|  |  |
| --- | --- |
| **Descripción: Descripción: escudo u de a** | **PROGRAMA OFICIAL DE CURSO** |
| **UNIVERSIDAD DE ANTIOQUIA** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **INFORMACIÓN GENERAL** | | | | | | | | | | | | |
| **Unidad Académica:** | | | Facultad de Educación | | | | | | | | | |
| **Programas académicos a los cuales se ofrece el curso:** | | | | | | Licenciatura en Matemáticas | | | | | | |
| **Vigencia:** | 2023-I | | | | | | | **Código curso:** | |  | | |
| **Nombre del curso:** | | | Electiva en Matemáticas II | | | | | | | | | |
| **Área o componente de formación del currículo (pregrado):** Saber específico y disciplinar | | | | | | | | | | | | |
| **Área o componente de formación del currículo (posgrado):** Elija un elemento. | | | | | | | | | | | | |
| **Tipo de curso:** | | Teórico - práctico | | | **Créditos académicos**[[1]](#footnote-0)**:** | | | | | | 3 | |
| **Características del curso:** Validable ☐ Habilitable ☐ Clasificable ☐ Evaluación de suficiencia ☐ | | | | | | | | | | | | |
| **Modalidad del curso:** Presencial | | | | | | | | | | | | |
| **Pre-requisitos:** | | | Fundamentos de Aritmética: Cantidades y Magnitudes (2096132) | | | | | | | | | |
| **Co-requisitos:** | | | Co-requisitos con nombre y código MARES. | | | | | | | | | |
| **Horas docencia directa:** 80 | | | | |  | | **Horas de trabajo independiente:** | | | | | 64 |
| **Horas totales del curso:** 144 | | | | | | | | | | | | |
| **Profesor(a) que elaboró:** Yuber Tapias  **Revisó y actualizó:** | | | | **Correo electrónico:** | | | | | yuber.tapias@udea.edu.co | | | |

|  |
| --- |
| 1. **INFORMACIÓN ESPECÍFICA** |
| **Descripción general y justificación del curso:** |
| El espacio académico *Electiva en Matemáticas II* se articula con los propósitos de formación del programa de Licenciatura en Matemáticas que apuntan a promover el conocimiento de los desarrollos de la ciencia y la tecnología. Además, atiende a un propósito general de la Facultad de Educación que propone formar maestros investigadores que innoven en pro de una educación digna y solidaria.  La *Electiva en Matemáticas II* destaca la importancia para los docentes en formación del estudio de teoremas, algoritmos y herramientas que posibilitan el desarrollo de habilidades para construir y analizar cálculos y procesos de automatización en los ejercicios de cifrado y descifrado, puesto que contribuyen a que los ciudadanos reconozcan el aporte de las matemáticas al ciudado de valores vitales en la sociedad tales como la seguridad y la privacidad.  La Licenciatura en Matemáticas busca una formación intelectual, reflexiva y ética, que promueva sujetos con responsabilidad política y es por ello que se propone un espacio para reflexionar sobre la criptografía y su enseñanza desde las matemáticas, dado que el análisis de nociones tales como *sistema de clave pública, intercambio de claves, moneda digital, entre otras,* permite a los docentes en formación fomentar valores éticos en el tratamiento de la información. |
| **Objetivo general:**  Reflexionar en torno a la enseñanza y aprendizaje de la criptografía con miras a promover sujetos con valores éticos y responsabilidad política. |
| **Objetivos específicos:**   * Reconocer el desarrollo histórico y teórico de la criptografía, para vincularlo con la práctica de la enseñanza y el aprendizaje de las matemáticas. * Desarrollar habilidades técnicas para implementar sistemas criptográficos con diferentes niveles de seguridad, para promover el estudio teórico-práctico de las matemáticas. * Reflexionar sobre la incidencia de la criptografía en prácticas cotidianas de comercio electrónico y tratamiento de la información, para promover en los docentes en formación posturas críticas frente a la ciberseguridad. |

|  |
| --- |
| **Contenido:** |
| **Eje Problémico 1**. Preliminares en Python.  **Pregunta(s) orientadora(s)**: ¿Cómo se declaran funciones en Python y cómo se pueden usar para automatizar procesos algebraicos? ¿Cómo respaldar en la nube procesos hechos en Python de forma que se puedan reeditar de manera colaborativa? ¿Cómo resolver problemas aritmético-algebraicos en forma automática con el módulo sympy.ntheory?  **No. de sesiones**: 5 sesiones de 2 horas (10 h).   * Cuadernos de Google Colab. * Tipos de datos, variables y arreglos en Python. * Funciones y clases. * Módulo sympy.ntheory.   **Eje Problémico 2**. Cifrados por sustitución.  **Pregunta(s) orientadora(s)**: ¿Por qué el algoritmo de la división y el cálculo con residuos se ajustan a modelar los cifrados por sustitución? ¿Cómo el criptoanálisis basado en distribuciones de frecuencias puede integrar la enseñanza y el aprendizaje de la aritmética y la estadística? ¿Cuáles son las debilidades en seguridad que presentan los cifrados por sustitución?  **No. de sesiones**: 7 sesiones de 2 horas (14 h).   * Divisibilidad y números primos. * Congruencias y aritmética modular. * Los teoremas de Fermat y Euler. * Cifrados por sustitución y su ataque con criptoanálisis por frecuencias.   **Eje Problémico 3**. Cifrado de clave pública RSA (Rivest, Shamir y Adleman).  **Pregunta(s) orientadora(s)**: ¿Hace parte de la formación en la componente lógica de un docente en matemáticas, el reconocimiento de la importancia de los números primos? ¿Favorece al desarrollo del pensamiento computacional la implementación de estrategias o atajos en los cálculos, promoviendo nuevas representaciones de los números enteros (por ejemplo: binario)? ¿Cuáles son las ventajas de usar números compuestos grandes que factoricen únicamente como producto de exactamente dos números primos? ¿Cómo se puede usar a favor de la seguridad en criptografía, el hecho de que un problema de factorización de un número entero grande y de pocos divisores, sea computacionalmente exigente?  **No. de sesiones**: 7 sesiones de 2 horas (14 h).   * Algoritmo para calcular potencias y raíces. * Firmas digitales. * RSA como cifrado de clave pública. * Ataque al RSA.   **Eje Problémico 4**. Funciones aritméticas. Raíces primitivas y logaritmos discretos.  **Pregunta(s) orientadora(s)**: ¿Puede el ordenamiento en tablas de cálculos aritméticos fomentar el reconocimiento de patrones antes de la formalización con teoremas? ¿Pueden las representaciones gráficas de funciones aritméticas y cálculos aritméticos anticipar procesos de formalización con teoremas? ¿Cuáles son las formas de resolver algunas ecuaciones en aritméticas módulo un número primo?  **No. de sesiones**: 5 sesiones de 2 horas (10 h).   * Las funciones de Euler y Möbius. * Raíces primitivas. * Logaritmos discretos. * Reconocimiento de patrones previos a la Ley de Reciprocidad Cuadrática.   **Eje Problémico 5**. Criptosistemas ElGamal y Rabin.  **Pregunta(s) orientadora(s)**: ¿Es la creación de criptosistemas un problema de aplicación que revela la pertinencia de la enseñanza y el aprendizaje de estructuras algebraicas? ¿Cómo puede la interdisciplinariedad con el álgebra promover criptosistemas más seguros?  **No. de sesiones**: 5 sesiones de 2 horas (10 h).   * Intercambio de claves Diffie-Hellman. * Criptosistema ElGamal. * Ley de reciprocidad cuadrática. * Criptosistema Rabin.   **Problémico 6**. Historia reciente de criptografía y responsabilidad política.  **Pregunta(s) orientadora(s)**: ¿Es el impacto ambiental la única preocupación de los gobiernos ante la inminente creación de monedas digitales? ¿Puede el análisis crítico de la historia reciente de la criptografía, favorecer a la formación intelectual, reflexiva y ética de los docentes en formación de la Licenciatura en Matemáticas?  **No. de sesiones**: 3 sesiones de 2 horas (6 h).   * Satoshi Nakamoto: Bitcoin P2P e-cash. * Activistas digitales Cyberpunk (protección de la privacidad). * “Cripto invierno” ¿Son las criptomonedas una burbuja? * Criptografía VS Otros servicios en internet. Alto impacto ambiental. * Euro digital, Dólar digital y Yuan digital. (¿Regulación?). |

|  |
| --- |
| 1. **METODOLOGÍA** |
| El espacio está programado para ser desarrollado en dos encuentros semanales de dos horas cada uno en docencia directa y una hora de docencia asistida. La comunicación continua, así como la asignación de tareas, se hará principalmente a través del correo electrónico y de una plataforma de trabajo y aprendizaje colaborativo tal como Microsoft Teams.  En este espacio se propondrá, de una parte, la lectura y discusión de algunos teoremas propios de la teoría de números y el álgebra, generando reflexión sobre la pertinencia de su enseñanza y aprendizaje. De otra parte, se estudiarán herramientas técnicas del módulo sympy.ntheory para trasladar lo teórico a lo práctico, es decir, para materializar los teoremas en la creación de criptosistemas.  Se propiciará que las clases tengan un alto componente de trabajo colaborativo tipo taller o laboratorio con computadoras, de manera que los estudiantes desarrollen la habilidad para gestionar tipos de errores que dicho instrumento pueda generar. Por lo anterior, algunas clases se desarrollarán en una sala de cómputo y se recomienda que en los días de no visita a dicha sala, los estudiantes tengan ordenadores o celulares en los que puedan hacer uso de una cuenta de correo de Gmail institucional o personal, de forma que puedan gestionar cuadernos de Google Colab.  El software utilizado en todos los procesos de creación de criptosistemas será de dominio libre. Las clases, funciones o herramientas de uso frecuente en el curso se publicarán en un repositorio público de GitHub para que los estudiantes en todo momento las puedan utilizar con el valor agregado de poder transformarlas a sus gustos y necesidades. |

|  |  |  |
| --- | --- | --- |
| 1. **EVALUACIÓN** | | |
| Atendiendo a los propósitos de formación del programa de *Licenciatura en Matemáticas* que apuntan al conocimiento de los desarrollos en ciencia y tecnología, los criterios para la evaluación que se proponen son: (a) dos parciales tipo pruebas escritas que evaluarán conocimientos científicos en criptosistemas; (b) dos quices tipo prueba escrita que sirvan para que los estudiantes focalicen ideas centrales que tendrán los parciales (los quices serán previos a cada parcial); (c) creación de un sistema criptográfico en un cuaderno de Google Colab, en el que se evaluarán conocimientos tecnológicos, además de la construcción de algoritmos, la edición de texto científico usando Markdown y la habilidad del docente en formación para comunicar definiciones claras en matemáticas. | | |
| **Actividad de evaluación** | **Porcentaje** | **Fecha** |
|  |  |  |
| Quiz 1. | 10% | Semana 8 |
| Parcial 1. | 20% | Semana 9 |
| Quiz 2. | 10% | Semana 13 |
| Parcial 2. | 20% | Semana 14 |
| Criptosistema digitalizado | 40% | Semana 16 |

|  |
| --- |
| **Actividades de asistencia obligatoria**[[2]](#footnote-1)**:** |
| **ARTÍCULO 77. (MODIFICADO POR EL ACUERDO SUPERIOR No. 170 DE FEBRERO 3 DE 2000).** El estudiante, al matricularse en un curso práctico, o en un componente curricular que contenga actividades de obligatorio cumplimiento, adquiere el compromiso de asistir, como mínimo, al 80% de las actividades académicas que exijan presencialidad.  **Parágrafo.** Los consejos de facultad, escuela e instituto definirán las actividades académicas obligatorias de los cursos o de los componentes curriculares mencionados.  **ARTÍCULO 78. (MODIFICADO POR EL ACUERDO SUPERIOR No. 170 DE FEBRERO 3 DE 2000)**. Cuando las faltas de asistencia registradas superen el 20% de las actividades académicas programadas y definidas como obligatorias, el docente encargado del curso reportará "cancelado por faltas", lo que, para efectos del promedio crédito, equivaldrá a una calificación de cero, cero (0.0). Los cursos cancelados por faltas no serán habilitables.  **Parágrafo 1. (MODIFICADO POR EL ACUERDO SUPERIOR No. 170 DE FEBRERO 3 DE 2000)** No se tendrán en cuenta las faltas de asistencia por motivos de enfermedad, calamidad doméstica o representación estudiantil ante los diferentes organismos de dirección o de asesoría de la Universidad, plenamente comprobadas ante el respectivo profesor. Sin embargo, el estudiante deberá asistir como mínimo al 80% de las actividades definidas como obligatorias.  **Parágrafo 2. (ADICIONADO POR EL ACUERDO SUPERIOR No. 170 DE FEBRERO 3 DE 2000)** En todos los cursos el estudiante tendrá la obligación de presentar las evaluaciones programadas.  En el caso de este curso, para el que están programadas 16 sesiones presenciales de 4 horas cada una, es necesario asistir como mínimo a 13 sesiones (o 52 horas). Con lo cual, la insistencia injustificada a 3 de estas sesiones (o 12 horas), desembocará en la cancelación del curso por faltas. |

|  |
| --- |
| **Bibliografía:** |
| **Eje problémico 1.** Preliminares en Python  *Colab*  *<https://colab.research.google.com/notebooks/basic_features_overview.ipynb>*  *Markdown*  *<https://colab.research.google.com/notebooks/markdown_guide.ipynb#scrollTo=5Y3CStVkLxqt>*  Marzal A, Gracia I, García P. Introducción a la programación con Python 3. *Universitat Jaume I, 2014.*  Matthes, Eric. Python Crash Course 2nd Edition A Hands-On, Project-Based  Introduction to Programming. *No Starch Press, Inc. Publisher: William Pollock, 2019.*  Ntheory Class Reference  <https://docs.sympy.org/latest/modules/ntheory.html>  Zed A. Shaw. Learn Python 3*.* The hard way*. Addison-Wesley Professional, 2017.*  **Eje problémico 2.** Cifrados por sustitución.  Apostol. Tom M. Introduction to Analytic Number Theory. *Springer Verlag Berlin Heidelberg*, 1976.  Ntheory Class Reference  <https://docs.sympy.org/latest/modules/ntheory.html>  Rubiano. G, Gordillo. J, Jiménez. L. Teoría de números [para principiantes]. *Universidad Nacional de Colombia, 2004.*  Zaldívar, Felipe. Introducción a la teoría de números. *Fonde de Cultura Económica, 2006.*  **Eje problémico 3.** Cifrado de clave pública RSA.  Ntheory Class Reference  <https://docs.sympy.org/latest/modules/ntheory.html>  Stein W. Elementary Number Theory: Primes, Congruences and Secrets. [A computational approach]. *Springer Science+Business Media, LLC, 2009.*  Zaldívar, Felipe. Introducción a la teoría de números. *Fonde de Cultura Económica, 2006.*  **Eje problémico 4.** Raíces primitivas y logaritmos discretos.  Nielson. S, Monson. C. Practical Cryptography in Python: Learning Correct Cryptography by Example. *Springer Science+Business Media New York, Apress, 2019.*  Ntheory Class Reference  <https://docs.sympy.org/latest/modules/ntheory.html>  Zaldívar, Felipe. Introducción a la teoría de números. *Fonde de Cultura Económica, 2006.*  **Eje problémico 5.** Criptosistemas ElGamal y Rabin.  Stein W. Elementary Number Theory: Primes, Congruences and Secrets. [A computational approach]. *Springer Science+Business Media, LLC, 2009.*  Ntheory Class Reference  <https://docs.sympy.org/latest/modules/ntheory.html>  Zaldívar, Felipe. Introducción a la teoría de números. *Fonde de Cultura Económica, 2006.* |
|  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. **PROFESORES** | | | | | |
| **Nombres y Apellidos** | **Dependencia** | **Formación en pregrado y posgrado** | **Eje N°** | **N° Horas** | **Fechas** |
| Alejandro Sánchez Yalí | Facultad de Educación | Licenciado en Matemáticas y Física.  Magister en Matemáticas. |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. **APROBACIÓN DEL CONSEJO DE UNIDAD ACADÉMICA** | | | | | | |
| Aprobado en Acta número del Haga clic aquí o pulse para escribir una fecha. | | | | | | |
|  |  |  |  |  |  |  |
|  | **Nombre Completo Secretario del Consejo de la Unidad Académica** |  | **Firma** |  | **Cargo** |  |

1. El número de créditos y la intensidad horaria debe estar acorde con el plan de estudios del programa para el que fue diseñado el curso. [↑](#footnote-ref-0)
2. Reglamento Estudiantil y Normas Académicas de Pregrado (Acuerdo 1 del 15 de febrero de 1981), artículos 77 y 78.

   Reglamento Estudiantil para los Programas de Posgrado (Acuerdo Superior 432 del 25 de noviembre de 2014), artículo 30. [↑](#footnote-ref-1)