Página Principal / Mis cursos / 2021-2K2-2-229 / 31 de Octubre - 06 de Noviembre / SEGUNDO PARCIAL PRÁCTICO - segundo cuatrimestre 2021 Turno 2	
	Tiempo restante 1:29:34

# Paradigmas de Programación Segundo Parcial Práctico

#### **Tema 3.3**

### Objetivo

Evaluar al estudiante en la parte práctica de las unidades nro. 4 y nro. 5 (Paradigma Funcional y Paradigma Lógico, respectivamente) a partir de la resolución que guarde en los archivos más abajo especificados, correspondientes a las consignas solicitadas para los ejercicios de cada paradigma.

### Condiciones de trabajo:

- El día pactado para el primer parcial en los horarios informados oportunamente, en el aula virtual de Moodle estará habilitada una actividad tipo cuestionario identificada como "2° Parcial Práctico".
- Una aclaración muy importante a tener en cuenta, es que si un estudiante desarrolla y entrega un programa que corresponde a un enunciado diferente al que le fue asignado, será reprobado.
- Este parcial práctico consta de dos partes: programación lógica y programación funcional. Para cada paradigma se deberá desarrollar un programa, utilizando el correspondiente entorno.
- Para resolver las consignas correspondientes al paradigma lógico, se deberá generar un archivo con el nombre Legajo\_ApellidoNombre.pl para definir los hechos y reglas que se soliciten en las consignas que se detallan más abajo.
- Para resolver las consignas correspondientes al paradigma funcional, se deberá generar un archivo con el nombre Legajo\_ApellidoNombre.hs para formular las funciones que se soliciten en las consignas que se detallan más abajo.
- Se aconseja copiar el enunciado al comenzar, para tenerlo disponible en caso de algún fallo de conexión durante el transcurso del mismo
- La duración prevista para el parcial es de 1:30hs, y comenzará en el horario asignado al curso correspondiente.
- Al finalizar el desarrollo del programa, el estudiante deberá subir los archivos .hs y .pl al cuestionario correspondiente al parcial, dentro de la hora de finalización especificada.
- Es responsabilidad de cada estudiante ir guardando periódicamente su archivo de trabajo, como así también del contenido de los mismos
- ACLARACION: El estudiante durante el transcurso del examen, no podrá tener dos instancias de UV abiertas y no puede salir del cuestionario sin finalizarlo correctamente, ya que la evaluación quedará invalidada.

# Paradigma Lógico

### **Enunciado**

Se han investigado durante el año 2020 más de 5000 muestras de ransomware (malware que encripta la información de un sistema y pide rescate) y se han identificado 10 familias de variaciones de ransomware, como se detalla a continuación:

A continuación se muestra en la tabla 1 las familias de ransomware existentes, ordenadas por la probabilidad de aparición:

Tabla 1: Familias de ransomware

Identificador	Nombre	Probabilidad	Fecha de aparición	Meses de campañas	
1	Grandcrab	78.5	10/01/2020	[enero,febrero,marzo,abril]	
2	Babuk	7.61	05/07/2020	[julio,agosto]	
3	Cerber	3.11	20/01/2020	[enero,febrero,diciembre]	
4	Matsnu	2.63	03/04/2020	[abril,octubre]	
5	Wannacry	2.41	29/06/2020	[junio,septiembre]	
6	Congur	1.52	05/07/2020	[julio]	
7	Locky	1.29	12/05/2020	[mayo,diciembre]	
8	Teslacrypt	1.12	04/11/2020	[noviembre,diciembre]	
9	Rkor	1.11	10/03/2020	[marzo,mayo]	
10	Reveton	0.70	29/08/2020	[agosto]	

La tabla 2 corresponde a los tipos de archivos mediante el cual se distribuyen los malware.

### Tabla 2: Tipos de archivos

Identificador	Tipo
1	Pe
2	Android
3	DII
4	Gzip
5	Javascript

Y por último, se sabe que los ransomware son distribuidos por troyanos a través de distintos tipos de archivos. La **tabla 3** muestra esta información:

**Tabla 3: Troyanos** 

Troyano	Detectable por firma	=	Ransomware que puede distribuir
Emotet	True	1	[2,3,4]
Ezbot	False	3	[6,1,10,2]
Edridex	False	5	[9,5,3]
Egozi	True	4	[7,10,4]
edanabot	True	2	[8,1,5]

#### Su tarea:

A partir de los hechos que se detallan a continuación, que representan todos los datos de las tablas 1,2 y 3.

#### **Hechos:**

%Familias de Ransomware

familia (1, grand crab, 78.5, fecha (10, 1, 2020), [enero, febrero, marzo, abril]).

familia(2,babuk,7.61,fecha(5,7,2020),[julio,agosto]).

familia(3,cerber,3.11,fecha(20,1,2020),[enero,febrero,diciembre]).

familia(4,matsnu,2.63,fecha(3,4,2020),[abril,octubre]).

familia(5, wannacry, 2.41, fecha(29, 6, 2020), [junio, septiembre]).

familia(6,congur,1.52,fecha(5,7,2020),[julio]).

familia(7,locky,1.29,fecha(12,5,2020),[mayo,diciembre]).

familia(8,teslacrypt,1.12,fecha(4,11,2020),[noviembre,diciembre]).

familia(9,rkor,1.11,fecha(10,3,2020),[marzo,mayo]).

familia(10,reveton,0.70,fecha(29,8,2020),[agosto]).

%tipos de archivos

tipos(1,pe).

tipos(2,android).

tipos(3,dll).

tipos(4,gzip).

tipos(5,javascript).

%Malware detectable por firma que lleva ransomware

malware(emotet,true,1,[2,3,4]).

malware (ezbot,false,3,[6,1,10,2]).

malware (edridex,false,5,[9,5,3]).

malware (egozi,true,4,[7,10,4]).

malware (edanabot,true,2,[8,1,5]).

### **Requerimientos:**

Usted deberá definir las reglas que permitan resolver lo siguiente:

- 1) Conocer si existe algún ransomware que haya aparecido entre Junio del 2020 y cuya probabilidad de aparición se encuentre entre 2 y 3%. Predicado sugerido para esta regla: **regla1**. (15 puntos)
- 2) Mostrar el o los nombres de malware y tipo de archivo que distribuye el ransomware Teslacrypt, que sea detectable por firma y que además distribuya por lo menos 3 ransomware. Predicado sugerido para esta regla: regla2/2. (15 puntos)
- **3)** Genere una lista con todos los nombres (no repetidos) de ransomware que hayan tenido actividad en Marzo pero no en Mayo, o que haya tenido actividad en Diciembre y cuyo malware no sea detectable por firma. Predicado sugerido para esta regla: regla3/1. **(20 puntos)**

# <u>Paradigma Funcional</u>

#### **Enunciado**

En relación con los troyanos que distribuyen ransomware, nos ha solicitado además el desarrollo de un programa en Haskell.

#### Requerimientos

Usted deberá definir las funciones que permitan resolver lo siguiente:

1) Realizar una función que reciba el nombre de un troyano y devuelva la probabilidad de que distribuya el ransomware Rkor. En el caso de que el nombre del troyano no se encuentre especificada en la tabla 1, la función deberá retornar un mensaje "no definido". (15 puntos)

Tabla 1: Troyano para un determinado ransomware

Troyano	Rkor (probabilidad que se distribuya)
Emotet	7.5
Ezbot	8
Edridex	22
Egozi	51
Edanabot	11.5

- 2) Dada una lista de nombres de troyanos, generar una nueva lista por comprensión o recursividad de todos aquellos troyanos que puedan distribuir el ransomware Rkor con una probabilidad que este comprendida entre 15% y 20%. (15 puntos)
- **3)** Dada una lista con los valores de probabilidades que se distribuya el ransomware Rkor, realizar la sumatoria de dichas probabilidades que se encuentren comprendida entre dos valores límites pasados como argumentos. Para resolver este punto debe definir una función recursiva. **(20 puntos)**

### Tabla de valoración de los ítems evaluados

Ítems a Evaluar	Pje	Observaciones	Obtenido
Implementación de la regla 1.	15		
Implementación de la regla 2.	15		
Implementación de la regla 3.	20		
Implementación de la función 1.	15		
Implementación de la función 2.	15		
Implementación de la función 3.	20		
Total	100		

Tamaño máximo para archivos nuevos: 500MB



Tipos de archivo aceptados

Todos los tipos de archivo

■ Haskell\_parcial2017\_ RESUELTO