

el portafolio de evidencias debe incluir

EP1

EP2

AC 1

P1

PROGRAMA RSA


P2

P3

A CADA UNO DE ESTOS DOCUMENTOS ES NECESARIO COLOCAR LA DESCRIPCION
TITULO LO QUE SE DEBE APRENDER OBJETIVOS E INCLUYENDO UNAS
CONCLUSIONES ESTO DE TOCA UNA DE LAS ACTIVIDADES
ESTE UNO SOLO COMPENDIO DE ACTIVIDADES ES UN FORMATO LIBRE Y SE PUEDE
GUARDAR DE CUALQUIER FORMA

SE DEBE COLOCAR O CREAR UN REPOSITORIO CON TODAS LAS CARPETAS O
ACTIVIDADES

DEBE TRAER LA CARATULA INTRODUCCION O BIBLIOGRAFIA TODO

 **colocar los objetivos en base a los objetivos que se dejan en la carta descriptiva de la carrera**

esta cosa debe tener una organizacion de las actividades por temas y subtemas (segun la estructura del curso incluyendo para cada actividad el titulo de la actividad es decir un ejemplo puede ser una hoja con un titulo de la actividad con una descripcion debe de la actividad como si fuera una especie de indice)

se debe de contar con una reflexion personal y una bibliografia

la evidencia no es nada mas ni nada menos que lo que nosotros vamos o estamos haciendo

ya tenemos desde ahora la primera evidencia es decir es desde ahora empezar a realizar el documento del entregable

r

recuerda que es imperativo realizar este compendio si buscamos

nota no solo se busca un repositorio

carpeta general y dentro puedes colocar la actividad 1

o el entregable previo 1

dentro de la carpeta colocar una descripción y la evidencia

para cada actividad debe incluir el título de la actividad descripción

"Pasted image 20240921072852.png" could not be found.

si no se sube no se tiene un derecho de entregar la actividad final

safe assign debe tener un valor de menos de 25%

a excepción del de programación

se debe utilizar la bibliografía recomendada
y la materia no trae un entregable final

controles criptograficos de seguridad

que es la criptografía clásica

la criptografía clásica se refiere a los métodos tradicionales de cifrado usados desde la antigüedad hasta la era moderna

su propósito ha sido mantener la confidencialidad de la información usando técnicas de sustitución y transposición de caracteres

motivación y problemas en criptografía

seguridad de la información

se utiliza para proteger datos valiosos

comunicación segura en tiempos difíciles

transmisión de mensajes sensibles entre

motivación y problemas de criptografía

protección contra espionaje

las técnicas criptográficas previenen que información caiga en manos enemigas

vulnerabilidad al criptoanálisis

los métodos de cifrado pueden ser atacados

otras limitaciones de la criptografía es el avance de las tecnologías

la criptografía se basa en técnicas de cifrado que han sido utilizadas a lo largo de la historia proporcionando la base para la seguridad moderna

entre los desafíos destacados se encuentran la seguridad de los métodos de cifrado y la evolución de técnicas de criptoanálisis

los esquemas básicos de comunicación

en el proceso de comunicación en criptografía se incluyen 3 actores

emisor, receptor y atacante

se usa una clave para cifrar y descifrar el mensaje con distintos esquemas según se trate de criptografía simétrica o asimétrica

la criptografía ayuda en la parte de la confidencialidad

todas las comunicaciones modernas actualmente poseen un cifrado

la integridad es otro aspecto importante un documento no debe ser interceptado ni modificado

la criptografía también nos apoya en la sección de la disponibilidad

el no repudio es otro punto importante

es decir el autenticar que un mensaje solo puede ser emitido por una persona dada, es decir si el canal está cifrado tus palabras son responsabilidad tuya

la triada de la seguridad CIDA también contempla en el contexto de la criptografía la sección de no repudio

CIDAN

Máquinas como ENIGMA y SIGABA jugaron un papel crucial en la segunda guerra los cifrados como cesar y vigenere son otros ejemplos de cifrados clásicos que utilizan la criptografía por sustitución

la máquina enigma

utilizada

SIGABA FUE MAS UTILIZADA POR ESTADOS UNIDOS Y FUE MUCHO MAS SEGURA QUE ENIGMA UTILIZABA 5 ROTORES

EXISTE OTRA MAQUINA ELECTROMECHANICA LLAMADA TYPEX QUE SE CONSIDERABA AUN MAS SEGURA QUE ENIGMA

maquina de cifrado combinado (CCM)

fue utilizada por los aliados y fue clave en la encriptacion de mensajes secretos combinada con las características anteriores es decir era poligramica

el sistema utilizado por los japoneses era la maquina purpura

estas maquinas utilizaban una sustitucion monoalfabetica

es decir reemplazar cada letra del texto original con una letra diferente

este tipo de cifrado reemplaza cada letra del texto original con una letra diferente dada una regla fija

cifrado de alberti

es uno de los primeros cifrados polialfabeticos y fue desarrollado por leon battista alberti que utiliza alfabetos diferentes para crear un texto claro

polialfabetico -> es el que utiliza un

AEO

se trata de un cifrado clasico de sustitucion monoalfabetica basada en el desplazamiento de las letras de acuerdo con una clave en el alfabeto AEO el principio clave es que cada vocal aeo se convierte en una consonante para realizar el cifrado

sustitucion polialfabetica

en este metodo se introduce una clave de cifrado

vigenere es un ejemplo de ello

nombre y apellido paterno y clave sera apellido materno
solo tomar un nombre

cripto analisis de algoritmos clasicos

la criptografia esta intimamente ligada a la parte matematica

criptoanalisis de sustitucion polialfabetica

la sustitucion polialfabetica utiliza multiples alfabetos para substituir la letra del mensaje original
a diferencia del mensaje monoalfabetico el cifrado polialfabetico cambia de alfabeto en funcion
de una clave o regla

el cifrado vigenere es un ejemplo de esto sin embargo una forma de reanalizar el criptoanálisis
es

para poder realizar el criptoanálisis se utiliza el metodo de kersk

atravez de metodos estadísticos uno de los enfoques mas comunes incluye el analisis de
frecuencias e incidencias

prueba de kasinsky sirve para determinar la longitud de la clave

prueba de friedman metodo estadístico para estimar la longitud de la clave

indice de coincidencias compara la frecuencia de las letras en un idioma determinado

[Calculadora en línea: Prueba de Kasiski \(planetcalc.com\)](http://planetcalc.com)

con base a la longitud de la clave se hace un ataque de fuerza bruta para poder identificar el
texto

criptografia de sustitucion poligrafica

es una forma de cifrado en el que se substituyen bloques de letras del cifrado original en lugar
de las letras individuales este introduce un mayor nivel de complejidad y por lo tanto de
seguridad

un ejemplo de esto es el cifrado de hill

este metodo puede operar en 2 o mas bloques a la vez

existen otros metodos modulares que son fundamentales como el descifrado de RSA y
intercambio de claves Diffie Hellman que se basan en algoritmos modulares que involucran

operaciones aritmeticas donde el resultado es un residuo de una division

cifrado de hill:

es un tipo de cifrado de sustitucion poligrafica es decir que un bloque de letras se trata como un vector que se multiplica por una matriz clave

esta matriz debe ser invertible en el modulo del alfabeto

1. definir el vocabulario

A,B,C,D,E

1,2,3,4,5

2. DEBO DE VECTORIZAR LOS CARACTERES Y TENER UNA MATRIZ CLAVE

si quiero cifrar

ES DECIR LA MATRIZ DEBE ESTAR COMPUESTA POR LOS NUMEROS DE INDICES DEL VOCABULARIO

IA TEX

1,2,3 |

3,2,1 |

3,3,4 |

V

SE ACOMODAN DE ARRIBA A ABAJO DE IZQUIERDA A DERECHA

ES DECIR MI LLAVE SE ACOMODA EN UNA MATRIZ

MI PALABRA SE VECTORIZA

ABC -> {1,2,3}

ENTONCES TENGO UNA MATRIZ VECTOR

AHORA

EL VECTOR SE ACOMODA IGUAL COMO UNA MATRIZ

SI NUESTRO VECTOR FUERA

ABCDE y si te das cuenta excede el tamaño de nuestra matriz clave que es 3x3 entonces debemos de agregar lo para que complete el mxn

ABC D

1,4

2,0

3,0

o por ejemplo con unitec

UNITEC

21 13 8 20 4 2

[21 | 20]

[13 | 4]

[8 | 2]

UNA VEZ CON ESTO HECHO VAMOS A REALIZAR LA MULTIPLICACION CON LA MATRIZ DE NUESTRA LLAVE

2 16 6 21 20

18 20 18 * 13 4

8 15 0 8 2

PARA MOUTLIPLICAR DEBEMOS DE UTILIZAR

PARA DETERMINAR EL LARGO USAMOS

33 32 =

SI ES LA MSMA CANTIDAD DE FILAS Y COLUMNAS SE PUEDE MULTIPLICAR
ENTONCES COMO AQUI NOS E HACE SOLO SE PUEDE MLTIPLICAR DE LA MATRIZ
MENOR A LA MAYOR

EN OTRAS PALABRAS SOLO CON MULTIPLICAR OBTENEMOS EL CIFRADO

2 16 6 21 20

18 20 18 * 13 4

8 15 0 8 2

MSJ CIFRADO

21 20 2 16 6 298 116

13 4 18 20 18 = 782 476

8 2 8 15 0 363 220

MENSAJE CIFRADO Y CODIFICADO EN ABECEDARIO

298%26 116%26

782%26 476%26

363%26 220%26

AHORA PARA HACER QUE ESTE MENSAJE CIFRADO SE CONVIERTA A CARACTERES DEBEMOS UTILIZAR EL OPERADOR DE MODULAR PARA COLAPSARLO AL ABECEDARIO QUE UTILIZAMOS

PARA SACAR EL MODULO EN EXCEL USAMOS RESIDUO

ENTONCES AHORA VAMOS A DECODIFICAR EL MENSAJE

PARA DESCIFRAR DE LA MATRIZ LLAVE OBTENGO MATRIZ INVERSA
ESTO SE HACE CON LA FUNCION MINVERSA DE EXCEL

UNA VEZ CON LA MATRIZ PARA DESCIFRAR O INVERSA POR EJEMPLO

$-0.1 \ -0.11 \ -0.214 \ 298 \pmod{26} \ 116 \pmod{26} \ 3 \ 313$

$-0.33 \ -0.55 \ -0.2 \cdot 782 \pmod{26} \ 476 \pmod{26} = 255 \ 672$

$-0.33 \ -0.6 \ -0.7 \ 363 \pmod{26} \ 220 \pmod{26} \ -231 \ 313$

A TODOS LOS RESULTADOS LE APLICAMOS EL OPERADOR MODULAR

$3 \pmod{26} \ 313 \pmod{26}$

$255 \pmod{26} \ 672 \pmod{26}$

$-231 \pmod{26} \ 313 \pmod{26}$

ESTA OPERACION SOBRE CADA MODULAR NOS PRODUCIRA EL RESULTADO DETERMINADO

DEBEMOS DE HACER EL MISMO PROCESO ES DECIR MULTIPLICAR LA MATRIZ INVERSA POR EL MENSAJE

llave publica y privada y cifrado con rsa

los metodos modulares

son fundamentales en la criptografia moderna especialmente en sistemas de cifrado como RSA
el intercambio de claves de diffie helman

los calculos involucran operaciones en las que el resultado es la division de un modulo o el residuo de un divisor

teoria de numeros y numero de euler los numeros que son 1 son coprimos y cumplen esa condicion

lo que corresponde a que sea congruente a 1 con el modulo de $\phi(n)$

la aritmetica modular es util en criptografia por que permite trabajar con grandes numeros y garantiza que el resultado de una operacion se mantenga en un conjunto de numeros dados

el desarrollo del criptoanalisis, son altamente eficientes para un volumen de datos

los cifrados simetricos utilizan la misma clave para cifrar y descifrar los mensajes son altamente eficientes para grandes volúmenes de informacion

algunos ejemplos es el cifrado AES

estandar de cifrado avanzado

es uno de los algoritmos de cifrados mas utilizados a nivel mundial utilizado en un esquema de sustitucion y permutacion

TDES

aplica un algoritmo tres veces sobre cada bloque incrementando su seguridad utilizando claves de 56 bytes extendiendolos

IDEA ALGORITMO INTERNACIONAL DE ENCRIPCIÓN DE DATOS

UTILIZA CLAVES DE 128 BITS REALIZA OPERACIONES DE MECLA DE BIT A NIVEL MUNDIAL

BLOWFISH

ALGORITMO DE CLAVE SIMÉTRICAS

CON TAMANO DE 64 BITS Y CLAVES SIMÉTRICAS DE 32 A 448 BITS

ES ÚTIL EN SISTEMAS DE SOFTWARE

ES CONOCIDO POR SU VELOCIDAD Y EFICIENCIA

CIFRADORES DE BLOQUE

PUEDEN OPERAR O PERMITEN REUTILIZAR LAS CLAVES Y HACER MÁS RESISTENTES EL CIFRADO CONTRA ALGUN MODO DE ATAQUE

CD BLOQUE DE CÓDIGO ELECTRÓNICO CIFRADO DE BLOQUES INDEPENDIENTES NO TIENE ALEATORIEDAD POR LO QUE ES VULNERABLE A PATRONES REPETITIVOS

CBC

CIFRADO DE BLOQUE DE ENCADENAMIENTO CADA BLOQUE DE TEXTO CIFRADO SE ENCADENA CON EL ANTERIOR PARA EVITAR BLOQUES REPETITIVOS

OFB OUT FEEDBACK

RETROALIMENTACIÓN DE SALIDA

EN EL BLOQUE DE CIFRADO NO SE ENCADENA SINO QUE SE RETROALIMENTA UN VALOR CIFRADO QUE SE COMBIANC ON EL SIGUIENTE BLOQUE ESTE MODO CONVIERTE EL CIFRADOR DE BLOQUE EN UN CIFRADOR DE FLUJO

CIFRADORES RC2 RC4 RC5 Y RC6

FAMILIA RC ALGORIMOS DE CIFRADO

LA FAMILIA DE ALGORITMOS RC RIVEST CIPHER INVLUYE VARIOS CERTIFICADOS SIMETRICOS AMPLIAMENTE UTILIZADOS

RC4 ES UN CIFRADOR DE FLUJO MIENTRAS QUE RC5 Y RC6 SON CIFRADORES DE BLOQUE CON DIFRENTES CARACTERISTICAS

rc veerse cipher incluye cifradores simetricos

Criptografia hash

los algoritmos de hash generan un valor fijo apartir de un mensaje de cualquier longitud son clave en la verifcacion

SHA256 fue creado por la NSA

secure hashing algorihm 256 indica el numero de bits quue utiliza en la memoria siempre esta escrito en hexademimal y su cadenas de salida siempre es de 64 caracteres

propiedades hash

undireccional no se puede realizar una operacion inversa apartir del resultado

determinista (siempre da el mismo resultado en base al mismo contenido)

calculo rapido

efecto avalancha (es decir que si cambia un solo digito que cambie todo)

debe soportar coisiones (el teorema de las palomas hay 9 palomas pero en uno hay unhueco

el teorema de las palomas dice que debe haber una probabilidad muy baja de que una persona comparta las mismas características de las huellas difitales)

criptografia moderna

clave publica y metodos algoritmicos

metodo de cuadrados latinos

registros de desplazamiento

funciones en un solo sentido

matematicas faciles de calcular en una direccion pero dificiles de invertir y son usadas como RSA

ejemplo:

el problema de factorizar numeros grandes es que es facil de multiplicar pero dificil de descomponer

la llave publica

es un sistema de cifrado donde se usa una llave publica para cifrar y una privada para descifrar

esquema de Diffie-Hellman

protocolo permite a dos partes intercambiar una clave y se basa en la complejidad de calcular logaritmos secretos

Criptosistema de envio de Otway-Rees

procedimiento ElGamal

algoritmo de clave publica de Rabin

es muy similar a RSA la ventaja es que si alguien puede romper el cifrado tambien puede factorizar el numero

RSA

dados $n = pq$ donde p y q son 2 numeros primos distintos

$$n = 3 \cdot 11 = 33$$

$$n = p \cdot q$$

p y q son arbitrarios siempre y cuando sean numeros primos distintos

$$\text{para tener } \phi(n) = (p-1) \cdot (q-1)$$

$$\phi(n) = (3-1) \cdot (11-1) = 20$$

ahora hace falta determinar que el numero euler cumpla 2 condiciones

$$e = 1 < e < \phi(n) \text{ y}$$

e debe ser mayor que 1 y menor que $\phi(n)$

en base a ello entonces debemos buscar un numero que aplique esta regla:

$$\text{mcd}(e, \phi(n)) = 1$$

para determinar los numeros

"Pasted image 20240921113525.png" could not be found.

partimos del 2 por que e no puede ser menor o igual a 1 pero no se debe cumplir que sea el mcd de 20

entonces colocamos el 20 -1

el maxio comun division debe ser 1

la frmula dice que para que e cumpla las 2 condiciones

al tener como $\phi(N) = 20$ debemos ir revisando de 1 a 1 cada valor del e mayour a 1 es decir del 2 al 20

siempre se va a iniciar en 2 por que el teorema me dice que debe ser mayor a 1 y menor a phi de n

para encontrar el mcd de e y phi de n debe ser igual a 1

"Pasted image 20240921105251.png" could not be found.

entonces estamos buscando el numero primo de este rango numerico

"Pasted image 20240921105312.png" could not be found.

$$20 / 3 = 1$$

entonces el mcd si es 1 entonces debe ser 1

debe ser un numero primo

si pruebo por ejemplo con 2

mcd 2 y 20 me dan 1 ? no

entonces es el 3 y el 7

si

despues podemos ahora si sacar la formula

despues de que tenemos nuestro e en este caso 3

ahora debemos coprobar o buscar a d el cual no es mas que un numero que sea entero en el cual se aplique la formula

"Pasted image 20240921105828.png" could not be found.

podemos calcular la siguiente tabla

para determinar quien es d que es utilizada para determinar la clave privada

k publica $(n,e) = (33,7)$ en este caso

para determinar d

$d/e \cdot d \text{ converge } 1 \pmod{\phi(n)}$

$d = (1 + 1 \cdot 20)/7 = 3$ entonces r es 3

d = debe cumplir con unas condiciones el cual es que el resultado se a un entero

k privada $(n,d) = (33,3)$ d siempre debe ser un entero

con estos dos como clave publica y privada
basta con aplicar esta frmula:

RESIDUO(POTENCIA(letra;e);n)

$(22^7) \cdot 33$

la formula de cifra es

$Ci = m1^E \cdot (\text{MOD } N) = 7^7 \text{ mod } 33 = 28$

m1 es la letra de abecedario que ponga

descifrado

$CI = CI^d \cdot \text{mod } N$

$DI = CI^D \cdot \text{MOD } N$

PARA CIFRAR EN rsa SE REQUIEREN 2 NUMEROS PRIMOS DISTINTOS QUE SON Q Y P

q y p

$q = 3$

$p = 11$

entonce sen base de dello vamos a sacar el valor de n

$n = 3 \cdot 11 = 33$

ahora sacaremos el valor de phi

$\phi(n) = (p-1)(q-1) = 2 \cdot 10 = 20$

ahora es necesario sacar el numero e
qe debe cumplir

$e > 1$ y $e < \phi$

para ello armamos una tabla apartir de el numero maximo de phi -1
y 2 por que e no puede ser 1
ademas que $\text{mcd}(e \text{ y } \phi(n)) = 1$
es decir que el mcd de 1 de ambos

e	phi	mcd(e,phi(n))
2	20	
3	20	1

al ser 1 es que se cumple la condicion entonces usaremos 3

ahora es necesario utilizar o determinar la letra de K y d
para ello lo determinamos siendo k

"Pasted image 20240921115507.png" could not be found.

k es determinado en base a un numero
pero k no es finito solo debe ser un numero o un rango
por lo cal utilizamos numeros aleatorios en k para determinar d
 $d = (1 + 4(20))/3 = 27$
si k es 4

ahora con estos valores determino la clave publica y privada
k publica (33,3) (n,e)
k privada (33,27) (n,d)

ahora para cifrar

$ci = 26^3 \text{ mod}(33) = 20$
 $ci = \text{letra}^e \text{ mod } n$

descifrado

$d = ci^d \text{ mod}(n) = 20^{27} \text{ mod}(33) = 26$

practica 1 se entrega el
act clase 1 excel 27 sep
act cisco 27 sep