Proyecto 1 Paradigma iterativo.

Instituto Tecnológico de Costa Rica

Proyecto ASM encriptación y desencriptación

Nombre del curso: ARQUITECTURA DE COMPUTADORAS **Código del curso:** IC-3101

Profesor: M.Sc, CARLOS BENAVIDES, Ing. **Asistente: Kenneth Obando.**

Vigencia: primer semestre, 2017. **Fecha de entrega:** 1 mayo, 2017

1. Antecedentes del proyecto

Criptografía

Data Encryption Standard (DES) es un algoritmo de cifrado, es decir, un método para cifrar información, escogido como un estándar FIPS en los Estados Unidos en 1976, y cuyo uso se ha propagado ampliamente por todo el mundo. El algoritmo fue controvertido al principio, con algunos elementos de diseño clasificados, una longitud de clave relativamente corta, y las continuas sospechas sobre la existencia de alguna puerta trasera para la National Security Agency (NSA). Posteriormente DES fue sometido a un intenso análisis académico y motivó el concepto moderno del cifrado por bloques y su criptoanálisis.

Hoy en día, DES se considera inseguro para muchas aplicaciones. Esto se debe principalmente a que el tamaño de clave de 56 bits es corto; las claves de DES se han roto en menos de 24 horas. Existen también resultados analíticos que demuestran debilidades teóricas en su cifrado, aunque son inviables en la práctica. Se cree que el algoritmo es seguro en la práctica en su variante de Triple DES, aunque existan ataques teóricos.

Desde hace algunos años, el algoritmo ha sido sustituido por el nuevo AES (Advanced Encryption Standard).

En algunas ocasiones, DES es denominado también DEA (Data Encryption Algorithm).

En el proceso de cifrado/descifrado se establecen una serie de términos y convenios para facilitar referirse a los distintos elementos que intervienen:

- El texto en claro o texto plano (en inglés, plain text) es el mensaje que se cifra.
- El criptograma o texto cifrado es el mensaje resultante una vez que se ha producido el cifrado, es decir, el mensaje cifrado.
- El cifrado es el proceso que consiste en convertir el texto plano en un galimatías ilegible (cifrar), el mensaje cifrado.
- El cifrador es el sistema que implementa el algoritmo de cifrado.
- El algoritmo de cifrado o cifra es el algoritmo que se utiliza para cifrar.
- La clave de cifrado se utiliza en el algoritmo de cifrado.
- El descifrado es el proceso de convertir el texto cifrado en el texto en claro.
- El descifrador es el sistema que implementa el algoritmo de descifrado.
- El algoritmo de descifrado o descifra es el algoritmo que se utiliza para descifrar.
- La clave de descifrado se utiliza en el algoritmo de descifrado.
- La gestión de claves es el proceso de generación, certificación, distribución y cancelación de todas las claves, necesarios para llevar a cabo el cifrado.
- El criptosistema es el conjunto estructurado de los protocolos, los algoritmos de cifrado/descifrado, los procesos de gestión de claves y las actuaciones de los usuarios.
- La descripción de entidades: cuando se desea describir un algoritmo de cifrado/descifrado que involucra el envío de mensajes secretos, muchos autores usan los nombres genéricos Alice y Bob en lugar de los crípticos A y B. Si intervienen otras entidades (C, D, F... -la E quedaría reservada-), se les asignan entonces nombres que empiecen con estas iniciales, y los más frecuentes son Carol y Dave. Cuando un escenario involucra protección frente a atacantes que hacen escuchas, entonces para referirse a ellos se suele usar el nombre Eve (del término inglés eavesdropper, "fisgón") o bien el nombre Mallory, en caso de que el atacante, además de interceptar el mensaje, tenga la habilidad de alterarla.

Con frecuencia a los procesos de cifrado y descifrado se les denomina encriptado y desencriptado

2. Objetivos del proyecto

1. Realizar la programación de un programa en lenguaje ensamblador x86.
2. Familiarizarse con la nomenclatura del lenguaje, sus estructuras y tratamientos de bits como también las interfases del lenguaje ensamblador asm 8086.
3. Revisar los conceptos de encriptación/ desencriptación.
4. Manejo de bits a nivel del lenguaje ensamblador x86..
5. Cohesionar los conceptos anteriores con la materia del curso.

3. Proyecto

Debe programar la decodificación de un algortimo de encriptación/desencriptación para cualquier archivo que el usuario desee. (archivos binarios y de texto)

El programa debe pedir los parámetros por línea de comando y debe de opciones por defecto.

El progama debe de: tener la siguiente sintáxis:

c:>\encri [e|d] [/?|h] archivo [/n | /m | /l:LETRA] [clave] [/w]

Los párentesis son opciones como sigue:
e: encriptar.
d: desencriptar.
/?: ayuda.
/h o /H: ayuda.
archivo: nombre de archivo.
/n, /m, /l: método de encriptar/desencriptar.
clave: contraseña para cifrar máximo de 255 carácteres.
/w: debe escribir 0 en el archivo original para borrarlo sin recuperación.

Métodos de encriptar/desencriptar.
Para todos los métodos se debe de realizar un xor con bloques del archivo del tamaño de la clave entrada en los

parámetros y a ese texto se le debe de aplicar algúno de los siguientes métodos:

/n | /N: Usar tabla de conversión de caracteres en números usando algún sistema de codificación de caracteres como ASCII. Por ejemplo el mensaje "Hello World" usando ASCII queda: 72 101 108 108 111 32 87 111 114 108 100 (H=72 e=101 l=108 l=108 o=111 ' '=32 W=87 o=111 r=114 l=108 d=100). Pero se debe de escribir en el nuevo archivo como "litte end" por palabra así: olleH dlroW, en ascii.

/m | /M: Uso de una matriz de permutación: como sigue.

L_0

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8

R_0

57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

A las dos matrices de 32 se le aplica el xor con la clave de entrada y escribe la matriz R0 primero y luego la L0 en el nuevo archivo.

/l | /L, l:LETRA: Se aplica el mismo método que /n pero antes de aplicarle la numeración se hace una sustitución según la letra que se entre como parámetro, utilizando para ello el alfabeto español. Por ejemplo si se entra: /l:W entonces ahora la a=w, b=x, c=y, d=z, e=a… y luego se aplica el método /n.

4. Evaluación y medición

Programa	**20%**
funcionamiento	
Funcionamiento y Defensa	**80%**
NOTA FINAL	**100%**

5. Bibliografía complementaria

Se recomienda el primer y segundo item como referencia de bibliografía.

I. https://es.wikipedia.org/wiki/Data_Encryption_Standard

II. https://www.youtube.com/watch?v=1R7slgTyMOs

III. http://spi1.nisu.org/recop/al02/jgargallo/index.html

IV. http://serdis.dis.ulpgc.es/~ii-cript/PAGINA%20WEB%20CLASICA/CRIPTPGRAFIA%20MODERNA/DES.html

V. http://www.ia.urjc.es/cms/sites/default/files/userfiles/file/SEG-I/2011/DES_detallado.pdf

6. Disposiciones generales

1. Los fraudes en cualquier actividad llevada a cabo durante el semestre implicará que se perderá el curso y se reportará la nota mínima. Además se enviará una carta al expediente del estudiante.
2. Habrá defensa del mismo de forma individual.
3. El trabajo es de forma grupal en tríos de trabajo.
4. La entrega se hará el día asignado antes de las 1800 hrs.
5. En la documentación interna del programa.

7. Medios disponibles para consulta estudiantil

Las habituales del curso.