PROYECTO 3

Criptografía

Instituto Tecnológico de Costa Rica
Escuela de Ingeniería en Computadores
Algoritmos y Estructuras de Datos II (CE 2103)
II Semestre 2024

Objetivo General

- ➔ Aplicar algoritmos de criptografía, corrección o detección de errores.

Objetivos Específicos

- ➔ Plantear una propuesta de investigación.
- ➔ Ejecutar una metodología de plan de investigación.
- ➔ Analizar los datos obtenidos en el desarrollo de la investigación.
- ➔ Elaborar conclusiones a partir de la síntesis y análisis de los resultados de la investigación.

Descripción del Problema

Mediante el desarrollo de este proyecto, el estudiante aplicará los conceptos de algoritmos de criptografía, corrección o detección de errores, mediante la propuesta y ejecución de un proyecto de investigación en un tema innovador o relevante.

Atributos relacionados

A continuación, se describen los atributos del graduado que se pretenden abordar con el desarrollo del proyecto.

- **Investigación (IN)**
  Capacidad para conducir investigaciones de problemas complejos por medio de conocimientos y métodos apropiados, incluyendo el diseño de experimentos, análisis e interpretación de datos y síntesis de información para proveer conclusiones válidas.

Descripción General

La investigación está presente en todos los ámbitos ya que la idea principal es documentar el conocimiento adquirido a través de los proyectos. Llevar un proyecto a ejecución conlleva una serie de estudios en temas innovadores para generar una propuesta. Esta propuesta debe ser valorada y aprobada por un comité técnico que determinará si el proyecto es apto para realizarse.

Este proyecto simulará la propuesta de un proyecto y la ejecución de este dentro del área de algoritmos de criptografía, corrección o detección de errores. Cada grupo podrá estar conformado por 3 o 4 estudiantes y el alcance dependerá de la cantidad de miembros en el grupo.

La primera fase del proyecto consistirá en una formulación de la propuesta de investigación la cual debe seguir un formato similar al solicitado en el TEC. Esta formulación analiza a detalle el problema que se quiere resolver. El problema por resolver debe ser de un escenario real mediante la aplicación de algoritmos de criptografía, corrección o detección de errores. Todo tema deberá ser aprobado primero por el profesor. Pueden proponer su propio tema, siempre y cuando sea innovador o relevante. La propuesta debe reflejar los posibles enfoques de solución basados en un estado del arte y la metodología que se planea seguir.

La segunda fase corresponde a la ejecución de la propuesta basándose en la metodología establecida. Se espera que se documente cada paso y se realice un análisis detallado de los resultados obtenidos.

A continuación, se describirá con mayor detalle ambas fases.

Propuesta de proyecto de investigación

Esta etapa consiste en la elaboración de una propuesta de proyecto de investigación sobre un problema que los estudiantes deben elegir. La solución a dicho problema debe relacionarse con algoritmos de criptografía, corrección o detección de errores. El tema deberá poseer una componente relevante o innovadora. Los componentes del documento se basan en la guía de presentación de proyectos estudiantiles de la Vicerrectoría de Investigación y Extensión (VIE). Las partes del documento son:

1. **Descripción general del proyecto:** debe explicar claramente en qué consiste el proyecto que pretende desarrollar. Debe referirse a las condiciones y antecedentes que originan el proyecto, definir con claridad y precisión el problema que se pretende estudiar. (máximo una página, tamaño de letra 10 puntos, espacio sencillo)
2. **Justificación:** Debe incluirse un planteamiento coherente que justifique la necesidad de resolver el problema planteado, la pertinencia de este y el abordaje que se propone. Además, cuando se trate de una investigación aplicada o un desarrollo experimental, se debe identificar los beneficiarios potenciales de los resultados del proyecto y explicar los beneficios económicos, tecnológicos y sociales tanto del (los) grupo (s), beneficiario (s), como para el país. Tómese en consideración las políticas nacionales e institucionales vigentes y las prioridades de desarrollo establecidas. (máximo una página, tamaño de letra 10 puntos, espacio sencillo).
3. **Marco Teórico/Estado del Arte:** Se debe realizar una revisión bibliográfica pertinente y actualizada en relación con el tema del proyecto, a partir de lo cual se deberá condensar lo más avanzado y relevante para el proyecto. Debe utilizar al menos 8 fuentes bibliográficas diferentes, provenientes de revistas y artículos científicos y / o libros (no se aceptarán como fuentes páginas web), con máximo 10 años de antigüedad. Las referencias y citas deberán realizarse correctamente de acuerdo a algún formato establecido (IEEE, APA, etc). (máximo dos páginas, tamaño de letra 10 puntos, espacio sencillo).
4. **Objetivos:** defina claramente los objetivos (generales y específicos) que se desean alcanzar. Es importante establecer la concordancia entre el problema que se estudia y los objetivos a lograr.
5. **Metodología:** Debe detallarse, de acuerdo con los objetivos planteados, posibles enfoques de solución, la técnica de recolección, sistematización y análisis de la información, incluyendo las suposiciones que se hacen en cada caso. Refiérase a los equipos y técnicas utilizadas en la

recolección y análisis de los datos, específicamente a las técnicas de muestreo, diseño experimental, análisis estadístico, etc. Es importante plantearla con un alto grado de detalle, capaz de ser evaluada científicamente, explicando claramente que va a realizarse y de qué manera.

6. **Plan de Acción:** Para cada objetivo específico, indique el producto o productos a obtener, las actividades que deben llevarse a cabo para lograrlos, el período en el que se realizará cada una de las actividades y el/la responsable de su ejecución. Utilice una tabla para la presentación del plan.
7. **Definición del cronograma:** Debe adjuntarse un cronograma que muestre la secuencia de las diferentes actividades del proyecto y los tiempos de duración.
8. **Divulgación y transferencia de tecnología:** Debe definir las acciones y medios que emplearía potencialmente para divulgar o transferir los resultados de la investigación.
9. **Presupuesto:** Debe incluir el presupuesto detallando cada uno de los insumos y sus respectivos precios. Justificar cada una de las partidas.

Evaluación y entregables

Esta evaluación tiene un valor de 5% del total del Proyecto 3. El entregable corresponderá al documento con las secciones descritas anteriormente. **No se aceptarán propuestas de temas de investigación sin la aprobación del profesor.**

Ejecución de la propuesta de investigación

Para ejecutar la propuesta, se debe llevar un registro escrito de todos los pasos y decisiones tomadas durante el desarrollo de la metodología establecida. También se deben documentar problemas encontrados, cambios y soluciones realizadas. Los detalles de la ejecución de la implementación se colocarán en un informe ejecutivo de máximo 6 páginas en el que se muestren las evidencias de cada una de las etapas definidas. El informe debe contener una introducción en la que se establezca el contexto del problema y mencione el enfoque elegido para la solución. El desarrollo del informe se debe estructurar por etapa de la metodología y debe contener las evidencias del a ejecución de esta (incluyendo el análisis de los datos). Finalmente, se deberá mostrar una sección de conclusiones en las que se discute la elección de la metodología seguida, así como posibles mejoras y cambios que deban realizarse.

Evaluación y entregables

La defensa será el mismo día de la entrega y todos los archivos (incluyendo código fuente) serán entregados a las 11:59 pm ese mismo día. Se evaluarán aspectos técnicos, así como estructura, orden, redacción y ortografía. **No se aceptarán informes ejecutivos de temas que no hayan sido aprobados por el profesor.** La evaluación del proyecto se da bajos los siguientes rubros contra rúbrica correspondiente:

- **Propuesta de investigación (5%)**
- **Presentación proyecto 100% funcional (5%):** cada grupo deberá demostrar en una sesión (previa cita con el profesor) de 20 minutos los diferentes componentes del proyecto. El profesor evaluará las pruebas según rúbrica correspondiente. En la sesión se harán preguntas relacionadas sobre cualquier etapa del sistema. Se habilitará un espacio en el tec digital para colocar un enlace del repositorio con el código fuente del proyecto.
- **Informe ejecutivo (5%):** Este documento se debe tener una extensión entre 5 y 6 páginas con los

siguientes componentes: Introducción, Desarrollo de metodología y Conclusiones.

Aspectos operativos y evaluación:

1. **Fecha de entrega: De acuerdo con el cronograma del curso y lo establecido en el TEC Digital**
2. El proyecto tiene un valor de 15% de la nota del curso.
3. El trabajo es **en grupos de 3-4 personas.**
4. La propuesta y el resumen ejecutivo deberán desarrollarse en Latex.
5. Deben entregar un documento con el link del repositorio de GitHub y el PDF de la documentación. Deben dar acceso al correo del profesor.
6. Es obligatorio utilizar un Git y GitHUB para el control de versiones del código fuente y evidenciar el uso de Commits frecuentes.
7. Es obligatorio integrar toda la solución.
8. Se evaluará que la documentación sea coherente, acorde a la dificultad/tamaño del proyecto y el trabajo realizado. Se recomienda que realicen la documentación conforme se implementa el código.
9. La nota de la documentación externa es proporcional a la completitud del proyecto.
10. Las citas de revisión oficiales serán determinadas por el profesor durante las lecciones o mediante algún medio electrónico.
11. Los estudiantes pueden seguir trabajando en el código hasta 15 minutos antes de la primera cita de revisión oficial.
12. Aún cuando el código y la documentación externa tienen sus notas por separado, se aplican las siguientes restricciones
    a. Si no se utiliza un manejador de código se obtiene una nota de cero en la nota final del proyecto.
    b. Si la documentación externa no se entrega en la fecha indicada se obtiene una nota de cero en la nota final del proyecto.
    c. Sí el código no compila se obtendrá una nota de cero en la nota final del proyecto, por lo cual se recomienda realizar la defensa con un código funcional.
    d. El código debe ser desarrollado en C++ (Linux), en caso contrario se obtendrá una nota de cero en la nota final del proyecto.
13. La revisión de la documentación podría ser revisada antes, durante o después de la cita de revisión del proyecto.
14. Cada excepción o error que salga durante la ejecución del proyecto y que se considere debió haber sido contemplada durante el desarrollo del proyecto, se castigará con 2 puntos de la nota final del proyecto.
15. Cada grupo es responsable de llevar los equipos requeridos para la revisión, si no cuentan con estos deberán avisar al menos 2 días antes de la revisión al profesor para coordinar el préstamo de estos.
16. Durante la revisión únicamente podrán participar el estudiante, asistentes, otros profesores y el coordinador del área.