

C6-P1. Introducción a la seguridad informática

- Elija **SOLO UNA** de las siguientes actividades

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

Table 1.4 Relationship Between Security Services and Mechanisms

SERVICE	MECHANISM							
	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Nonrepudiation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y					Y		
Traffic flow confidentiality	Y				Y	Y		
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

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

Servicios	Ataques Pasivos		Ataques Activos			
	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						Y



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 descryptarla 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

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