UNIVERSIDAD DE CARABOBO
DEPARTAMENTO DE COMPUTACIÓN
REDES DE COMPUTADORAS II
SEMESTRE 2 2016

PROYECTO DE CIFRADO

V4.1

ADVERTENCIA: LEA CUIDADOSAMENTE TODO EL DOCUMENTO A CONTINUACIÓN PARA EVITAR CONFUSIONES/OMISIONES Y ESCUCHE DETENIDAMENTE EL AUDIO DE LA SESIÓN DE ACLARATORIAS Y CONSULTAS (QUE SE REMITIRÁ POSTERIORMENTE).

Objetivo:

Desarrollar un esquema de Criptografía que cumpla las condiciones que se expresan en las condiciones del Proyecto y aplicarlo a un texto llano para ser evaluados por los demás integrantes del curso para intentar descifrarlo.

Descifrar la mayor cantidad de los textos encriptados por sus compañeros de curso.

Condiciones y pautas del proyecto:

1º_ Podrán emplear **únicamente** el método de Cifrado por Transposición o Sustitución de forma simple (es decir solo una vez), y podrán emplear cualquiera de los esquemas o variantes del método empleado (deberán justificarlo en el informe inicial con referencias que lo demuestren).

2º_ La clave será (de ser el caso) de hasta **16 caracteres** alfanumérica (incluyendo la ñ) diferenciando mayúsculas de minúsculas.

3º_ El texto llano original (inicial a ser encriptado) será tomado de algún párrafo de un libro de literatura clásica en castellano de entre **600 y 1.000 caracteres** de longitud (Tomaremos el libro de la Biblia propuesto en clase y que se les remito por correo para unificar una versión, se tomará solo el texto principal de uno cualquiera de los libros principales y no de los comentarios, notas al pie de página o cualquier otro texto). Se le quitarán los números de los capítulos, versículos o cualquier otro carácter inválido que pueda contener. El texto cifrado no podrá sobrepasar la **relación de 3:1** es decir entre los **1800 y los 3000 caracteres** de longitud**.**

4º_ Solo se aceptan caracteres alfanuméricos incluyendo la ñ, mayúsculas y minúsculas, punto, coma, punto y coma, dos puntos, comillas, abre paréntesis, cierra paréntesis, signos de interrogación, salto de línea y el espacio en blanco de último (el salto de línea no se considerará si aparece como último carácter del texto) como se muestra a continuación (y en ese orden):

AaBbCcDdEeFfGgHhIiJjKkLlMmNnÑñOoPpQqRrSsTtUuVvWwXxYyZz.,;:”()¿?$&

Siendo:
$= Salto de línea
&= Espacio en blanco

Todo otro carácter que aparezca diferente deberá ser eliminado (incluso los acentos). Asimismo los números de los capítulos y versículos. Ejemplo:

En la página 1082 donde dice “según San Juan” (copiando y pegando el texto del archivo remitido):

El Logos
1En un principio° era° el Logos,° y el
Logos estaba ante° Dios, y Dios era el
Logos.
2 En un principio Éste estaba ante Dios.°
3 Todas las cosas por Él° fueron hechas, y
sin Él, nada de lo que ha sido hecho fue
hecho.°
4 En Él había vida°, y la vida era la luz de
los hombres.
5 La luz resplandece en las tinieblas, y las
tinieblas no prevalecieron contra ella.°
6 (Hubo un hombre enviado de° Dios, de
nombre Juan;°
7 éste vino como testigo para que diera
testimonio de la luz, a fin de que todos
creyeran por él;
8 no era él la luz, sino para que diera testimonio
de la luz.)
9 La luz° verdadera, que alumbra a todo
hombre al venir al mundo,
10 estaba en el mundo, y el mundo fue hecho
por Él, pero el mundo no lo conoció.
11 A lo suyo° vino, y los suyos no lo recibieron,
12 pero a todos los que lo recibieron, a los
que creen en su nombre, les dio potestad
de ser hechos hijos de Dios,
13 los cuales no nacieron° de sangres,° ni
de voluntad de carne, ni de voluntad de
varón, sino de Dios.
14 Y el Logos se hizo carne, y tabernaculizó°
entre nosotros, y contemplamos su
gloria (gloria como del Unigénito del Padre),
lleno de gracia y de verdad.

Luego de depurado (quitando acentos, numeración y otros caracteres) quedará así (como texto corrido):

En un principio era el Logos, y el Logos estaba ante Dios, y Dios era el Logos.
En un principio Este estaba ante Dios.
Todas las cosas por El fueron hechas, y sin El, nada de lo que ha sido hecho fue hecho.
En El habia vida, y la vida era la luz de los hombres.
La luz resplandece en las tinieblas, y lastinieblas no prevalecieron contra ella.

(Hubo un hombre enviado de Dios, de nombre Juan;
este vino como testigo para que diera testimonio de la luz, a fin de que todos creyeran por el;
no era el la luz, sino para que diera testimonio de la luz.)
La luz verdadera, que alumbra a todo hombre al venir al mundo,
estaba en el mundo, y el mundo fue hecho por El, pero el mundo no lo conocio.
A lo suyo vino, y los suyos no lo recibieron,
pero a todos los que lo recibieron, a los que creen en su nombre, les dio potestad de ser hechos hijos de Dios,
los cuales no nacieron de sangres, ni de voluntad de carne, ni de voluntad de varon, sino de Dios.
Y el Logos se hizo carne, y tabernaculizo entre nosotros, y contemplamos su gloria (gloria como del Unigenito del Padre), lleno de gracia y de verdad.

Este texto tiene 1.085 caracteres incluyendo los espacios al que hay que agregarle 13 saltos de línea (recordemos que el último salto de línea no cuenta) para un total de 1098 caracteres (según el contador de Word de la máquina) por lo que no cumple con lo establecido, luego hay que reducirlo quedando por ejemplo:

En un principio era el Logos, y el Logos estaba ante Dios, y Dios era el Logos.
En un principio Este estaba ante Dios.
Todas las cosas por El fueron hechas, y sin El, nada de lo que ha sido hecho fue hecho.
En El habia vida, y la vida era la luz de los hombres.
La luz resplandece en las tinieblas, y lastinieblas no prevalecieron contra ella.
(Hubo un hombre enviado de Dios, de nombre Juan;
este vino como testigo para que diera testimonio de la luz, a fin de que todos creyeran por el;
no era el la luz, sino para que diera testimonio de la luz.)
La luz verdadera, que alumbra a todo hombre al venir al mundo,
estaba en el mundo, y el mundo fue hecho por El, pero el mundo no lo conocio.
A lo suyo vino, y los suyos no lo recibieron,
pero a todos los que lo recibieron, a los que creen en su nombre, les dio potestad de ser hechos hijos de Dios,
los cuales no nacieron de sangres, ni de voluntad de carne, ni de voluntad de varon, sino de Dios.

Ahora contiene 935 caracteres incluidos los espacios en blanco (y hay que agregarle 12 saltos de línea para un total de 947 caracteres) y no hay caracteres inválidos ni la numeración. por lo que se cumplen las condiciones establecidas, el texto concluye con un punto.

4º_ La fecha tope para remitir el Informe inicial (en .pdf) con los textos llano y cifrado (en .txt) será el **sábado 18 de marzo de 2017** (por correo electrónico). Luego de una revisión básica del material enviado por Uds. y contactados los casos con inconvenientes, se les remitirá a su dirección de correo electrónico el domingo 19/03 como Casos (los textos cifrados de cada uno sin identificar a sus autores para que trabajen sobre ella).

5º_ Deberán emplear/desarrollar una aplicación que les facilite el proceso de cifrar/descifrar los archivos (esta aplicación la remitirán para su evaluación y formará parte de su respuesta).

6º_ El proyecto inicial lo remitirán con un informe (en pdf) y adicionalmente enviaran el texto original y el cifrado en archivo .txt (solo el texto, no añada ningún comentario o similar) titulando el archivo como “Texto cifrado” y el otro como “Texto llano”, con los siguientes componentes:

Informe Inicial:

Portada
Con encabezado de la Universidad, Facultad y Departamento, el nombre del proyecto, autor y C.I., Curso, Nombre del Profesor y fecha.

Marco Teórico
Describir detalladamente las particularidades del método empleado por Ud. demostrando que cumple los requerimientos exigidos en este proyecto.

Resultados
Aquí colocarán dos párrafos, uno con el texto llano y el otro con el texto cifrado según exigencias anteriores, asimismo colocaran la clave empleada y el programa para cifrar su texto. Además deberán añadir aquí la cantidad total de caracteres del texto llano y del texto cifrado mostrando que cumplen con las exigencias del proyecto (En general, colocarán cualquier información asociada con la realización y ejecución del proyecto).

Conclusiones/Recomendaciones

Referencias Bibliográficas

Adicionalmente enviaran aparte los 2 archivos en .txt con el texto llano y el cifrado.

7º_ Al final cuando entreguen (con todos sus datos) el informe final del proyecto con los resultados de los casos resueltos, estos deberán presentarse en el mismo formato con que se les remitió llenando los campos faltantes, así mismo deberán remitir enlaces o programas empleados para romper el cifrado.

Informe Final:

Portada
Con encabezado de la Universidad, Facultad y Departamento, el nombre del proyecto, autor y C.I., Curso, Nombre del Profesor y fecha.

Marco Teórico
Describir detalladamente las particularidades de los métodos empleados por Ud. para descifrar a sus adversarios.

Resultados
Aquí colocarán dos párrafos, uno los casos resueltos indicando el texto cifrado y el texto descifrado. Igualmente deberán indicar si algún caso no cumple con las especificaciones del proyecto mostrando las razones por las que no cumple (requisito básico para obtener los puntos de ese caso), asimismo colocaran la clave empleada (Todo esto lo harán para cada caso). En general, colocarán cualquier información asociada con el proceso de descifrar de interés (como programas hechos por Ud. o de otros, enlaces de interés, etc.).

Conclusiones/Recomendaciones

Referencias Bibliográficas

Adicionalmente enviaran aparte los archivos en .txt por cada caso descifrado con el texto llano obtenido (indicando el número de caso en cada uno).

8º_ La fecha tope para enviarme el informe final del proyecto con los criptogramas descifrados será hasta la media noche del **martes 18 de abril de 2017**.

9º_ Con respecto a la evaluación esta constará de cuatro partes:

a) La primera parte, involucra la realización del archivo encriptado con su respectivo informe inicial el cual vale hasta 4 puntos (y será válido si y solo si, han desencriptado correctamente al menos un caso diferente al suyo) de lo contrario su nota cera de cero.
b) La segunda parte, implica en informe final y los casos desencriptados de sus compañeros y vale hasta otros 4 puntos (deberá romper al menos un caso para poder considerar válida la parte "a" anterior). Por cada caso extra que des encripté (es decir de 2 en adelante) sumará 3 puntos a su nota para un máximo de 20 puntos en la definitiva del proyecto (es decir que si des encriptó un caso añade 0 puntos, desencriptó 2 casos añade 3 puntos, desencriptó 3 casos añade 6 puntos y así sucesivamente).
c) La tercera parte es la de los descuentos, el cual establece que por cada participante que logré desencriptar su archivo le restará 4 puntos de su nota (el límite es hasta llegar a cero).
d) Se considerará buena la respuesta desencriptada, si el texto descifrado esta correcto en al menos un 90% de los caracteres, para ello emplearemos algún programa para comparar como Notepad++, Beyond Compare, etc, o también en línea como (http://www.ddginc-usa.com/spanish/text-compare-tool.html).

10º_ En caso de que su archivo encriptado estuviere errado, se le asignará 2 puntos a todos los demás y desde luego Ud. quedará descalificado (con 0 puntos de definitiva), por lo que le recomendamos que revise muy bien su archivo antes de enviarlo. Al final una vez que todos hayan enviado las respuestas les remitiré los resultados de los casos de cada uno a todos sus compañeros, para que puedan revisar y evaluarse durante la defensa que cada uno hará de su trabajo, de donde se colocará la nota definitiva del proyecto.

CUIDE SU INFORMACIÓN PUES LA SEGURIDAD DE SU DATA ES SU RESPONSABILIDAD…….

Cronograma (Resumen):

Fecha 2017	Actividad	Observaciones
12/03	Pliego de Condiciones y texto de la literatura clásica seleccionada en clase.	Lo recibirán por correo
Del 12 al 15/03	Recepción de correos con dudas.	Estas serán expuestas en la clase de Aclaratorias y dudas (se mantendrá el anonimato de quien plantea la pregunta).
16/03	Aclaratorias y dudas	En clase, remitiremos por correo la sesión grabada de la

		consulta a cada uno para referencia.
18/03	Entrega Informe Inicial y los 2 archivos txt (texto llano y texto cifrado)	Informe en .pdf, el texto llano y cifrados en .txt (un archivo por cada uno). Recordar no colocar ni en el contenido ni en el nombre del archivo algún nombre o descripción que los identifique, simplemente llamen los archivos como Texto Llano y Texto Cifrado. El Informe si lo identifican como: Informe Inicial + (Su nombre)
19/03	Remisión del listado de casos cifrados.	Por correo electrónico
18/04	Entrega Informe Final y los archivos en .txt descifrados	Informe en .pdf, el texto descifrados de cada caso resuelto en .txt (un archivo por cada caso). Identificar el archivo .txt resuelto con el número del caso correspondiente así: Resuelto Caso XX. El Informe si lo identifican como: Informe Final + (Su nombre)
19/04	Remisión de los Informes finales y archivos descifrados de todos para todos	Por correo electrónico
20/04	Primera sesión de defensa.	En clase
24/04	Segunda sesión de defensa.	En clase
27/04	Tercera sesión de defensa.	En clase

En clase sortearemos el orden para la defensa de su proyecto……

En caso de algún detalle, favor notificármelo por correo a la brevedad posible…

MUCHO ESFUERZO Y BUENA SUERTE……

Prof. Antonio Castañeda