UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERIA
ESCUELA DE ELECTRÓNICA

Asignatura:	**Diseño de sistemas de seguridad en redes de datos**	Código:	**DSS101**
Grupos:	**01T**	Ciclo / año:	**02 - 2025**

Documento de investigación
"Implementación de algoritmo de cifrado polimórfico"

Condiciones de realización:

Fecha de Entrega:	**08 - 13 de septiembre del 2025 (Semana 11)**
Porcentaje:	15% nota de teoría.
Forma de Entrega:	Documento con el código fuente de la implementación adecuadamente descrito y presentación de la solución para mostrar el funcionamiento del algoritmo.
Grupos:	4 personas

Descripción de la actividad:

Basado en el trabajo descrito en el artículo técnico "Cryptography model to secure IoT device endpoints, based on polymorphic cipher OTP". Y después de un análisis a profundidad de su funcionamiento se requiere que se desarrolle lo siguiente:

a. Implementar el algoritmo para tamaños de llave de 64bits usando un lenguaje de programación de mediano nivel como Python o C++.
b. Evaluar la calidad de la generación de llaves de cifrado en cada punto final basado en el número de llaves especificadas.
c. La selección de las funciones descritas en el artículo es libre, pero deben documentarse las propuestas por el grupo.
d. Debe probarse con los dos programas el adecuado cifrado/descifrado de los mensajes recuperando el mensaje original en el receptor.
e. Debe probarse el adecuado funcionamiento de los tipos de mensajes intercambiados por los puntos finales.

Lista de estimación:

Actividad a evaluar	Criterio a evaluar	Porcentaje (%)	Puntaje (0-10)
Contenido del documento del experimento de investigación	El documento presenta: introducción, objetivo, conclusiones y referencias.	10	
	Describe claramente las funciones esenciales del algoritmo propuesto.	15	
	Documenta de manera clara el código fuente (enlace del código en un repositorio).	15	
Funcionamiento del programa desarrollado	Genera las tablas de llaves eficientemente	20	
	Cifra/descifra claramente los mensajes intercambiados	20	
	Implementa todos los tipos de intercambio de mensajes propuestos por el algoritmo	20	
		Promedio:	