



## Examen Parcial

**CURSO:** SEGURIDAD Y PROTECCION INFORMATICA  
**GRUPO(s):** 1

**PROFESOR(s):** Ing. Yolanda Yopla

**FECHA:** 08 de Mayo del 2012

**HORA:** 20:00 hrs

**DURACION DEL EXAMEN:** 90 minutos

**DEVOLUCION DEL EXAMEN CALIFICADO/ Fecha:** 15/05/12

**Hora:** 19:00 **Aula:** 404

### IMPORTANTE:

- El examen es sin copias ni apuntes.
- Está prohibido el préstamo de calculadoras, correctores, uso de celulares, etc

---

**APELLIDOS Y NOMBRE:**

**CÓDIGO:**

---

1. Relacione los siguientes conceptos de seguridad ( 2.5 puntos):

( ) Denegación de Servicio

( ) Disponibilidad

( ) No Repudio

( ) Integridad

( ) Autenticación

( ) Confidencialidad

(A) Verificación que realiza el sistema sobre una identificación

(B) Asociado a la aceptación de un protocolo de comunicación entre emisor y receptor, normalmente a través el intercambio de certificados digitales de autenticación.

(C) Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informatico.

(D) La información puede ser modificada sólo por personal autorizado, es decir el sistema no debe modificar o corromper la información que almacena o permitir que alguien no autorizado lo haga.

(E) ataques que apuntan a afectar negativamente el funcionamiento de un servicio ofrecido por algún sistema o dispositivo de red.

2. Explique y dé ejemplos de las siguientes amenazas de seguridad (6 puntos):

- Ataques de Fuerza Bruta:
- Ingenieria Social:
- Ataques de Diccionario:

3. Relacione los protocolos con su correspondiente Nivel del modelo OSI ( 2.5 puntos):

( ) TCP, UDP

( ) X.21, HSSI

( ) ARP, PPP

( ) SSL, SQL

( ) HTTP, FTP, SMTP

( ) RIP, IP

(A) Nivel Sesión

(B) Nivel Red

(C) Nivel Transporte

(D) Nivel Aplicación

(E) Nivel Enlace

4. Haciendo uso del cifrado de alfabeto vertical, obtener el alfabeto cripto y cifrar el mensaje adjunto, considerando: Alfabeto Normal, Alfabeto de 26 caracteres, desplazamiento de 3 y clave = TRANSPORTE ( 3 puntos)

Mensaje a cifrar:

Una obra solo se completa cuando el objetivo es alcanzado

5. Haciendo uso de la tabla de Vigenère, cifrar el mensaje adjunto, considerando la clave=FRAME (3 puntos)

Mensaje a cifrar: Elegir un sendero implica abandonar otros.

6. Haciendo uso del cifrado de Cesar, con alfabeto de 27 caracteres, desplazamiento de 4, descifre el siguiente mensaje: (3 Puntos)

YQEZMHEWMQGEYWEIWYQEZMHEWMQIJIGXS

### TABLA DE VIGENERE

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y