Información General del curso

Nombre del curso	Criptografía
Código del curso	CLV-077
Duración	20 horas

Descripción del curso

Este curso destaca la importancia del uso de la criptografía en nuestros días y exhibe las razones por las cuales se considera que es uno de los pilares en los que se apoya la seguridad de la información.

De forma general, se puede decir que la criptografía es una metodología científica que aplica una combinación de matemática compleja y lógica con el fin de diseñar métodos de cifrado que puedan ser utilizados para codificar o encriptar mensajes.

El propósito de este curso es desarrollar las competencias básicas para que el estudiante pueda diseñar y evaluar soluciones criptográficas, relacionadas con problemas prácticos (confidencialidad, autentificación) presentes en los sistemas informáticos utilizados en las empresas.

El curso tiene una naturaleza virtual utilizando los altos estándares establecidos por la Universidad, apoyados en las diferentes herramientas para una adecuada ejecución, comprensión y análisis de los diferentes tópicos de la criptografía.

Objetivos del curso

Objetivo General

El estudiante será capaz de analizar los elementos claves de la criptografía, a través del estudio de las principales funciones, protocolos y algoritmos de cifrado, para la evaluación y diseño de soluciones empleando funciones de hash, cifrado simétrico y asimétrico.

Objetivos específicos

- Identificar las características básicas de la criptografía
- Distinguir los componentes de las principales funciones y algoritmos de cifrado clásicos y modernos.
- Comparar el diseño de soluciones empleando técnicas de cifrado simétrico y asimétrico.
- Analizar las utilidades de las funciones de Hash en criptografía

Contenidos

Módulo 1: Historia y Evolución de la criptografía

- Historia de la criptografía
- Conceptos básicos de seguridad y criptografía
- Métodos para la codificación de la información
- Seguridad de los algoritmos criptográficos

Módulo 2: Criptografía clásica y cifra moderna

- Principios de Kerckhoffs
- Clasificación de los sistemas de cifra clásica
    - Cifrado por permutación
    - Cifrado por sustitución
    - Cifrado por matrices
- Características de los sistemas de cifra modernos
- Usos de la criptografía moderna

Módulo 3: Criptografía simétrica y Asimétrica

- Generalidades de la cifra simétrica
- Algoritmos DES, 3DES, AES
- Generalidades de la cifra asimétrica
- Método Diffie y Hellman
- Algoritmo RSA
- Esquema firma digital

Módulo 4: Funciones hash y protocolos de seguridad

- Características y propiedades de las funciones hash
- Funciones hash MD5 y SHA-1
- Las funciones hash más utilizadas hoy en día
- Protocolos de seguridad SSL, SET

Metodología

El curso se desarrolla con una metodología virtual, donde los estudiantes analizan y desarrollan su aprendizaje a su propio ritmo, por medio de los videos y los recursos digitales disponibles, mientras que el 70% de su tiempo se dedica a realizar actividades prácticas, lo que los lleva a una comprensión más profunda de los contenidos, mediante una metodología de aprendizaje basada en proyectos ABP-STEM, la cual supone una manera concreta de aprender críticamente tomando elementos y problemas del contexto.

Esta experiencia de aprendizaje, constituye un modelo de instrucción auténtico en el que los estudiantes planean, implementan y evalúan proyectos que tienen aplicación en el mundo real más allá del aula de clase. En ella se recomiendan actividades interdisciplinarias, de largo plazo y centradas en el estudiante, en lugar de lecciones cortas y aisladas, más importante aún, los estudiantes encuentran los proyectos divertidos, motivadores y retadores, porque desempeñan en ellos un papel activo tanto en su escogencia como en todo el proceso de concepción, diseño, implementación y operación.

Estrategias de aprendizaje

Este curso está compuesto de las siguientes actividades de aprendizaje, las cuales le permitirán profundizar en el conocimiento de los contenidos, así como la aplicación en contexto real de lo abordado durante las 4 semanas:

- **Talleres investigativos:** Un taller investigativo es un espacio para la reflexión, el debate y la confrontación, de ideas, de conocimientos y saberes que permitan la construcción colectiva de conceptos y teorías en torno al conocimiento, fortalecimiento y desarrollo del espíritu científico de los estudiantes. Esta es una actividad colaborativa y asincrónica, en la cual el docente es un guía en el proceso.

  Taller 1 (Criptografía Clásica y moderna): Se analizarán algoritmos y aplicaciones de los métodos de cifra clásicos. Se resolverán casos específicos.

Taller 2 (Funciones de Hash y protocolos de seguridad): En este taller se analiza el uso de funciones de Hash y cifra moderna en aplicaciones tales como Firma Digital y Blockchain.

El paso a paso para realizar los talleres investigativos son :

1. Delimitación: El docente plantea de manera clara, precisa y concreta, el tema objeto del taller, aclarando la situación o contexto dentro del que está enmarcado el problema y el enfoque que se le va a dar trabajo.
2. Participación en el taller: El estudiante debe desarrollar las siguientes actividades:

   - Debe proponer una solución a la problemática planteada demostrando un amplio dominio del tema en estudio y una excelente habilidad para aplicar los conocimientos adquiridos en el curso.
   - En el análisis y en la solución debe considerar diferentes dimensiones de análisis posibles para el caso propuesto.
   - La solución debe estar estrechamente relacionada con el diagnóstico realizado.
   - Debe entregar un documento siguiendo los lineamientos establecidos por el docente.

- **Foro:** El foro es un espacio dedicado a tratar temas de interés derivadas de las lecturas y tiene la función de ser una herramienta de comprobación, permite desarrollar las competencias de comunicación escrita, pensamiento crítico, asociación de ideas, participación responsable, relevante, oportuna y creativa. En el curso de criptografía el foro estará relacionado con la temática de los métodos de criptografía simétricos y asimétricos.

- **Mapa Conceptual:** El mapa conceptual es una herramienta que muestra de manera gráfica y sencilla los términos claves o conceptos de un tema específico, con la idea de ser fáciles de recordar y analizar. En el curso de criptografía el mapa conceptual estará relacionado con la evolución de los métodos para la codificación de la información.

Evaluación

El curso se aprueba con una nota mínima de 70 puntos y se le hará entrega de un certificado emitido por la Universidad.

Actividades de aprendizaje	Porcentaje
Taller investigativo (2 actividades, 25% c/u) Los estudiantes analizan la situación propuesta en cada taller • Taller #1 (Criptografía clásica y moderna) • Taller #2 (Funciones de Hash y protocolos de seguridad)	**50%**
Mapa Conceptual (1 actividad, valor 25%)	**25%**
Foro (1 actividad, valor 25%)	**25%**
TOTAL	**100%**

Rúbricas

Taller investigativo (Valor de 50%, cada uno 25%).

En el curso de Criptografía el taller es una actividad orientada a garantizar la aplicación de diferentes temáticas que forman parte del uso de la criptografía, en la resolución de problemas puntuales. Se verifica que los nuevos conocimientos, provenientes de diferentes fuentes, se integren en un producto que presenta una solución a una situación planteada.

Título: 1. Taller #1 (Criptografía clásica y moderna) 2. Taller #2 (Funciones de Hash y protocolos de seguridad)					
Producto: Informe del taller sobre las diferentes temáticas; Desarrollo del pensamiento crítico y analítico relacionado con la seguridad de la información.					
	Excelente (100%)	**Muy Bien (90-80%)**	**Bien (70-60%)**	**Regular (50%-40%)**	**No lo hace (0%)**
Aplicación conceptual	La solución al caso planteada demuestra amplio dominio del tema en estudio y una excelente	La solución al caso planteada demuestra dominio del tema en estudio y habilidad para	La solución al caso planteada demuestra algún dominio del tema en estudio y/ alguna	La solución al caso planteada demuestra poco dominio del tema en estudio y/o poca	No demuestra conocimiento del tema. El caso está mal desarrollado.

	habilidad para aplicar este conocimiento en casos concretos.	aplicar este conocimiento en casos concretos.	habilidad para aplicar este conocimiento en casos concretos.	habilidad para aplicar este conocimiento en casos concretos.	
Dimensiones	En el análisis y en la solución se consideran todas las dimensiones de análisis posibles para el caso.	En el análisis y en la solución se consideran gran parte de las dimensiones de análisis posibles para el caso.	En el análisis y en la solución se consideran algunas de las dimensiones de análisis posibles para el caso.	El análisis y la solución se hacen con un escaso abordaje de las dimensiones del caso.	No se analizó el caso, el análisis realizado no tiene relación o congruencia con el caso.
Pertinencia de la solución	La solución está estrechamente relacionada con el diagnóstico realizado.	La solución está relacionada con el diagnóstico realizado.	La relación entre el diagnóstico y la solución es confusa o está incompleta.	La solución está poco relacionada con el diagnóstico.	La solución no tiene relación con el diagnóstico realizado.
Calidad del informe	Entregó a tiempo. Respeta los lineamientos del instructivo. Excelente redacción y ortografía.	Entregó a tiempo. Respeta los lineamientos del instructivo. Redacción y ortografía aceptable o buena.	Entregó hasta un día tarde. Respeta los lineamientos del instructivo. Redacción y ortografía aceptables.	Entregó hasta dos días tarde. Obvió algunos lineamientos del instructivo. Redacción y ortografía regular.	Entregó más de dos días tarde o no entregó. Obvió la mayoría de lineamientos del instructivo. Mala redacción y ortografía.
Total Final:					

Foro (Valor de 25%).

En el curso de Criptografía el foro de discusión es una actividad que promueve el intercambio de opiniones en torno a un tema de interés común. En el foro se comparten experiencias y se dan respuesta a preguntas que surgen en torno al tema que se analiza. Se verifica que los nuevos conocimientos, provenientes de diferentes fuentes, se integren en un producto que presenta una solución a una situación planteada.

Título:

1. **Métodos de criptografía Simétrica y Asimétrica.**

Producto: Participación argumentativa registrada en los foros, además del desarrollo del pensamiento crítico y analítico relacionado a la seguridad de datos.

Concepto	**Excelente (10 puntos)**	**Bueno (8 puntos)**	**Satisfactorio (6 puntos)**	**Deficiente (0 puntos)**
Participación	Participa en el foro por lo menos con 3 intervenciones	Participa en el foro por lo menos con 2 intervenciones	Participa en el foro por lo menos con 1 intervención	No participa en el foro.
Importancia del tema y nuevas ideas	La intervención muestra la importancia del tema, aporta nuevas ideas y las justifica	La intervención muestra la importancia del tema, aporta nuevas ideas, pero no las justifica.	La intervención muestra algún interés en el tema, pero no aporta nuevas ideas.	Realiza la intervención pero no muestra interés por el tema y tampoco aporta ideas.
Calidad de las intervenciones.	Las intervenciones son muy claras, concisas y respetuosas.	Las intervenciones son claras, concisas y respetuosas.	Las intervenciones son poco claras, concisas y respetuosas.	Las intervenciones no son claras, concisas y respetuosas.
Interacción con los compañeros y tutor.	Establece un diálogo con los compañeros y el tutor, debatiendo y defendiendo ideas, y construyendo nuevos aportes en conjunto.	Establece un diálogo con los compañeros y el tutor, aporta en la construcción de nuevas ideas.	No logra establecer acertadamente un diálogo con los compañeros y el tutor, el aporte en la construcción de nueva idea es poco.	No establece un diálogo con los compañeros y el tutor.

Mapa Conceptual (Valor de 25%).

En el curso de Criptografía el mapa conceptual es una herramienta que muestra de manera gráfica y sencilla los términos claves o conceptos de un tema específico. El tema del mapa conceptual estará relacionado con la evolución de los métodos criptográficos.

Criterios a Evaluar	Cumple con lo solicitado 2 puntos	Cumple parcialmente 1 punto	No cumple lo solicitado 0 puntos	Observaciones al estudiante
1. El mapa conceptual tiene como título el tema principal que se analiza.				
2. El tema principal queda claramente definido.				
3. Luego del tema principal (como si fuera una jerarquía), aparecen los términos asociados.				
4. Los temas asociados al tema principal se definen con claridad.				
5. Existen líneas conectoras que enlazan los diferentes términos que se desprenden del tema principal, donde se denota una secuencia lógica de los términos.				
6. Usa palabras de enlace en todo el mapa conceptual que son de apoyo a las líneas conectoras y la compresión de todo el mapa que se elabora.				
7. Incluye las referencias en formato de APA vigente.				
8. Se demuestra el uso correcto de ortografía y redacción como factor de comunicación escrita asertiva.				
Total 16 puntos. Para obtener la nota se utiliza regla de 3.				

Recursos

Para fomentar el aprendizaje según las estrategias de enseñanza, nuestras plataformas virtuales proveen de herramientas importantes fomentando el acceso a la información, construcción del aprendizaje, comunicación entre los participantes y facilitador (a), almacenamiento de los entregables y presentación de proyectos a través de medios modernos digitales.

Particularmente en el curso se tiene acceso a:

Recursos Sincrónicos

- Masterclass
- Horas de atención semanales.

Recursos Asincrónicos

- Campus Virtual de la Universidad
- Foros de consultas
- Tareas.
- Mensajería interna de la plataforma

Software externo (Con o sin licencia)

- EBSCO
- E-Libro
- Office 365 con licencia (Office, Stream, Teams).

Bibliografía

Obligatoria

Hernández Encinas, L. (2016). La criptografía. Editorial CSIC Consejo Superior de Investigaciones Científicas. https://elibro.net/es/lc/ufidelitas/titulos/41843

Arboledas Brihuega, D. (2017). Criptografía sin secretos con Python. RA-MA Editorial. https://elibro.net/es/lc/ufidelitas/titulos/106497

Complementarios

García, R. D. M. (2009). Criptografía clásica y moderna. Septem Ediciones. https://elibro.net/es/lc/ufidelitas/titulos/102985 (clásico)

Rojo, M. I. (2019). Blockchain: fundamentos de la cadena de bloques. Ediciones de la U. https://elibro.net/es/lc/ufidelitas/titulos/127086

Muñoz Muñoz, A. (2016). Privacidad y ocultación de información digital: esteganografía: protegiendo y atacando redes informáticas. RA-MA Editorial. https://elibro.net/es/lc/ufidelitas/titulos/106496

Maillo Fernández, J. A. (2017). Sistemas seguros de acceso y transmisión de datos. RA-MA Editorial. https://elibro.net/es/lc/ufidelitas/titulos/106503

Cronograma

Semana	Contenido	Estrategias de aprendizaje	Actividades de Evaluación (Entregable)
0	Indicaciones generales	Video de bienvenida Programa del curso Foro de presentación	Observar el video de bienvenida Leer el programa del curso Participar en el foro de presentación
1	Historia y evolución de la criptografía • Conceptos básicos de seguridad y criptografía • Métodos para la codificación de la información • Seguridad de los algoritmos criptográficos	Videos de contenidos Lectura de unidad 1. Instrucciones de la asignación de la semana 1.	Leer unidad 1 de Hernández Encinas, L. (2016). La criptografía. Madrid: Editorial CSIC https://elibro.net/es/ereader/ufidelitas/41843?page=24 **Entrega del mapa conceptual 1.**
2	Criptografía clásica y cifra moderna • Principios de Kerckhoffs • Clasificación de los sistemas de cifra clásica • Características de los sistemas de cifra modernos • Usos de la criptografía moderna	Videos de contenidos Lectura de unidad 2. Instrucciones de la asignación de la semana 2.	Leer unidad 2 de Hernández Encinas, L. (2016). La criptografía. Madrid: Editorial CSIC. https://elibro.net/es/ereader/ufidelitas/41843?page=70 **Entrega del taller 1**

3	Criptografía simétrica y Asimétrica • Generalidades de la cifra simétrica • Generalidades de la cifra Asimétrica	Videos de contenidos Lectura de unidad 3. Instrucciones de la asignación de la semana 3.	Leer unidad 3 de Hernández Encinas, L. (2016). La criptografía. Madrid: Editorial CSIC.https://elibro.net/es/ereader/ufidelitas/41843?page=83 **Entrega del foro 1**
4	Funciones de Hash y protocolos. • Características y propiedades de las funciones hash • Protocolos de seguridad	Videos de contenidos Lectura de unidad 4. Instrucciones de la asignación de la semana 4.	Leer unidad 4 de Hernández Encinas, L. (2016). La criptografía. Madrid: Editorial CSIC.https://elibro.net/es/ereader/ufidelitas/41843?page=110 **Entrega del taller 2**