Proyecto de investigación y aplicación

I. Competencias a desarrollar:

Identificar y explotar características de paralelización potencial en algoritmos utilizando pthreads. Resuelve problemas que involucran modelo de programación paralela y métodos de sincronización. Ejecuta operaciones implementando variables mutex y variables de condición.

II. Instrucciones:

Los estudiantes deberán:

- Analizar el algoritmo Data Encryption Standard (DES) para realizar el diseño de su algoritmo.
- Formar **grupos** de **dos** integrantes.

Cada grupo implementará el diseño de un nuevo algoritmo (de su propia autoría) para encriptación (a realizar por el estudiante A) y desencripción (a realizar por el estudiante B) de mensajes de tamaño variable, de forma paralela, usando pthreads, variables mutex y condicionales. El método básico de programación paralela a implementar es PThreads, adicionalmente cada integrante del grupo deberá implementar dentro del desarrollo de código un mecanismo sincronización establecido.

SINCRONIZACIÓN ENCRIPCIÓN	SINCRONIZACIÓN DESENCRIPCIÓN
Mutex	Condicionales

RESTRICCIONES:

- Los mensajes deben tener una longitud mínima de 70 caracteres.
- La cantidad mínima de rondas Feistel para encripción debe ser 2.
- Todos los integrantes deberán estar de acuerdo en el diseño del algoritmo.

III. Condiciones y fechas de entrega:

Entrega Preliminar: martes 24 de septiembre.

1. **Material a entregar en *Blackboard*:**
    a. Informe de antecedentes algoritmos DES, diagrama de flujo preliminar de proyecto, catálogo de funciones principales de programa.
    b. Avances de código fuente.

Entrega Final y presentación: jueves 03 de octubre.

2. **Material a entregar en *Blackboard*:**
    a. Informe del proyecto de investigación en formato PDF, siguiendo las normas para informes en formato pdf, no impreso.
    b. Código fuente.
3. **El día de la presentación:**
    a. El estudiante A recibirá un mensaje aleatorio que deberá ser encriptado.
    b. El estudiante B deberá descifrar el mensaje encriptado y entregarlo como prueba de funcionamiento,

IV. Lista de cotejo para Evaluación

	Aspectos a cumplir	Puntos
Entrega 1 (Total: 35 puntos)		
1	Informe de investigación y proceso de diseño. Incluye: - Especificaciones necesarias de algoritmo DES - Información sustentada y confiable - Sigue completamente las normas para informes: carátula, contenido o índice, introducción, texto o cuerpo, citas textuales, notas al pie, conclusiones de los conceptos más significativos, bibliografía de mínimo 3 fuentes confiables en el formato correcto.	10
2	Diagrama de flujo	8
3	Catálogo de funciones	7

	Aspectos a cumplir	Puntos
Entrega Final (Total: 65 puntos)		
1	Informe de investigación y proceso de diseño. Incluye las mejoras o correcciones: - Especificaciones necesarias de algoritmo DES - Información sustentada y confiable - Marco teórico no superior a 5 hojas - Sigue completamente las normas para informes: carátula, contenido o índice, introducción, texto o cuerpo, citas textuales, notas al pie, conclusiones de los conceptos más significativos, bibliografía de mínimo 3 fuentes confiables en el formato correcto.	10
2	Funcionamiento de programa	45
3	Documentación y comentarios	5
4	Orden del programa	5
5	Uso de método de sincronización asignado	10
6	% de conocimiento (la nota final obtenida se multiplicará por el porcentaje de conocimiento del estudiante y la calificación de los compañeros, obtenida de las coevaluaciones)	