informáticas, programas y bases de datos: herramientas, medidas y controles para mantener la confidencialidad, disponibilidad e integridad de una aplicación, programa o una base de datos.**
- **Gestión de seguridad en equipos y sistemas informáticos: Proceso por el cuál se implementan los controles del plan de seguridad.**
- **Informática forense: Proceso para rastrear y enjuiciar a ciberdelincuentes**
- **Ciberdelito, ciberseguridad: Ciberdelito es un tipo de crimen que se comete usando medidas informáticas, ciberseguridad son las herramientas, normas y medidas que se usan para controlar la seguridad informática.**

2) **Describa los siguientes términos (áreas de la seguridad de la información)**
   - **Gestión de la seguridad de la información**
   - **Asesoría y auditoría de la seguridad**
   - **Análisis y gestión de riesgos**
   - **Continuidad de negocio**
   - **Buen gobierno**
   - **Comercio electronico**
   - **Legislación relacionada con seguridad**

   Respuestas:
   - **Gestión de la seguridad de la información: Es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización.**
   - **Asesoría y auditoría de la seguridad: Grupos encargados de supervisar, evaluar, administrar y asesorar la seguridad de una empresa.**
   - **Análisis y gestión de riesgos: Proceso que ayuda a determinar vulnerabilidades y amenazas de una empresa/organización con el fin de crear controles que minimicen los riesgos.**
   - **Continuidad de negocio: Cualidad que determina si aún bajo un ataque, el servicio puede continuar funcionando.**
   - **Buen gobierno: Liderazgo, estructura y proceso para proteger la información.**
   - **Comercio electrónico: Transacciones electrónicas, que permiten comprar y vender productos y servicios.**
   - **Legislación relacionada con seguridad: Conjunto de leyes y normas que regulan un sistema de seguridad implementado.**

3) **Describa alguna otra operación o función de preprocesamiento que se implemente sobre el texto claro en los criptosistemas, en que afecta la complejidad de estas funciones al desempeño del mismo**

   Respuesta:
   Es un formato

4) **Describa la máquina enigma, luego muestre usando un simulador en internet la encriptación de la frase QUERIDA HIJA, para tres posiciones distintas de los rotores**

   Respuesta:
   Es un formato

5) **Describa la aplicación de Unicode-8**

   Respuesta:
   Es un formato de codificación de caracteres Unicode e ISO 10646 que utiliza símbolos de longitud variable. Divide los caracteres Unicode en grupos según los bytes que se requieren para codificarlos, siendo las siguientes categorías:
   - **Caracteres de 1 byte: caracteres US-ASCII**
   - **Caracteres de 2 bytes: caracteres romances, griegos, armenios, hebreos, etc.**
   - **Caracteres de 3 bytes: caracteres multilingüe y del grupo CJK.**
   - **Caracteres de 4 bytes: caracteres del plano suplementario multilingüe, Lineal B, persa, etc.**

   Cada uno de estos se codifica de la siguiente manera:
   - **Caracteres de 1 byte: Símbolos de un único byte donde el bit más significativo es 0**

- **Caracteres de 2 bytes: El primer byte comienza con 110, el segundo byte comienza con 10**
- **Caracteres de 3 bytes: El primer byte comienza con 1110, los bytes siguientes comienzan con 10**
- **Caracteres de 4 bytes: El primer byte comienza con 11110, los bytes siguientes comienzan con 10**

Por ejemplo, la letra “ñ” al ser codificada primero se cambia a los valores de 0 y 1, siendo:
0000 0000 1111 0001
Siendo de 2 bytes, por lo que al codificarse se tiene lo siguiente:
110x xxxx 10xx xxxx
Luego se eliminan los bits innecesarios, en este caso, los 5 primeros:
000 1111 0001
Y ahora procedemos a reemplazarlo en sus respectivos campos:
1100 0111 1011 0001
Lo que nos da el siguiente resultado:
1100 0111 1011 0001 = C3B1

Repositorio de Github usado:
https://github.com/UbertoGC/Laboratorio-B-Seguridad-en-la-Computacion