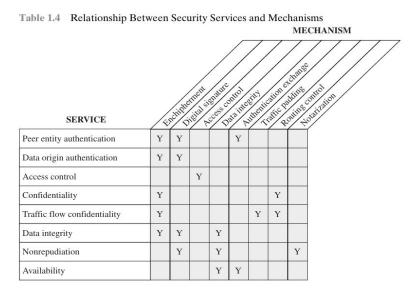
# C6-P1. Introducción a la seguridad informática

### • Elija SOLO UNA de las siguientes actividades

- a. Realice una matriz similar a la Tabla 1.4 que muestre la relación entre los <u>servicios</u> de seguridad y los tipos de ataque.
- b. Realice una matriz similar a la Tabla 1.4 que muestre la relación entre los mecanismos de seguridad y los tipos de ataque.





Nombre: Alberto Rodríguez Z.

RUT: 19.950.454-1

# C6-P1 Relación entre servicios y tipos de ataque

La matriz de la siguiente diapositiva muestra que servicio se encarga de cierto tipo de ataque. Se marca con un "Y" si este servicio ayuda a evitar ese tipo de ataque.



# C6-P1 Matriz

Tipos de Ataques

	Ataques Pasivos		Ataques Activos			
Servicios	Divulgación del contenido del mensaje	Análisis de tráfico	Mascarada	Replay	Modificación de mensajes	Denegación del servicio
Autenticación de entidad par			Y	Y		
Autenticación del origen de los datos			Y			
Control de acceso			Y			
Confidencialidad de datos	Y					
Confidencialidad del flujo de tráfico		Y				
Integridad de los datos				Y	Y	Y
No repudio			Y	Y		
Disponibilidad						Υ

## C6-P2. Criptografía clásica

- Encripte su primer nombre y primer apellido usando un cifrado Playfair y una llave K. Obtenga la llave K con el siguiente procedimiento:
  - a. La llave K está encriptada con un cifrado Playfair y llave J = "cipher"
    - La llave K encriptada es "UPEOACYH"
  - b. Determine K y diseñe su cifrado Playfair. Muestre la matriz que generó para cifrar.
  - c. Encripte su nombre y primer apellido con la llave K

Hint: Para evaluar los revisores deben ser capaces de desencriptar su nombre y apellido a partir de su texto cifrado y la llave K conocida



### C6-P2

Lo primero que se debe hacer es saber cual es la llave K, la cual encriptada es "**UPEOACYH**". Para poder desencriptarla se usa el cifrado PlayFair, cuya llave J = "cipher". Entonces la matriz es la siguiente. (Se deja afuera la letra J al hacer la matriz).

#### Matriz con llave J

С	I	Р	Н	E
R	Α	В	D	F
G	K	L	М	N
0	Q	s	Т	U
V	W	Х	Υ	Z

Entonces al tener la matriz y al realizar el algoritmo, al descifrar la llave K, se obtiene que la llave K = SECURITY

### Matriz con llave K

S		Е	С	U	R
I		Т	Y	А	В
D		F	G	Н	K
L		М	N	0	Р
0	PARTAMENT VGEN VFOF	PE <b>Y</b> IIERÍA IMÁTICA	W	Х	Z

Ya con la llave K se realiza la matriz de cifrado, la cual es la que está a la izquierda. Ahora con esa matriz vamos a encriptar mi nombre (Alberto) y primer apellido (Rodriguez). Al realizar el algoritmo se obtiene que:

- -Mi nombre encriptado: **IOTREBXU** (Mi nombre tiene 7 letras, entonces al ser impar, el último par sería ox, y al encriptarlo da XU. Un dato curioso es que los pares BE y RT, en esta matriz al encriptarlo, toman los valores del otro pero en orden inverso, BE=TR y RT=EB)
- -Mi apellido encriptado: **UPKSYDRCQZ** (Al igual que en el caso anterior, al mi apellido ser impar, el último par sería ZX, que al encriptarlo sería QZ).

Al desencriptar el nombre y el apellido se obtendrá, ALBERTOX Y RODRIGUEZX, lo cual por lógica se sabe que las X no se deben considerar y se obtendrá de nuevo la información.