UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Material de apoyo al proceso de enseñanza y aprendizaje en línea para la asignatura de criptografía

MATERIAL DIDÁCTICO

Que para obtener el título de

Ingeniería en Computación

P R E S E N T A

Aarón Enrique Mejia Ortiz

ASESORA DE MATERIAL DIDÁCTICO

Dra. Rocío Alejandra Aldeco Pérez

Ciudad Universitaria, Cd. Mx., 2022

Dedicatoria

En agradecimiento a todo el apoyo recibido a lo largo esta etapa, dedico este trabajo como la culminación de todo el esfuerzo propio y de terceros, sin el cual, esto no sería posible.

Agradecimientos

Se agradece a DGAPA por el proyecto PAPIME PE10772, a CUAIIED por sus aportaciones, y en especial los profesores y tutores Ing. Jorge Alberto Solano Gálvez y Dra. Rocío Alejandra Aldeco Pérez por el apoyo y acompañamiento durante la elaboración del proyecto.

Declaración de autenticidad

Declaro que, el contenido de esta tesis es original, salvo donde se haga referencia específica al trabajo de otras personas, y ha sido desarrollado en su totalidad y exclusivamente para el presente. Este trabajo se realizó en colaboración con un equipo de trabajo conformado por personal de CUAIEED (como asesores pedagógicos), los tutores Ing. Jorge Alberto Solano Gálvez y Dra. Roció Alejandra Aldeco Pérez; y al Ing. Ricardo Sáenz Barragán.

Aarón Enrique Mejia Ortiz

Ciudad Universitaria, Cd. Mx., 2021

Resumen

La creciente educación digital y las condiciones generadas a partir de la pandemia evidenciaron la necesidad de diversificar las maneras en las que se imparte la educación a nivel licenciatura. Por esto, se decidió generar material teórico, práctico y de evaluación para crear un curso en línea de Criptografía, utilizando metodologías de aprendizaje basado en retos.

Para el desarrollo del material, se tomaron como base la selección de temas que comprende el plan de estudios 2016 de la carrera Ingeniería en Computación y otras fuentes, como libros, artículos de revistas, publicaciones académicas. Este material incluye el contenido teórico necesario para que el estudiante se familiarice y comprenda los temas descritos en dicho plan de estudios y además ponga a prueba sus conocimientos teóricos con una serie de actividades de investigación, prácticas y de evaluación.

Con el material generado, se podrá construir un curso en línea para la materia de criptografía, servir como material de apoyo para los estudiantes de curso presenciales o quienes requieran presentar un examen extraordinario. Con todo lo anterior, se reducirá la deserción académica de la materia y aumentará el aprovechamiento de esta.

Índice general

1. Introducción *1*

1.1. Antecedentes 1

1.2. Descripción del problema 2

1.3. Propuesta de solución 3

1.4. Objetivo general 3

1.5. Objetivos específicos 4

1.6. Justificación 4

1.7. Alcance 4

1.8. Resultados esperados 5

2. Marco teórico *6*

2.1. Educación basada en competencias 6

2.2. Aprendizaje Basado en Retos 9

2.3. Educación a distancia y en línea 12

2.4. La importancia de la criptografía en la educación universitaria 13

2.5. Educación en línea sobre Criptografía 18

2.5.1. Cursos en línea de criptografía tipo MOOC 18

2.5.2. Cursos en línea de criptografía ofertados por universidades 20

3. Desarrollo del proyecto *22*

3.1. Estructura de cada módulo 23

3.2. Metodología para la creación de material 24

3.3. Descripción de material completo 25

3.4.1. Módulo 1: Panorama general 31

3.4.2. Módulo 2: Técnicas clásicas de cifrado 31

3.4.3. Módulo 3: Criptografía simétrica o de clave secreta 32

3.4.5. Módulo 4: Criptografía asimétrica o de clave pública 35

3.4.6. Módulo 5: Gestión de claves 37

3.4.7. Módulo 6: Aplicaciones Criptográficas 39

4. Resultados *42*

4.1. Unidad o módulo teórico 42

4.2. UAPA 44

4.3. Evaluaciones 47

4.3.1. Evaluación de módulo 47
4.3.2. Examen 48
4.4. Actividades 50
4.5. Actividades de programación 53
4.6. Estructura de curso y material generado 56
5. Conclusiones y trabajo futuro ***60***
Bibliografía ***62***
Anexos ***67***
A. Ligas de acceso a los materiales 67

Capítulo 1

1. Introducción

1.1. Antecedentes

Para las universidades es importante generar profesionistas que sean capaces de reproducir los conocimientos adquiridos en las aulas, pero también de aplicar estos conocimientos en diversos ámbitos siguiendo un conjunto de actitudes y valores (Corvalán, et al., 2015). Este es uno de los objetivos buscados por la **Educación Basada en Competencias (EBC)** (Argudín, 2005), en donde se definen las competencias que se desea estos futuros profesionistas adquieran a través de procesos de enseñanza – aprendizaje en los que se busca simular retos de la vida profesional. De ahí, surge el **Aprendizaje Basado en Retos (ABR)** (Jou et al., 2010) cuyo objetivo es involucrar al futuro profesionista en un problema para que este sea resuelto. Actualmente, muchas de las experiencias de aprendizaje diseñadas a partir de los modelos EBC y ABR desarrollan competencias definidas o por programas de estudio o por la necesidad del sector productivo, generando un marco para diseñar experiencias de aprendizaje que generen estas competencias y permitan evaluarlas.

Estas experiencias de aprendizaje se pueden diseñar usando como complemento las llamadas tecnologías de la información y la comunicación (TIC). Las TIC son parte de los procesos de formación de estudiantes de diferentes niveles educativos lo que permite a los docentes innovar y mejorar las estrategias para la enseñanza – aprendizaje (Navarro & Edel, 2012). Así surge el término TAC, Tecnologías del Aprendizaje y el Conocimiento, que tratan de orientar el uso de las TICs en los procesos de enseñanza y aprendizaje con el objetivo de aprender más y mejor (Cituk & Vela, 2010). Para eso se crean metodologías en donde estas herramientas tecnológicas se ponen al servicio del aprendizaje y de la adquisición de conocimiento. De esta forma surgen nuevas modalidades de estudio como la semi-presencial (b-learning) y la modalidad a distancia (e-learning) en donde el uso de internet, sistemas de

gestión de aprendizaje y diversos recursos digitales se ponen al servicio de la educación (Watson & Watson, 2017).

Estas dos modalidades unidas presentan diversas ventajas en los procesos de enseñanza – aprendizaje de las cuales podemos mencionar: (1) procesos de aprendizaje flexibles en los que no importa el lugar, tiempo, ocupación o edad del estudiante, (2) estudiantes más responsables de sus propios procesos de aprendizaje haciendo del profesor un facilitador o guía y (3) desarrollo de habilidades digitales apoyadas del uso de plataformas digitales. Así las TACs ofrecen una gran cantidad de ventajas para los procesos de enseñanza aprendizaje particularmente para apoyar los modelos EBC y ABR mientras se promueve su acceso masivo.

En esta tesis presentamos la aplicación de estás modalidades en el desarrollo de material digital que apoyará el proceso de enseñanza aprendizaje para la asignatura en línea de criptografía.

1.2. Descripción del problema

En el contexto actual, con la pandemia del virus COVID-19 presente por más de un año, los estudiantes y profesores han sido obligados a permanecer en casa y laborar desde ahí. Por su parte, los profesores tuvieron que modificar la planeación de sus clases, crear material y actividades nuevas para adaptar sus estilos de enseñanza a la modalidad digital. Muchos de estos docentes carecen del tiempo o la experiencia de, en tan corto tiempo, generar un curso completo. Se enfrentan a falta de material digital ya existente que apoye el proceso de enseñanza-aprendizaje lo que puede afectar la finalización exitosa de las asignaturas por parte de los estudiantes. Es aquí donde se observa claramente el beneficio de las Tecnologías del Aprendizaje y el Conocimiento y la técnica didáctica de Aprendizaje Basado en Retos. Tener material que cubra el temario de un curso, basada en una técnica didáctica y creado para su uso en un ambiente digital, permitiría a los profesores tener mejores resultados en el aprendizaje de los estudiantes, incluso bajo condiciones complicadas como las actuales.

1.3. Propuesta de solución

Como una solución a dicha problemática proponemos generar material para una plataforma en línea para la asignatura de “criptografía” usando la técnica didáctica de Aprendizaje Basado en Retos. Esta es una asignatura optativa que pertenece al campo de profundización de Ingeniería de Software que consta de 64 horas teóricas ofertada a estudiantes de 9o semestre en adelante. Como parte del uso de la técnica de ABR, se propone la inclusión de retos en forma de actividades de programación que permitirán la evaluación de la aplicación del conocimiento teórico que será adquirido a partir de material en línea generado.

El material generado será complementario con el trabajo presentado por Ricardo Sáenz Barragán en la tesis llamada “Plataforma educativa en línea para la asignatura de Criptografía”, finalizada en mayo de 2021. La actual propuesta se enfoca en la generación del material teórico donde se desarrollan los temas, actividades teóricas y prácticas, así como evaluaciones para cada unidad y exámenes que permitan evaluar los conocimientos del estudiante inscrito; mientras que el trabajo mencionado se enfoca en contenido de apoyo constituido por actividades didácticas, generación de material multimedia que apoye las explicaciones teóricas, así como la propuesta de diseño de una plataforma en línea donde se pueda implementar la propuesta actual.

En conjunto, tanto el material teórico como las actividades de apoyo brindarán más recursos y herramientas de estudio en línea para los cursantes de la materia de criptografía que en semestres posteriores podrán ser evaluados y usados por los mismos estudiantes y los profesores. Además de servir como una base sólida para la creación de un curso en totalmente línea administrado por la Facultad de Ingeniería.

1.4. Objetivo general

Generar material teórico, práctico y de evaluación siguiendo la técnica didáctica de Aprendizaje Basado en Retos (ABR) para distribución digital. Este material apoyará el proceso enseñanza-aprendizaje de los estudiantes de la asignatura de criptografía

permitiéndoles aprender los conceptos de esta materia y evaluar dichos conocimientos con exámenes en línea por temas particulares y actividades de programación en forma de retos.

1.5. Objetivos específicos

1. Creación del contenido teórico digital de la asignatura.
2. Generación de actividades de evaluación de las competencias del curso.
3. Diseño y elaboración de actividades de autoevaluación para el material didáctico generado.
4. Diseño y elaboración de material práctico en forma de retos para la asignatura.

1.6. Justificación

El desarrollo del material propuesto permitirá facilitar la impartición de la asignatura de criptografía, así como el desarrollo de las competencias de los estudiantes que estén inscritos a la misma. A su vez, esto permitirá formar mejores profesionales al finalizar los estudios con un mejor aprovechamiento y una posible reducción de deserción de la asignatura

El material digital está dirigido a apoyar a la asignatura de criptografía dentro del plan de estudios de Ingeniería en Computación 2016 de la Facultad de Ingeniería. Con la creación del material propuesto en línea, se estará beneficiando a alrededor de 70 alumnos por semestre que cursen la asignatura de criptografía de la carrera de Ingeniería en Computación en la Facultad de Ingeniería.

1.7. Alcance

Como se mencionó, el material está diseñado para la asignatura de criptografía, impartida en 9º. semestre para la carrera de Ingeniería en Computación. El material se generó con base en los temas incluidos en el plan de estudios 2016 de la carrera de Ingeniería en Computación, usando la plataforma y complementando el trabajo presentado en mayo del 2021 por Ricardo Sáenz Barragán en la tesis llamada “Plataforma educativa en línea para la asignatura de Criptografía”, finalizada en mayo de 2021.

1.8. Resultados esperados

El material teórico y práctico generado esta diseñado para su distribución por medio de una plataforma en línea, esto permitirá el rápido acceso por parte de alumnos y profesores. Además, dicho material, se diseñó para ser parcialmente autogestivas por parte de los estudiantes. De esta manera tanto el contenido teórico, como actividades, autoevaluaciones y elementos multimedia que se utilizan como complemento, deben ser claros para facilitar la asimilación del conocimiento a transmitir. Las actividades propuestas y prácticas de programación están pensadas para complementar, expandir y consolidar el conocimiento adquirido con el contenido teórico, tal cual como la técnica didáctica ABR lo describe.

Inicialmente, se propone que los alumnos usen este material teórico y práctico como apoyo para el curso al que están inscritos donde interactúan con un profesor. Así el material apoya para reforzar el conocimiento adquirido, e incluso como método de preparación para sus evaluaciones. Por su parte los profesores podrán utilizar el material teórico y práctico desarrollado para complementar sus clases, referir a los alumnos al contenido y mejorar la experiencia didáctica del curso.

Posteriormente, se podrá ofertar la materia completamente en línea para los alumnos y profesores que así lo deseen, sin reducir la calidad de conocimiento en comparación con un curso presencial.

Capítulo 2

2. Marco teórico

Como se menciona anteriormente, esta propuesta toma elementos importantes de dos técnicas didácticas EBC y ABR para crear una experiencia de aprendizaje en línea parcialmente autogestiva lo más cercana a una clase presencial. Así, en esta sección revisamos los conceptos usados en el desarrollo de esta tesis.

2.1. Educación basada en competencias

Las enseñanzas basadas en competencias (EBC) se basan en que los alumnos puedan demostrar el dominio del conocimiento, habilidades actitudes y valores de una competencia específica, está enfocada en los resultados más que en el tiempo que se le dedica, como sucede en los modelos tradicionales de enseñanza. (Everhart, Sandeen, Seymour y Yoshino, 2014).

En la EBC el instructor deja el rol de expositor o presentador de información y se convierte en un guía y orientador que apoya a los alumnos con el uso de herramientas para que desarrollen las habilidades y competencias de interés previamente definidas, con objetivos claros y medibles.

Una competencia se refiere a la integración de conocimientos habilidades, actitudes y valores que permitirán a los alumnos desenvolverse de una forma más efectiva en una diversidad de contextos. Generalmente se enfocan en un desarrollo integral para el futuro profesional y problemas reales desde un punto de vista humano (Blanco, 2009).

Características de una Competencia

- El progreso depende de la demostración de dominio o maestría
- Los objetivos de aprendizaje son explícitos, cuantificables y transferibles

- La evaluación como experiencia de aprendizaje significativa y positiva
- La instrucción es diferenciada y con apoyo oportuno
- Los resultados de aprendizaje incluyen aplicación y creación de conocimiento

Tipos de competencias

Existe una divergencia en los tipos de competencias dependiendo de la literatura que se consulte, sin embargo, se pueden generalizar y agrupar en los siguientes 3 grupos:

Competencias genéricas

Competencias base que promueven el autoaprendizaje, desarrollo de relaciones y participación eficaz en la vida social y profesional, facilitan la adquisición de otras competencias, valores éticos e inteligencia emocional (Tobón, 2009) (SEMS, 2008) (Lozano y Herrera, 2011).

Competencias disciplinares

Competencias consideradas mínimas necesarias para cada campo disciplinar, incluyendo capacidades agnósticas al campo, capacidades y conocimientos propios de una ocupación o profesión (SEMS, 2008). Tienen un alto grado de especialización y procesos educativos específicos (Lozano y Herrera, 2011).

Competencias laborales y profesionales

Competencias relacionadas a la vida laboral y que no necesitan de estudios formales para desarrollarse. Se enfocan en habilidades técnicas y operativas, así como en la toma de decisiones, pensamiento crítico y creativo y resolución de problemas complejos (Lozano y Herrera, 2011).

Beneficios

- **Enfoque en las necesidades de la sociedad y el mundo laboral:** se concentra en conectar la formación y el aprendizaje del estudiante con el mundo laboral para responder a las necesidades de la sociedad (Tuning, 2007).
- **Reconocimiento de aprendizajes previos:** utilizan conocimiento previo adquirido fuera de un salón de clases, con el fin de acelerar su proceso educativo permitiendo a los alumnos reconocer áreas de oportunidad (Degree Prospects, 2015).
- **Flexibilidad y accesibilidad:** se enfoca en el aprendizaje y no en el tiempo invertido. Los estudiantes no tienen que seguir programas académicos rígidos en contenido ni periodos de tiempo (Degree Prospects, 2015). Al ser un proceso más eficiente lo hace más accesible económicamente (Blot en PR, N.; Everhart, 2014).
- **Autogestión del aprendizaje:** mejorar la capacidad de los estudiantes para reconocer, gestionar y construir continuamente sus propias competencias (Everhart, 2014). También permite a los estudiantes evaluar y mejorar su desempeño, interpretar situaciones, resolver problemas y realizar acciones innovadoras (Tuning, 2007).
- **Transparencia en las capacidades de los egresados:** El modelo EBC permite comunicar eficazmente lo que los estudiantes saben y pueden hacer (Klein-Collins, 2012). Esto proporciona a los empleadores una mayor comprensión de los resultados de aprendizaje de los estudiantes (Everhart, 2014).
- **Formación integral y transversal:** prepara a los estudiantes de manera integral desarrollando competencias que serán útiles en un contexto general como el acceso al empleo y el ejercicio de una ciudadanía responsable a través de competencias como: pensamiento lógico, autoaprendizaje, manejo de la comunicación verbal y el lenguaje, la creatividad, la empatía, así como también una conducta ética (Tuning, 2007).
- **Desarrollo de nuevas competencias docentes:** impulsa el continuo desarrollo pedagógico y profesional de la planta docente (Tuning, 2007).

2.2. Aprendizaje Basado en Retos

El aprendizaje basado en retos (ABR) es un enfoque pedagógico que involucra a los estudiantes en problemas reales y relevantes vinculados a su contexto. Este enfoque busca la definición de retos y soluciones a partir de esos problemas.

El Aprendizaje Basado en Retos tiene sus raíces en el Aprendizaje Vivencial, el cual propone que los estudiantes aprenden mejor cuando participan de forma activa en experiencias abiertas de aprendizaje, que cuando participan de manera pasiva en actividades estructuradas. Esto permite que los estudiantes apliquen su conocimiento en situaciones reales donde enfrentan problemas que los hacen aprender y reforzar su conocimiento (Moore, 2013). Basado en esto, el Aprendizaje Basado en Retos aprovecha el interés de los estudiantes por darle un significado práctico a la educación, mientras desarrollan competencias esenciales como el trabajo colaborativo y multidisciplinario, la toma de decisiones, la comunicación efectiva, la ética y el liderazgo (Malmqvist, Rådberg y Lundqvist, 2015).

El enfoque incorpora cuatro elementos que cuando son aplicados adecuadamente y en conjunto optimizan el aprendizaje aumentando el conocimiento de los alumnos y su capacidad de aplicarlo en resolución de problemas (Rowe y Klein, 2007). Los elementos son:

- **Conocimiento**: La información es presentada de forma adecuada, ordenada y en forma secuencial
- **Estudiantes**: El conocimiento es relevante al contexto de los estudiantes y hace referencia a conocimientos previos.
- **Evaluaciones**: Existen oportunidades de retroalimentación tanto de estudiantes como de docentes, donde los estudiantes comprueban sus conocimientos y los docentes la eficacia de su enseñanza.
- **Comunidad**: El ambiente promueve y permite el trabajo colaborativo para la adquisición y solución de problemas.

Challenge Based Learning de Apple

La metodología empleada por el ABR está basada por el marco propuesto por Apple llamada en inglés "*Challenge Based Learning*" (Apple, 2011), mostrado en la Fig 2.1. El acercamiento presentado por Apple propone un enfoque práctico de la adquisición de conocimiento por medio del trabajo colaborativo entre estudiantes, docentes e investigadores esto para la solución de problemas reales en sus comunidades y la divulgación de los resultados. Además, proponen el uso de la tecnología para la comunicación y generación de nuevas ideas a través de medios digitales.

Figura 2.1. Marco metodológico del Aprendizaje Basado en Retos de Apple (2011).

A continuación, se definen los elementos que se integran en el marco propuesto por Apple para el Aprendizaje Basado en Retos:

1. **Idea general**: Concepto amplio que puede ser explorado en múltiples formas, es atractivo, de importancia para los estudiantes y para la sociedad. Es un tópico con

significancia global, en este caso, la protección de la información a través del uso de algoritmos criptográficos.

2. **Pregunta esencial:** Por su diseño, la idea general posibilita la generación de una amplia variedad de preguntas. El proceso se va acotando hacia la pregunta esencial que refleja el interés de los estudiantes y las necesidades de la comunidad. Crea un enfoque más específico para la idea general y guía a los estudiantes hacia aspectos más manejables del concepto global. Por ejemplo, ¿Cómo puedo proteger la confidencialidad de un mensaje usando el proceso de cifrado por bloque?
3. **Reto:** Surge de la pregunta esencial, es articulada e implica a los estudiantes crear una solución específica que resultará en una acción concreta y significativa. El reto está enmarcado para abordar la idea general y las preguntas esenciales con acciones locales. En este caso, protege un mensaje usando el algoritmo de cifrado por bloque SDES.
4. **Preguntas, actividades y recursos guía:** Estos recursos son proporcionados por la plataforma en línea, de manera ordenada y con algunas autoevaluaciones. Estos representan el conocimiento necesario para desarrollar exitosamente una solución.
5. **Solución:** En este caso, el reto establece que la solución deberá presentarse como una implementación en algún lenguaje de programación. Así, la solución será el diseño de dicha implementación.
6. **Implementación:** Los estudiantes implementan su diseño usando el lenguaje de programación de su elección.
7. **Evaluación:** Esto se realiza a través de rúbricas diseñadas para este fin. Los resultados de la evaluación formal e informal confirman el aprendizaje y apoyan la toma de decisiones a medida que se avanza en la implementación de la solución. Tanto el proceso como el producto pueden ser evaluados por el profesor.
8. **Validación:** Los estudiantes prueban la eficacia de su implementación a través de pruebas unitarias que son parte del diseño de las actividades.
9. **Documentación y publicación:** Estos recursos pueden servir como base de un portafolio de aprendizaje y como un foro para comunicar su solución con el mundo. Esta etapa se deja fuera del alcance de este trabajo, pero se menciona para trabajo futuro.

10. **Reflexión y diálogo:** Mucho del aprendizaje profundo tiene lugar al considerar este proceso, se reflexiona sobre el aprendizaje propio, sobre las relaciones entre el contenido, los conceptos y la experiencia e interactuando con la gente. Esta etapa se deja fuera del alcance de este trabajo, pero se menciona para trabajo futuro.

2.3. Educación a distancia y en línea

La educación en línea tiene su origen con la consolidación de internet como método global de intercambio de información, y consiste en el uso de Tecnologías de Informática y de la Comunicación (TICS's) para la impartición de educación a distancia de forma asíncrona y sin estar en un mismo espacio (Global, 2021).

Es importante entender que la educación en línea es un tipo de educación a distancia, pero no son sinónimos, la educación en línea requiere el uso de herramientas y estrategias pedagógicas en Internet; mientras que la educación a distancia hace uso de otros medios de comunicación como el radio y la televisión.

La educación en línea tiene un enfoque donde los estudiantes adquieren un rol más autónomo y de autogestión, mientras que los docentes se transforman en tutores que guían y asisten a los estudiantes en el proceso de aprendizaje.

A continuación, se describen alguna de las ventajas de la educación en línea:

- **Apertura**: mayor acceso a la información independientemente de la localización geográfica.
- **Flexibilidad**: favorece la autogestión de los tiempos de dedicación y disponibilidad de los estudiantes.
- **Eficacia**: mayor aprovechamiento de recursos multimedia y herramientas que facilitan y agilizan la asimilación de nuevo conocimiento.
- **Acompañamiento personalizado**: La educación en línea se distingue por hacer un acompañamiento personalizado al alumno, aún con trabajos grupales.
- **Economía**: se reduce el costo de operación además de los costos inherentes a traslados, y por lo tanto se vuelve más accesible.

- **Comunidad**: promoción del debate y el diálogo como herramienta de socialización e intercambio de ideas, además de una comunidad vinculada a los conocimientos académicos.

En este sentido, actualmente la UNAM cuenta con La Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia que se encarga de coordinar e impulsar la creación, el desarrollo y la evaluación permanente de los modelos y las metodologías de enseñanza-aprendizaje en ambientes educativos multimodales, así como de asesorar y apoyar en el diseño, desarrollo y evaluación de proyectos y programas de estudio mediados por tecnología. También existe el Sistema de Universidad Abierta Y Educación a Distancia, que proporciona flexibilidad de estudio para la obtención de un título universitario eliminando algunos obstáculos como el horario, lugar, trabajo, edad, etc.

Estos son ejemplos de educación a distancia y en línea en nuestra universidad. Estos se han encargado de generar diseños de materias y grados a nivel licenciatura completos en estas modalidades. Como consecuencia, sus metodologías y experiencias son de gran utilidad para trabajos como el nuestro. De ahí que su apoyo haya sido clave en el desarrollo de esta tesis.

2.4. La importancia de la criptografía en la educación universitaria

La ciberseguridad es un tema que ha tomado mayor relevancia en los últimos años con el uso masivo de tecnologías digitales como el internet. Un tema pendiente dentro de la sociedad y varios planes de estudio a nivel licenciatura es la enseñanza de las bases de la ciberseguridad como una herramienta necesaria en el desarrollo profesional de los recién egresados. De ahí que en esta tesis nos enfoquemos en el desarrollo de material que impacta en esta área.

La ciberseguridad es la práctica de proteger sistemas críticos e información sensible de ataques digitales con le uso de medidas y estrategias de seguridad que abarcan varias capas de protección para combatir ataques a sistemas en redes y aplicaciones, sin importar si las amenazas son de origen interno o externo a una organización (IBM, 2021). Particularmente en México la comunidad científica se ha enfocado en 3 principales líneas de investigación en

la ciberseguridad que a continuación describimos (Aldeco, Gallegos, & Rodríguez, Líneas de Investigación en México, 2020).

Criptografía

Criptografía se refiere a la ciencia en la que se aplican conceptos matemáticos y ciencias de la computación para proteger información a través del cumplimiento de los cuatro servicios de seguridad: confidencialidad, integridad, autenticación y no repudio (Information security and cryptography, 1996). De acuerdo con el periodo histórico la criptografía se clasifica en:

- **Clásica**: con inicios durante el imperio egipcio hasta la implementación de máquinas mecánicas y electromagnéticas en la segunda guerra mundial, la criptografía clásica utilizó técnicas como la permutación y sustitución para ocultar información y compartirla de forma segura.
- **Moderna:** con la popularización de la computación a finales de los 60 se inició la implementación de técnicas criptográficas en sistemas computacionales y dando pie a la criptografía de llave pública, que es una parte esencial de las comunicaciones seguras que utilizamos hoy en día.
- **Cuántica:** alrededor de los años 70 se inició la aplicación de conceptos de física cuántica en la computación, en los años 80 comienzan las publicaciones de nuevos protocolos de seguridad basados en principios cuánticos como el de la superposición y de incertidumbre.
- **Post-cuántica:** A finales de los años 90 los algoritmos de criptografía moderna comenzaron a verse afectados por los algoritmos y avances en la criptografía cuántica. El desarrollo de algoritmos capaces de resolver los problemas matemáticos con un computador cuántico con suficientes *qubits* representa un riesgo para la seguridad basada en criptografía moderna, ya que se podría vulnerar los algoritmos y, por lo tanto, todos los sistemas de seguridad que utilicen esos algoritmos. Como respuesta, se comenzaron a buscar nuevos problemas matemáticos que fueran difíciles incluso para la computación cuántica, por ejemplo: algoritmos basados en lattices, algoritmos basados en ecuaciones multi-variables, algoritmos basados en curvas elípticas

isogéneas súpersingulares, algoritmos basados en hashes, algoritmos basados en códigos, entre otros. (Edu Trends: Educación Basada en Competencias, 2015)

Este es el área abordada en este trabajo de tesis, siendo la base sobre la que las siguientes líneas se apoyan.

Seguridad en infraestructura

Toda la comunicación digital se lleva a cabo por medio redes locales y abiertas, por lo tanto, se debe implementar infraestructura necesaria para garantizar la integridad y confidencialidad de la información que transita en esas redes. Para ello se hace uso de sistemas de seguridad interna y perimetral, sistemas de detección, análisis de riesgos y pruebas de penetración; junto con políticas que permitan cumplir con las mejores prácticas y apegarse a estándares y obtener certificaciones. Una subrama de la infraestructura es el *"hacking ético"* que consiste en someter a pruebas de estrés los sistemas y redes con el fin de identificar vulnerabilidades para prevenir riesgos.

Internet de las cosas

La implementación de variados dispositivos *IoT* ya es popular y está en incremento de forma abrumadora por su fácil configuración y compatibilidad. Sin embargo, estas contienen la mínima cantidad o poco adecuadas capas de seguridad, dando pie a la explotación de sus vulnerabilidades. El constante incremento de estos dispositivos en uso y su poder computacional aumenta la urgencia de implementar métodos de seguridad adecuados.

Esto muestra la importancia de la criptografía dentro de la formación de estudiantes y como el tener un mayor número de recursos disponibles para ellos ayuda a incrementar el interés de esta área en la academia y la industria y, por lo tanto, un incremento en aplicaciones e investigación.

Educación y ciberseguridad en México

En México existen varias instituciones educativas que ofrecen formación en el área de ciberseguridad en forma de licenciaturas, maestrías y diplomados, la mayoría de ellas se

imparten de forma presencial. A continuación, presentamos un listado de las instituciones y su oferta académica en la rama:

- **Centro de Investigación y de Estudios Avanzados:** constante investigación en criptografía y seguridad informática, además de que sus integrantes fueron parte fundamental de la fundación de *The International Conference on Cryptology and Information Security in Latin America (Latincrypt)* y la *Advanced School on Cryptology and Information Security in Latin America (ASCrypto),* eventos relevantes en Latinoamérica sobre criptografía y seguridad informática.
- **Instituto Politécnico Nacional:** creación de las primeras especialidades y maestría en seguridad informática de México, fundan en 2013 el Centro de Investigación en Computación (CIC), donde se realizan investigaciones sobre seguridad en el ciberespacio, seguridad en el Internet de las cosas, criptografía, algoritmos evolutivos para ciberseguridad y biometría; entre otras.
- **Universidad Iberoamericana:** ofrecen especialidades y maestrías enfocados a un aspecto ético y normativo de la seguridad informática.
- **La Salle:** impartición de especialidades y maestrías donde se abordan temas como tocan temas como: seguridad en redes, criptografía, *hacking* ético, gestión de incidentes y análisis forense y auditoría de la seguridad, todo esto sin descuidar temas de factores Humanos en la seguridad de la información y algunos temas de normatividad.
- **Universidad Tecnológica de México:** ofrece una maestría en Seguridad de Tecnología de Información donde se abordan temas de arquitectura de la seguridad, controles criptógrafos de seguridad, *hacking* ético y análisis forense, seguridad en dispositivos móviles y telefonía, normatividad y legislación de IT, entre otras.
- **Instituto Nacional de Astrofísica Óptica y Electrónica:** ofrece la Maestría en Ciencias Computacionales y la Maestría en Ciencias en Tecnologías de Seguridad. El primero tiene un enfoque en las ciencias computacionales aplicadas a la seguridad, mientras que el segundo se enfoca completamente a la seguridad en los aspectos de análisis, diseño, aplicación y evaluación de proyectos de seguridad.

- **Tecnológico de Monterrey:** Ofrece una Maestría en Ciberseguridad que forma profesionistas que innoven investiguen y desarrollen dentro de organizaciones en el área de seguridad, y un diplomado en Tecnologías de Ciberseguridad donde integran servicios, mecanismos y controles para contribuir a las mejores prácticas de arquitectura, operación y gobierno de la ciberseguridad en organizaciones.
- **Universidad Autónoma de Nuevo León:** ofrece la Maestría en Ingeniería en Seguridad de la Información. Aborda temas de criptografía, seguridad en base de datos, sistemas de control de accesos, *hacking* ético, y normativa que conlleva la ciberseguridad.
- **UNIR:** la Maestría en Seguridad Informática de la Universidad en Internet tiene la característica de ser impartida 100% en línea y de tener validez como título en México y España por parte de la Universidad Internacional de la Rioja. El plan de estudios abarca la seguridad de la información con un enfoque legal, técnico y de gestión.
- **Centro de Estudios Superiores Navales:** Ofrece una Maestría en Seguridad de la Información exclusivo para miembros de las Fuerzas Armadas de México y para elementos del Consejo Nacional de Seguridad de México. El plan de estudios ofrece dos especializaciones o enfoques: el administrativo donde se enseña el desarrollo e implementación de aplicaciones de ciberseguridad además del análisis y evaluación de propuestas con base en las políticas de seguridad; mientras que el lado operativo se encarga del soporte técnico, aplicación de técnicas de cómputo forense, criptografía y de inteligencia de señales.

- **Universidad Nacional Autónoma de México:** ofrece dos diplomados en "Redes y Seguridad" y el segundo "Seguridad de la Información y Ciberseguridad"; con el fin de aportar conocimientos teórico prácticos para la aplicación y promoción de la ciberseguridad. El diplomado abarca conocimientos sobre estratégica, finanzas, área humana, ciberseguridad industrial y área humana.
- **Universidad del Valle de México:** oferta el diplomado de Ciberseguridad y ciberdefensa con el objetivo de profundizar sobre los principales elementos de identificación, protección, detección, respuesta y recuperación ante una amenaza en ciberseguridad en el contexto de negocios o instituciones.

- **Universidad Anáhuac:** ofrece un diplomado en línea dirigido a profesionales encargados de la operación y gestión de sistemas digitales, consultores de seguridad informática, técnicos vinculados a las TIC y personas que hagan uso de las TIC. Tiene un enfoque holístico abordando los siguientes temas: introducción a la ciberseguridad, riesgos actuales en ciberseguridad, informática forense, seguridad de la información y legislación nacional e internacional en ciberseguridad.

Esto muestra que la oferta de opciones para que los estudiantes se preparen en áreas como la criptografía son limitadas. De ahí que la creación del material propuesto en este documento de tesis a largo plazo podría volverse en una opción más para la adquisición de este conocimiento y su práctica, ya muy necesaria hoy en día.

2.5. Educación en línea sobre Criptografía

Los primeros cursos en línea fueron creados por universidades y su popularidad dio pie a la creación de miles de cursos por parte de otras universidades, profesionistas y educadores que comparten su conocimiento y experiencia por medio de plataformas destinadas a la educación en línea con el uso de material didáctico digital.

Aunque todos los cursos que existen se distribuyen de la misma forma, existen ventajas y desventajas entre cursos ofertados por universidades y por profesionistas o educadores. De forma general, los cursos ofertados por universidades tienen mayor validez y requisitos que cumplir. A continuación, una breve descripción de ventajas y desventajas de estos dos grupos enfocándonos al área que nos concierne, la enseñanza de la criptografía.

2.5.1. Cursos en línea de criptografía tipo MOOC

Los cursos en línea masivos y abiertos o MOOC (*Massive Open Online Course*) son cursos ofertados por medio de plataformas que están dirigidos a todo aquel interesado en un tema. Generalmente se distribuyen por medio de plataformas especializadas en cursos en línea creadas con este objetivo, como son *Udemy* o *Coursera*.

Este tipo de cursos son de fácil y rápido acceso, y generalmente con costo accesible. Existen algunos con un alcance general sobre la materia y otros que se enfocan en algún tema en especifico. Además, muchos tienen una óptica aplicativa, por lo que los participantes no solo adquieren conocimiento teórico si no también práctico. Tienen la ventaja sobre cursos tradicionales de poder ser completados según la disponibilidad de tiempo del alumno, y de poder repetir y revisar contenido según lo necesite el alumno.

Uno de los problemas más severos es la falta de profundidad con la que se transmiten algunos temas. Aunque logran que el estudiante entienda el tema de forma conceptual y cómo se puede utilizar, muchos procesos importantes, como el funcionamiento de algoritmos criptográficos o criptosistemas, se manejan como cajas negras, dejando lagunas en el conocimiento y entendimiento de los estudiantes.

El segundo problema es la mala información sobre el contenido de los cursos, títulos engañosos que sugieren la adquisición de cierto conocimiento que, al observar el contenido o temario del curso, en realidad es solo una fracción del conocimiento que se debería de entregar. Esto hace que los estudiantes que adquieren el curso reciban sólo una parte de la información necesaria para dominar los temas, además, ignorando los temas que aun faltan por estudiar. Que una persona adquiera alguno de estos cursos y no obtenga lo prometido, representa una perdida de tiempo y dinero. Cabe mencionar que muchas de estas plataformas ofrecen reembolso por cursos adquiridos durante un periodo de tiempo determinado a partir del momento de compra. Esto es bastante útil ya que los estudiantes tienen oportunidad de revisar el contenido y calidad de los cursos, sin embargo, esto requiere del previo conocimiento y criterio para discernir si un curso le resultará útil y si será capaz de satisfacer sus necesidades.

Este tipo de cursos puede ser útil para explorar nuevos conocimientos o tener una base con la cual poder profundizar en los temas de forma más rápida y eficiente gracias a su accesibilidad y facilidad de consumo, sin olvidar que el conocimiento que se adquiera por este medio no es total ni tampoco completo.

2.5.2. Cursos en línea de criptografía ofertados por universidades

Las universidades fueron las primeras impulsoras de la educación en línea por medio de plataformas digitales. Universidades como Standford, Yale, Princeton, Hardvard, Berkley y MIT ofrecen cursos en línea por medio de plataformas como *Coursera*, y *edx*. El principal objetivo de este tipo de cursos es facilitar el acceso a educación de calidad a cualquiera interesado sin limitaciones de tiempo, geográficas o económicas.

Estos cursos tienen material revisado y con lo estándares de calidad y excelencia que otorga el prestigio a estas universidades. Sin embargo, tienden a ser solo extractos de los programas que se imparten a alumnos inscritos presencialmente. Además, la mayoría tienen un costo elevado comparado con el resto de los cursos tipo *MOOC*. Algunos de estos cursos en línea son parcialmente gratuitos, permitiendo a los interesados consultar el material, pero sin permitir el acceso a materiales de apoyo o de evaluación y sin la emisión de un certificado que compruebe que se completó el curso.

Otros promotores de este tipo de cursos, que no son instituciones educativas, son las empresas tecnológicas. Estas ofrecen este tipo de cursos para promover la formación y autoformación de profesionistas mejores preparados que pueden ser potencialmente sus empleados o para los que ya lo son. Uno de los más conocidos es *Google Academy*, manejado por Google, que ofrece cursos de seguridad y criptografía por medio la plataforma *Coursera* totalmente enfocados a conocimientos aplicativos con la teoría necesaria para poder entender el contenido prometido desde un enfoque muy práctico.

La elección de este tipo de cursos presenta un problema similar que en los cursos tipo *MOOC*. Para los casos en los que no esta disponible el contenido total o se presenta de forma parcial, es difícil identificar cómo se van a abordar el material del curso o con qué profundidad se hará. Incluso, si es un área de conocimiento totalmente nueva que se quiere explorar, es sumamente difícil identificar qué cursos son lo que podrían satisfacer las necesidades del estudiante interesado. Así que el sólo tener que decidir que curso será en mejor para aprender estos conceptos es difícil para un estudiante que carece aún de la experiencia para tomar esta decisión.

En conclusión, este tipo de cursos van enfocados a un público profesional, con la capacidad de decidir cual será la mejor opción usualmente para explorar nuevo conocimiento o fortalecer conocimiento que ya se tiene. Muy diferente a un estudiante que requiere de conocimiento base para posteriormente explotarlo en el ambiente profesional.

Capítulo 3

3. Desarrollo del proyecto

En esta tesis se propone generar **material teórico digital dirigido a una plataforma en línea** para la asignatura de "Criptografía" usando la técnica didáctica de Aprendizaje Basado en Retos. El Aprendizaje Basado en Retos (ABR) es una técnica didáctica que sostiene que los estudiantes aprenden mejor cuando se involucran activamente en experiencias abiertas de aprendizaje a cuando participan pasivamente en actividades estructuradas (*Association for Experiental Education*, 2015). Por esta razón, propone confrontar al estudiante a situaciones reales y problemáticas en donde debe aplicar lo aprendido, probando diferentes soluciones (Moore, 2013). Este aprendizaje emula las experiencias de un lugar de trabajo moderno, dándole un significado práctico al proceso de enseñanza – aprendizaje. En nuestro caso, emulando el trabajo que un desarrollador realiza al presentar una solución a un problema en un lenguaje de programación que debe pasar cierta cantidad de pruebas unitarias.

Así, se espera que el estudiante desarrolle una solución a un reto delimitado en contexto y tiempo usando nuevos conceptos y reforzando los ya aprendidos. Esto soportado por material previamente revisado de manera digital. De esta manera, el material estará diseñado siguiendo el temario de la materia y servirá de base para resolver cada uno de los pequeños retos. El objetivo es mejorar la capacidad de solución de nuevos problemas del estudiante, así como su habilidad de transferir conocimiento de un contexto a otro (Cordray et al., 2009).

Por esta razón, primero presentaremos el material desarrollado describiendo su estructura, la metodología que se siguió para su creación y finalmente una descripción detallada de dicho material.

3.1. Estructura de cada módulo

Tomando como referencia el temario de la materia, cada módulo representa una unidad de este temario dentro plan de estudios 2016 de la carrera de Ingeniería en Computación. Cada unidad consta de temas y subtemas igualmente alineados al plan de estudios.

En nuestro diseño, cada módulo incluye contenido teórico estructurado de manera secuencial y este a su vez contiene varias secciones (temas y subtemas) que son introducidos con un breve resumen de lo que se aprenderá (el objetivo). Dentro de los temas también hay contenido digital en forma de imágenes animaciones y videos que refuerzan las explicaciones teóricas y que permiten el aprendizaje y análisis del contenido de forma visual.

Cada módulo contiene actividades de reforzamiento y prácticas. Estas prácticas representan retos que el alumno deberá resolver utilizando conocimientos previos. Las actividades son distribuidas según sea necesario y tendrán un orden sugerido con el fin de tener un flujo natural e intuitivo entre los temas y actividades.

Al finalizar un módulo, el alumno encontrará una actividad y un examen de autoevaluación que le permitirá evaluar su desempeño y reforzar el conocimiento más importante aprendido en el módulo correspondiente.

Se incluye también la realización de exámenes de evaluación que permitan al docente evaluar el conocimiento adquirido por los estudiantes. Estos exámenes evalúan el contenido de varios módulos, y son distribuidos a lo largo del curso según convenga de acuerdo con la segmentación del curso y el tiempo dedicado a cada módulo o unidad. Así podemos clasificar el material generado en los tipos mostrados en la Tabla 3.1.

A.	Documentos con contenido teórico e imágenes.
B.	Contenido digital con elementos teóricos e imágenes.
C.	Actividades de reforzamiento del conocimiento.
D.	Actividades prácticas de programación basadas en ABR.
E.	Autoevaluaciones.
F.	Exámenes.

Tabla 3.1. Tipos de material a desarrollar

3.2. Metodología para la creación de material

Para generar el material digital que presenta el contenido teórico de la materia se usarán las siguientes fuentes:

- Libros.
- Artículos de revistas.
- Publicaciones académicas.
- *Request For Comments* (RFC), son una serie de publicaciones del grupo de trabajo de ingeniería de internet (en inglés IETF *Internet Engineering Task Force*) que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras incluyendo protocolos y algoritmos.
- Estándares del área, mayormente del Instituto Nacional de Estándares y Tecnología (por sus siglas en inglés NIST, *National Institute of Standards and Technology*) uno de los institutos más importantes en la estandarización de algoritmos y protocolos criptográficos.
- Información, presentaciones y material utilizado en clases presenciales.

Usando estas fuentes se recabó la información necesaria para después realizar la redacción del contenido conceptual descrito en los módulos de la materia. Posteriormente se generaron diversos diagramas para facilitar la visualización y comprensión del texto donde se considere necesario.

Una vez generado el contenido teórico se planearon las actividades y prácticas de programación e investigación que complementen y expandan el conocimiento teórico. Las prácticas estas diseñadas con base en la técnica ABR por lo que deberán tener la siguiente estructura:

- Instrucciones de la actividad, incluyendo los elementos de la metodología ABR: Idea General, Pregunta Esencial y Reto (Apple, 2011).
- Pruebas unitarias.
- Rúbrica de evaluación.

- Referencias de consulta.

Cada unidad constará de una autoevaluación en la que se realizaron las siguientes acciones para obtener una evaluación teórica significativa.

- Identificar la información más relevante, que será aquella que se utilizará en temas posteriores.
- Generar preguntas a partir de la información identificada en el punto anterior que permitan evaluar y reforzar el conocimiento.
- Generar retroalimentación para cada respuesta de cada pregunta generada.

Finalmente, se agruparán las unidades en dos o tres bloques tomando en cuenta la carga de información, el tiempo destinado a cada tema y la relación entre la información de los temas y subtemas. Una vez formados los bloques se realizarán exámenes para cada bloque en los que se evalúen los conceptos más importantes y que sean de utilidad para los siguientes bloques y el curso en general.

Una vez que una unidad completa este terminada, entendiendo por unidad completa el contenido teórico, las actividades prácticas, actividades complementarias y autoevaluaciones, esta se enviará a un asesor pedagógico asignado por CUAIEED que revisará el material generado con el fin de realizar observaciones que puedan mejorar su efectividad. Esta revisión garantiza que el material cumple con un proceso pedagógico adecuado para el aprendizaje en línea, un estilo de escritura correcto, elementos visuales adecuados y actividades y evaluaciones que son posibles de realizar en un entorno digital.

Una vez recibidas las correcciones y observaciones por parte de la asesora pedagógica, estas se aplicarán y en ese momento el material se subirá a la plataforma digital de Moodle que se tiene, a la vez que la CUAIEED hará lo mismo para su plataforma digital.

3.3. Descripción de material completo

El material diseñado para la asignatura de Criptografía se generó con base en los temas incluidos en el plan de estudios 2016 de la carrera de Ingeniería en Computación,

complementando el trabajo presentado en mayo del 2021 por Ricardo Sáenz Barragán en la tesis llamada “Plataforma educativa en línea para la asignatura de Criptografía” (Sáenz, 2021).

Para mayor claridad de las aportaciones de este documento complementando las hechas por Sáenz Barragán, se anexa la Tabla 3.2, donde se muestra en color verde el trabajo realizado por él mientras que en rojo el incluido en esta propuesta. Esta tabla muestra los contenidos desarrollados en cada uno de los trabajos, estos contenidos están clasificados de acuerdo con los tipos de material descritos en la Tabla 1. Cabe aclarar que cada tema no necesariamente tiene materiales de todos los tipos ni tampoco un elemento por cada tipo. Como se puede apreciar, los materiales tipo D (Actividades prácticas de programación basadas en ABR) son presentadas exclusivamente en este trabajo.

Temas	Ricardo Sáenz						Propuesta					
	A	B	C	D	E	F	A	B	C	D	E	F
1. Panorama general												
1.1. Historia de la criptografía												
1.1.1. Criptografía en el mundo												
1.1.2. Historia de la criptografía Criptografía en México												
1.2. Servicio y mecanismos de seguridad												
2. Técnicas clásicas de cifrado												
2.1. Introducción y clasificación de los sistemas de cifrado												
2.1.1. Número de claves: algoritmos simétricos y asimétricos												
2.1.2. Formas de procesar datos: algoritmos en flujo y en bloque												
2.1.3. Operaciones utilizadas: sustitución y transposición												
2.2. Algoritmos de sustitución												
2.2.1. Monoalfabética: Polybios, César, Afin, Playfair y Hill												

2.2.2. Polialfabética: Alberti, Vigenere, Beaufort, Vernam y Enigma												
2.3. Algoritmos de transposición												
2.3.1. Inversa, simple y doble												
2.3.2. Grupos y series												
2.3.3. Filas y columnas												
2.3.4. Máscaras rotativas												
3. Criptografía simétrica o de clave secreta												
3.1. Introducción a la criptografía simétrica												
3.1.1. Características de los algoritmos simétricos												
3.1.2. Principales algoritmos simétricos por flujo: RC4, A5												
3.1.3. Principales algoritmos simétricos por bloque: DES, 3DES, IDEA, AES												
3.2. DES y 3DES (*Data Encryption Standard*)												
3.2.1. Orígenes												
3.2.2. Proceso de cifrado y descifrado												
3.2.3. Aplicaciones												
3.2.4. Análisis de seguridad												
3.3. AES (*Advanced Encryption Standard*)												
3.3.1. Orígenes												
3.3.2. Proceso de cifrado y descifrado (bloques de 128, 192 y 256 bits)												
3.3.3. Modos de funcionamiento												
3.3.4. Aplicaciones												
3.3.5. Análisis de seguridad												
4. Criptografía asimétrica o de clave pública												
4.1.1. Introducción a la criptografía asimétrica												
4.1.2. Características de los algoritmos asimétricos: El Gamal, RSA (Rivest-Shamir-Adleman), DSA (*Digital Signature Algorithm*) y ECC (*Elliptic Curves Cryptosystems*)												

4.1.3. Algoritmo El Gamal												
4.1.3.1. Orígenes												
4.1.3.2. Problema del Logaritmo Discreto												
4.1.3.3. Algoritmo El Gamal												
4.1.3.4. Análisis de seguridad												
4.1.4. Algoritmo RSA												
4.1.4.1. Orígenes												
4.1.4.2. Aritmética Modular y el problema de factorización de primos												
4.1.4.3. Generación de par de llaves												
4.1.4.4. Proceso de cifrado y descifrado												
4.1.4.5. Aplicaciones del algoritmo												
4.1.5. Funciones Hash												
4.1.5.1. Orígenes												
4.1.5.2. Funciones sólo de ida y sus propiedades												
4.1.5.3. Funcionamiento de MD5 y sus ataques												
4.1.5.4. Funcionamiento SHA1 y sus ataques												
4.1.5.5. Funcionamiento SHA2 y SHA3												
4.1.5.6. Aplicaciones de los algoritmos												
4.1.6. Curvas Elípticas												
4.1.6.1. Orígenes												
4.1.6.2. Curvas Elípticas sobre el campo de los números primos: descripción geométrica y algebraica												

4.1.6.3. Curvas Elípticas sobre el campo de los números binarios: descripción geométrica y algebraica											
4.1.6.4. Estándares y aplicaciones											
4.1.7. Introducción a Criptografía Cuántica											
4.1.7.1. Introducción y entrelazamiento cuántico											
4.1.7.2. Propiedades y protocolos											
4.1.7.3. Conjunción de criptografía cuántica y moderna											
5. Gestión de claves											
5.1. Políticas y gestión de claves											
5.1.1. Motivos											
5.1.2. Políticas											
5.2. Tipos de claves											
5.2.1. Estructural											
5.2.2. Maestra											
5.2.3. Primaria y secundaria											
5.2.4. De generación de claves											
5.2.5. De sesión o de mensaje											
5.2.6. De cifrado de archivos											
5.2.7. Generadores y distribución de claves											
5.3. Generadores pseudoaleatorios											
5.3.1. Postulados de Golomb y pruebas estadísticas											
5.4. Protocolos de Distribución de Llaves											
5.4.1. Autenticación Kerberos (Needham-Schroeder y Denning-Sacco)											
5.4.2. KDC (*Key Distribution Center*) y KTC (*Key Translation Center*)											

5.4.3. Diffie-Hellman											
5.4.4. IKE (*Internet Key Exchange*)											
5.4.5. TLS / SSL											
6. Aplicaciones Criptográficas											
6.1. Firmas Digitales											
6.1.1. El Gamal											
6.1.2. DSA											
6.1.3. RSA											
6.1.4. ECDSA											
6.2. Certificados Digitales											
6.2.1. IPSec: Protocolo IKE (*Internet Key Exchange*) y ESP (*Encapsulated Secure Payload*)											
6.2.2. Redes WiFi: Protocolos WEP, WPA, WPA2 y WPA3											
6.2.3. Autenticación de Mensajes: MAC y HMAC											
6.2.4. Herramientas a nivel aplicación: PGP											
6.3. Aplicaciones Descentralizadas											
6.3.1. Hash chains											
6.3.2. Merkle-Trees											
6.3.3. Blockchain											
6.3.4. Aplicaciones de Blockchain: Criptomonedas, Voto Electrónico, Notario Digital											

Tabla 3.2. Contenidos desarrollados en la propuesta por tipo y tema

A continuación, se muestra una descripción detallada de la estructura del curso incluyendo las actividades complementarias y prácticas, autoevaluaciones y exámenes que se desarrollaron de acuerdo con la Tabla 3.2. También se incluye una descripción de cada actividad, así como su objetivo.

3.4.1. Módulo 1: Panorama general

- **Temas:**
  1. Historia de la criptografía
     1.1. Criptografía en el mundo
     1.2. Historia de la criptografía
     1.3. Criptografía en México
  2. Servicio y mecanismos de seguridad
- **Actividades:**
  - **Conceptos básicos de criptografía:** El objetivo de esta actividad es que el estudiante refuerce los conceptos básicos de este módulo, conceptos que serán relevantes a lo largo del curso. Esta relación de concepto-definición se hace por medio de una sopa de letras.
  - **Noticia reciente de criptografía:** El estudiante tendrá que investigar una noticia reciente relacionada con la criptografía. Esta actividad tiene como objetivo contextualizar al alumno en el presente de la criptografía y como está relacionada con su día a día.
- **Autoevaluación:** La autoevaluación consta de 22 preguntas divididas en 4 secciones donde se evaluarán los conocimientos del alumno adquirido en este módulo respecto a los siguientes temas: conceptos básicos de criptografía, historia general de la criptografía e historia de la criptografía en México. Las preguntas están basadas en información que será relevante en los siguientes capítulos.

3.4.2. Módulo 2: Técnicas clásicas de cifrado

- **Temas:**
  1. Introducción y clasificación de los sistemas de cifrado
     1.1. Número de claves: algoritmos simétricos y asimétricos
     1.2. Formas de procesar datos: algoritmos en flujo y en bloque
     1.3. Operaciones utilizadas: sustitución y transposición
  2. Algoritmos de sustitución
     2.1. Monoalfabética: Polybios, César, Afin, Playfair y Hill
     2.2. Polialfabética: Alberti, Vigenere, Beaufort, Vernam y Enigma

3. Algoritmos de transposición
    3.1. Inversa, simple y doble
    3.2. Grupos y series
    3.3. Filas y columnas
    3.4. Máscaras rotativas

- **Actividades prácticas:**
    - **Poema cifrado:** En esta actividad el estudiante tendrá que completar un poema, donde algunas palabras fueron reemplazadas por criptogramas de las palabras originales. Para descifrar los criptogramas, se tendrán que utilizar algunos de los algoritmos de cifrado clásico aprendidos en el módulo. Esta actividad tiene como objetivo que el alumno se familiarice con las principales operaciones que se utilizan en los algoritmos criptográficos modernos que se estudiarán en los siguientes módulos.
- **Autoevaluación:** La autoevaluación consta de 7 preguntas donde se evaluarán los conocimientos del alumno adquirido en este módulo respecto a los siguientes temas: conceptos básicos criptográficos, operaciones criptográficas básicas en algoritmos criptográficos, clasificación de los algoritmos por: contexto histórico, tipo de alfabeto y operaciones utilizadas. Las preguntas se formularon con base en los conceptos y conocimientos que serán necesarios para comprender los siguientes módulos donde se explican algoritmos de criptografía moderna y criptosistemas.

3.4.3. Módulo 3: Criptografía simétrica o de clave secreta

- **Temas:**
    1. Introducción a la criptografía simétrica
        1.1. Características de los algoritmos simétricos
        1.2. Principales algoritmos simétricos por flujo: RC4, A5
        1.3. Principales algoritmos simétricos por bloque: DES, 3DES, IDEA, AES
    2. DES y 3DES (*Data Encryption Standard*)
        2.1. Orígenes

2.2. Proceso de cifrado y descifrado

2.3. Aplicaciones

2.4. Análisis de seguridad

3. AES (*Advanced Encryption Standard*)

3.1. Orígenes

3.2. Proceso de cifrado y descifrado (bloques de 128, 192 y 256 bits)

3.3. Modos de funcionamiento

3.4. Aplicaciones

3.5. Análisis de seguridad

- **Actividades prácticas:**
  - **Práctica A5:** Práctica de programación en que el estudiante deberá programar el algoritmo de cifrado por flujo A5. Tiene como objetivo que el estudiante se familiarice con la aplicación de operaciones criptográficas básicas en un algoritmo criptográfico moderno y el funcionamiento de los algoritmos de cifrado por flujo. Consta de una descripción del problema, un ejemplo del proceso de solución y pruebas unitarias que el algoritmo debe resolver correctamente para considerarse solucionado el problema.
  - **Práctica RC4:** Práctica de programación en la que el estudiante deberá programar el algoritmo de cifrado por flujo RC4. Tiene como como objetivo que el estudiante se familiarice con la aplicación de operaciones criptográficas básicas en un algoritmo criptográfico moderno y el funcionamiento de los algoritmos de cifrado por flujo. Consta de una descripción del problema, un ejemplo del proceso de solución y pruebas unitarias que el algoritmo debe resolver correctamente para considerarse solucionado el problema.
  - **Práctica sDES:** Práctica de programación en la que el estudiante deberá programar el algoritmo de cifrado por flujo sDES. Tiene como objetivo que el estudiante se familiarice con la aplicación de operaciones criptográficas básicas en un algoritmo criptográfico moderno y que entienda el funcionamiento del algoritmo AES, siendo sDES una versión simplificada del algoritmo DES, predecesor de AES y con quien comparte operaciones y una estructura similar. Consta de una descripción del problema, un ejemplo del proceso de solución y

pruebas unitarias que el algoritmo debe resolver correctamente para considerarse solucionado el problema.

- **Actividades:**
  - **Lectura *Exhaustive Cryptanalysis of the NBS DES*:** Esta lectura presenta un análisis sobre distintos factores que comprometen la seguridad del algoritmo DES, además de realizar predicciones sobre el futuro del algoritmo. La lectura ayudará al estudiante a entender el funcionamiento del algoritmo DES y cómo se fundamenta matemática y computacionalmente la seguridad de los algoritmos criptográficos.
  - **Lectura *Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data*:** En esta lectura el estudiante se relacionará con el funcionamiento del algoritmo de cifrado simétrico AES, sus ventajas respecto a algoritmos anteriores y ventajas y desventajas de su seguridad. La lectura reforzará y complementará los conocimientos adquiridos en el material teórico.
- **Autoevaluación:** La autoevaluación consta de 12 preguntas con las que se evaluarán los conocimientos adquiridos en el módulo. Se da énfasis al reforzamiento de las principales características de los algoritmos de criptografía simétrica, los algoritmos más representativos como RC4, A5, DES y AES. Ya que los algoritmos simétricos son fundamentales para los criptosistemas que se estudiaran más adelante, el principal objetivo de la autoevaluación es asegurar que el alumno comprenda las aplicaciones ventajas y desventajas de los algoritmos de criptografía simétrica.

3.4.4. Examen Parcial 1: En este primer examen parcial se evalúa el conocimiento más relevante que el alumno adquirió en los primeros tres módulos del curso. La relevancia del contenido depende de qué tan necesario son es para el avance del estudiante en los siguientes módulos. El examen consta de 17 ejercicios variados de opción múltiple donde cada respuesta correcta o incorrecta tiene retroalimentación para el estudiante. Entre los temas que se evalúan se puede encontrar: definición de seguridad informática y criptografía, clasificación de ataques, servicios de la seguridad informática, criptosistemas clásicos, partes de un criptosistema, clasificación de criptosistemas y conceptos de criptografía simétrica

3.4.5. Módulo 4: Criptografía asimétrica o de clave pública

- **Temas:**
  1. Introducción a la criptografía asimétrica
  2. Características de los algoritmos asimétricos: El Gamal, RSA (Rivest-Shamir-Adleman), DSA (*Digital Signature Algorithm*) y ECC (*Elliptic Curves Cryptosystems*)
  3. Algoritmo El Gamal
     3.1. Orígenes
     3.2. Problema del Logaritmo Discreto
     3.3. Algoritmo El Gamal
     3.4. Análisis de seguridad
  4. Algoritmo RSA
     4.1. Orígenes
     4.2. Aritmética Modular y el problema de factorización de primos
     4.3. Generación de par de llaves
     4.4. Proceso de cifrado y descifrado
     4.5. Aplicaciones del algoritmo
  5. Funciones Hash
     5.1. Orígenes
     5.2. Funciones sólo de ida y sus propiedades
     5.3. Funcionamiento de MD5 y sus ataques
     5.4. Funcionamiento SHA1 y sus ataques
     5.5. Funcionamiento SHA2 y SHA3
     5.6. Aplicaciones de los algoritmos
  6. Curvas Elípticas
     6.1. Orígenes
     6.2. Curvas Elípticas sobre el campo de los números primos: descripción geométrica y algebraica
     6.3. Curvas Elípticas sobre el campo de los números binarios: descripción geométrica y algebraica
     6.4. Estándares y aplicaciones

7. Introducción a Criptografía Cuántica
    7.1. Introducción y entrelazamiento cuántico
    7.2. Propiedades y protocolos
    7.3. Conjunción de criptografía cuántica y moderna

- **Actividades prácticas:**
    - **Práctica *Kid Crypto*:** El estudiante deberá implementar el algoritmo criptográfico Kid Crypto, que es una versión simplificada de RSA, así podrá familiarizarse con la criptografía de llave pública. La práctica consta de una descripción del problema, un ejemplo del proceso de solución y pruebas unitarias que el algoritmo debe resolver correctamente para considerarse solucionado el problema.
    - **Práctica *MD2*:** Práctica de programación en la que el estudiante deberá programar el algoritmo función HASH MD2. Tiene como como objetivo que el estudiante se familiarice con el funcionamiento de los algoritmos solo de ida. Consta de una descripción del problema, un ejemplo del proceso de solución y pruebas unitarias que el algoritmo debe resolver correctamente para considerarse solucionado el problema.
    - **Investigación de funciones sólo de ida con trampa:** Esta investigación tiene como objetivo que el estudiante profundice su conocimiento sobre funciones solo de ida con trampa y sus aplicaciones, usos e importancia para la seguridad informática y la criptografía. La actividad requiere que el alumno investigue 5 funciones trampa y explique cómo se utilizan en la seguridad informática.
- **Actividades:**
    - **Lectura *ElGamal*:** Esta lectura presenta un análisis sobre el funcionamiento de una implementación del esquema de distribución de llave y un esquema de firma digital. La lectura reforzará el conocimiento sobre la criptografía de llave pública, el uso de problemas de logaritmo discreto y campos finitos como problema computacional y su utilidad para la criptografía asimétrica.
    - **Lectura *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*:** Esta lectura presenta la aplicación de RSA como esquema de firmas digitales, los métodos de cifrado y descifrado, así como las bases matemáticas que lo soportan. El estudiante se familiarizará con el problema de

factorización de primos, su utilidad como funciones trampa, así como con el algoritmo RSA.

- **Lectura *A Review Paper of Message Digest 5 (MD5):*** Esta lectura realiza una explicación del funcionamiento del algoritmo MD5, así como un análisis de ataques realizados al mismo. Con esta lectura el estudiante reforzará el conocimiento sobre los algoritmos de solo de ida y cómo se analiza la seguridad de los algoritmos criptográficos.
- **Lectura *Secure Hash Algorithm 1 (SHA1):*** La lectura presenta una explicación detallada sobre el el algoritmo solo de ida SHA-1 que permitirá al estudiante comprender el funcionamiento a detalle de este algoritmo.
- **Lectura *SHA-1 is a Shambles*:** Esta lectura complementaria a la lectura sobre SHA-1 presenta un análisis de seguridad basado en un ataque que compromete la seguridad del algoritmo y todos los criptosistemas que lo implementaron.
- **Lectura *The State of ECC*:** En la lectura se explican las bases matemáticas, su aplicación como algoritmo criptográfico y como criptosistema; además de una explicación de la seguridad. La lectura reforzará la comprensión de la criptografía de curvas elípticas y su importancia para la seguridad informática.
- **Lectura *Experimental Quantum Cryptography*:** Esta lectura presenta una investigación sobre criptografía cuántica por medio de una introducción en la evolución de esta rama de la criptografía, su aplicación como criptosistema, bases de seguridad y sus implicaciones en la seguridad informática.

- **Autoevaluación:** La autoevaluación consta de 11 preguntas donde se evalúan temas esenciales para la adquisición de conocimiento en módulos posteriores, entre los temas se incluye: funcionamiento y aplicación de funciones trampa, funciones solo de ida, funcionamiento RSA y criptografía de curvas elípticas, junto con sus ventajas y desventajas.

3.4.6. Módulo 5: Gestión de claves

- **Temas:**
  1. Políticas y gestión de claves
     1.1. Motivos

1.2. Políticas

2. Tipos de claves
   2.1. Estructural
   2.2. Maestra
   2.3. Primaria y secundaria
   2.4. De generación de claves
   2.5. De sesión o de mensaje
   2.6. De cifrado de archivos
3. Generadores y distribución de claves
   3.1. Generadores pseudoaleatorios
   3.2. Postulados de Golomb y pruebas estadísticas
4. Protocolos de Distribución de Llaves
   4.1. Autenticación Kerberos (Needham-Schroeder y Denning-Sacco)
   4.2. KDC (*Key Distribution Center*) y KTC (*Key Translation Center*)
   4.3. Diffie-Hellman
   4.4. IKE (*Internet Key Exchange*)
   4.5. TLS / SSL

- **Actividades prácticas:**
  - **Investigación Gestión de llaves:** En esta actividad el estudiante deberá generar un certificado digital, esto le permitirá conocer de primera mano el contenido y proceso de generación de este además de generar su par de llaves publica y privada.
- **Actividades:**
  - **Lectura *An Overview of Public Key Infrastructures (PKI):*** La lectura proveé una explicación de cómo se establece una comunicación segura por medio de *PKI.* En el artículo se mencionan las partes involucradas, los procesos, y la funcion de los certificados y llaves publicas y privadas, lo que permitirá al estudiante entender las aplicaciones de la criptografía asimétrica.
  - **Lectura *Kerberos: An Authentication Service for Open Network Systems:*** Esta lectura describe qué es Kerberos, cómo funciona y las partes necesarias que

componen el sistema. Con esto, el estudiante reforzará el conocimiento sobre el tema y sobre los criptosistemas.

- **Autoevaluación:** La autoevaluación de este módulo consta de 10 preguntas en las que se evalúan y refuerzan los conocimientos obre los temas abordados en este módulo, en partículas: conceptos sobre la gestión de llaves, su importancia para la seguridad, tipos y propiedades de las llaves, así como los esquemas de distribución de llave más importantes como Diffie-Hellman, IKE, PKS y Kerberos.

3.4.7. Módulo 6: Aplicaciones Criptográficas

- **Temas:**
  1. Firmas Digitales
     1.1. El Gamal
     1.2. DSA
     1.3. RSA
     1.4. ECDSA
  2. Certificados Digitales
     2.1. IPSec: Protocolo IKE (*Internet Key Exchange*) y ESP (*Encapsulated Secure Payload*)
     2.2. Redes WiFi: Protocolos WEP, WPA, WPA2 y WPA3
     2.3. Autenticación de Mensajes: MAC y HMAC
     2.4. Herramientas a nivel aplicación: PGP
  3. Aplicaciones Descentralizadas
     3.1. Hash chains
     3.2. Merkle-Trees
     3.3. Blockchain
     3.4. Aplicaciones de Blockchain: Criptomonedas, Voto Electrónico, Notario Digital
- **Actividades:**
  - **Lectura *Do you need a Blockchain:*** al finalizar esta lectura el estudiante comprenderá mejor las diferencias de blockchain como aplicación de redes

descentralizada respecto a las redes tradicionales, las ventajas y desventajas, implicaciones técnicas y de usabilidad.

  - **Lectura *Analysing WPA3's Dragonfly Handshake:*** En esta lectura se presenta un análisis de seguridad del *Dragonfly Handshake* utilizado en el protocolo WPA3, con el que el estudiante reforzará su conocimiento sobre el protocolo de seguridad para redes inalámbricas WPA3, y la seguridad en redes inalámbricas.

- **Actividades prácticas:**
  - **Investigación Aplicaciones de TLS:** Con esta investigación el estudiante reforzará su conocimiento sobre el protocolo TLS, conocerá sus aplicaciones y cómo se utiliza en ellas. Deberá investigar el uso de TLS en SMTP, VPN, y HTTP; explicando los pasos en esos procesos y las propiedades de seguridad que proporciona cada protocolo.
  - **Investigación Bitcoin VS Ethereum:** Esta actividad permitirá a los estudiantes familiarizarse con una implementación diferente de blockchain llamada Ethereum, reforzará sus conocimientos sobre blockchain y comprenderá mejor su uso para establecer sistemas de dinero digital.
- **Autoevaluación:** La autoevaluación consta de 13 preguntas donde se evalúan los puntos principales de los protocolos y sus conceptos, se da énfasis a los subtemas de aplicaciones descentralizadas, los conceptos necesarios para que el estudiante comprenda la relevancia de esta tecnología y evaluando las bases necesarias para que expanda o especialice sus conocimientos.

3.4.8. Examen Parcial 2: En el segundo examen parcial se evalúa el conocimiento más relevante que el alumno adquirió en los módulos cuatro cinco y seis, sin contar lo evaluado en el primer examen parcial. La relevancia del contenido depende de qué tan necesario son es para el avance del estudiante en los siguientes módulos. El examen consta de 40 ejercicios variados de opción múltiple donde cada respuesta correcta o incorrecta tiene retroalimentación para el estudiante. Entre los temas que se evalúan se puede encontrar: funciones criptográficas, criptosistemas asimétricos, esquema de llave pública, firma digital, certificados digitales, tipos de llaves, esquemas de distribución de llave, criptografía de

curvas elípticas, criptografía cuántica, protocolos de seguridad en redes, criptografía descentralizada y *blockchain*.

Con este diseño de material cumplimos con el objetivo de la materia que es “Reconocer los diferentes algoritmos y protocolos criptográficos a través de las distintas metodologías y técnicas de cifrado orientadas a brindar seguridad informática.”, además de cumplir con el objetivo de este trabajo que es generar material teórico y práctico de distribución digital utilizando metodología de aprendizaje basado en retos. Siempre apegados al plan de estudios 2016 oficial para la carrera de Ingeniería en Computación.

Capítulo 4

4. Resultados

En esta sección detallaremos el material desarrollado que se describió previamente. Como se pudo apreciar en la sección anterior, todo el material teórico y práctico generado para este curso comparten la misma estructura. En afán de no ser redundantes, no mostraremos todo el material, en su lugar se tomará una muestra representativa de los tipos de material generados y se dará una breve explicación de su composición y estructura. Sin embargo, todos los documentos del material generado serán anexados a este para su consulta.

4.1. Unidad o módulo teórico

Cada módulo está conformado por los temas dictados en el plan de estudios para la respectiva unidad que representa ese módulo. Cada tema de un módulo está desarrollado en un sólo documento para facilitar y agilizar el proceso de revisión y desarrollo. Un ejemplo de esto puede verse en la Figura 4.1.

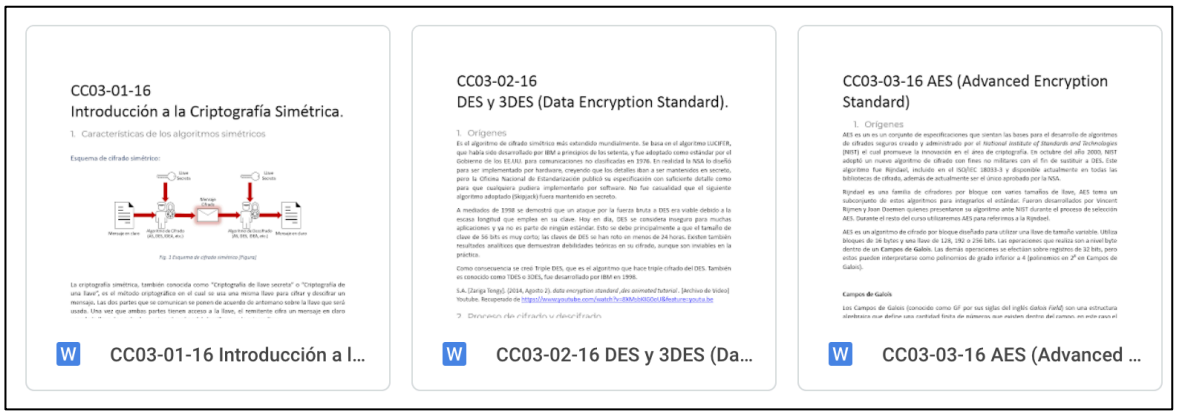


Figura 4.1. Captura de pantalla de los documentos temas que conforman los temas la Unidad 3: "Plataforma educativa en línea para la asignatura de Criptografía".

Los temas constan de una introducción donde se contextualizan los subtemas del tema respecto al curso, a la criptografía y seguridad; seguido de los subtemas, también apegados al plan de estudios. Un ejemplo puede verse en la Figura 4.2 donde se introduce el tema 3.1.

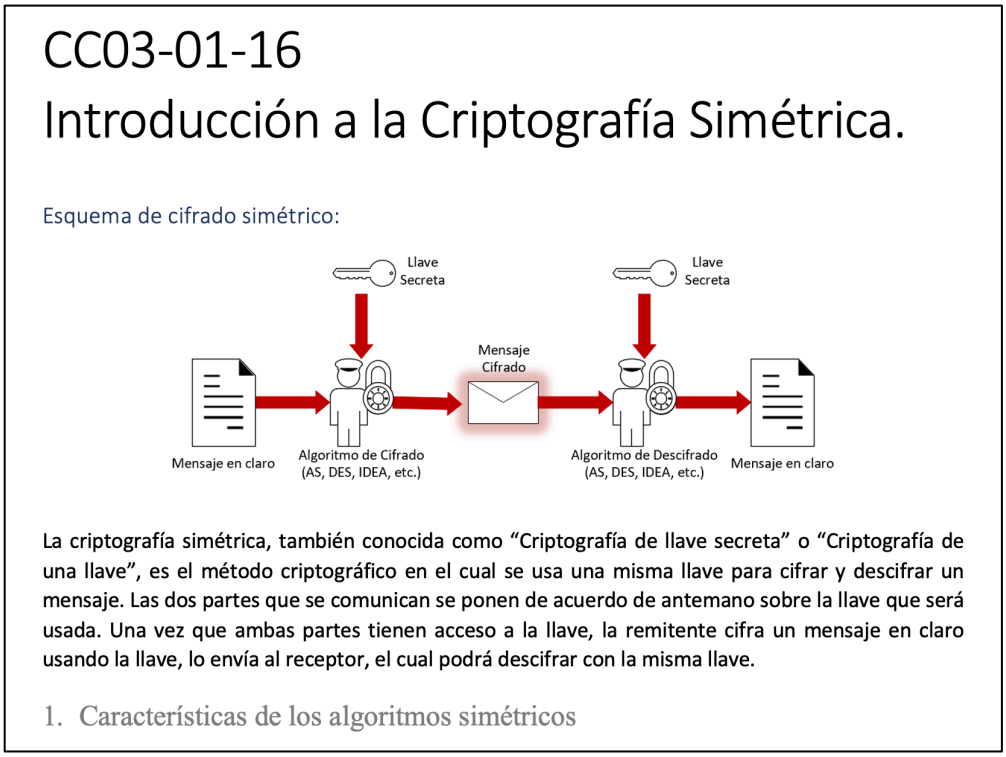
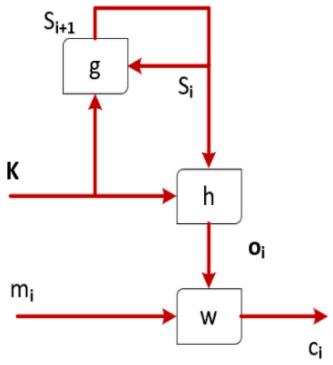


Figura 4.2. Captura de pantalla de introducción del tema: Introducción a la Criptografía Simétrica

El contenido de cada tema y subtema está complementado con imágenes, tablas y diagramas que ayudan a visualizar y comprender mejor las explicaciones, como se observa en el ejemplo de la Figura 4.3. donde se muestra el diagrama de un generador asíncrono. En algunas unidades se incluyeron las animaciones y videos generados por el Ing. Ricardo Sáenz como parte de su tesis llamada "Plataforma educativa en línea para la asignatura de Criptografía".

Generadores Síncronos

Un generador *síncrono* es aquel en el que la secuencia es calculada de forma independiente tanto del texto en claro como del texto cifrado. Dado por las siguientes ecuaciones:



$$s_{i+1} = g(s_i, k)$$
$$o_i = h(s_i, k)$$
$$c_i = w(m_i, o_i)$$

Fig. 6 Generadores síncronos funcionamiento [Figura]

Donde:

- **k** es la llave
- **S_i** es el estado interno del generador
- **S_0** es el estado inicial
- **O_i** es la salida en el instante **i**
- **m_i** y **c_i** son la i-ésima porción del texto claro y cifrado respectivamente
- **w** es una función reversible, usualmente OR exclusivo

En muchos casos, la función **h**(x) depende únicamente de s_i , siendo k = s_0.

Figura 4.3. Captura de pantalla de "Generadores Asíncronos" del subtema "Cifrado por flujo" de la Unidad 3: "Criptografía simétrica o de clave secreta".

4.2. UAPA

Las Unidades de Apoyo para el Aprendizaje o UAPA, sugerencias por parte de la CUAIEED que se decidieron implementar y consta de educativo destinado a ser público y accesible por cualquiera, en este caso disponible por medios electrónicos. Los temas seleccionados fueron elegidos por su relevancia en la actualidad además de por su aporte a diversas carreras de la UNAM, más allá de la Ingeniería en Computación. A continuación, presentamos un listado de los temas que son UAPA y la unidad a la que pertenecen.

- Unidad 3: AES (Advanced Encryption Standard)
- Unidad 4: RSA
- Unidad 4: Funciones HASH

- Unidad 4: Introducción a la criptografía cuántica
- Unidad 6: Blockchain

La estructura interna del tema es igual que la descrita en el punto anterior unidad o módulo teórico, se introducen los temas, se desarrollan y se complementan las explicaciones con animaciones, imágenes, tablas y diagramas. En la Figura 4.4. se muestra un ejemplo de la estructura del tema Introducción a la Criptografía Cuántica, con una introducción al tema, subtemas con contenido y material de apoyo.

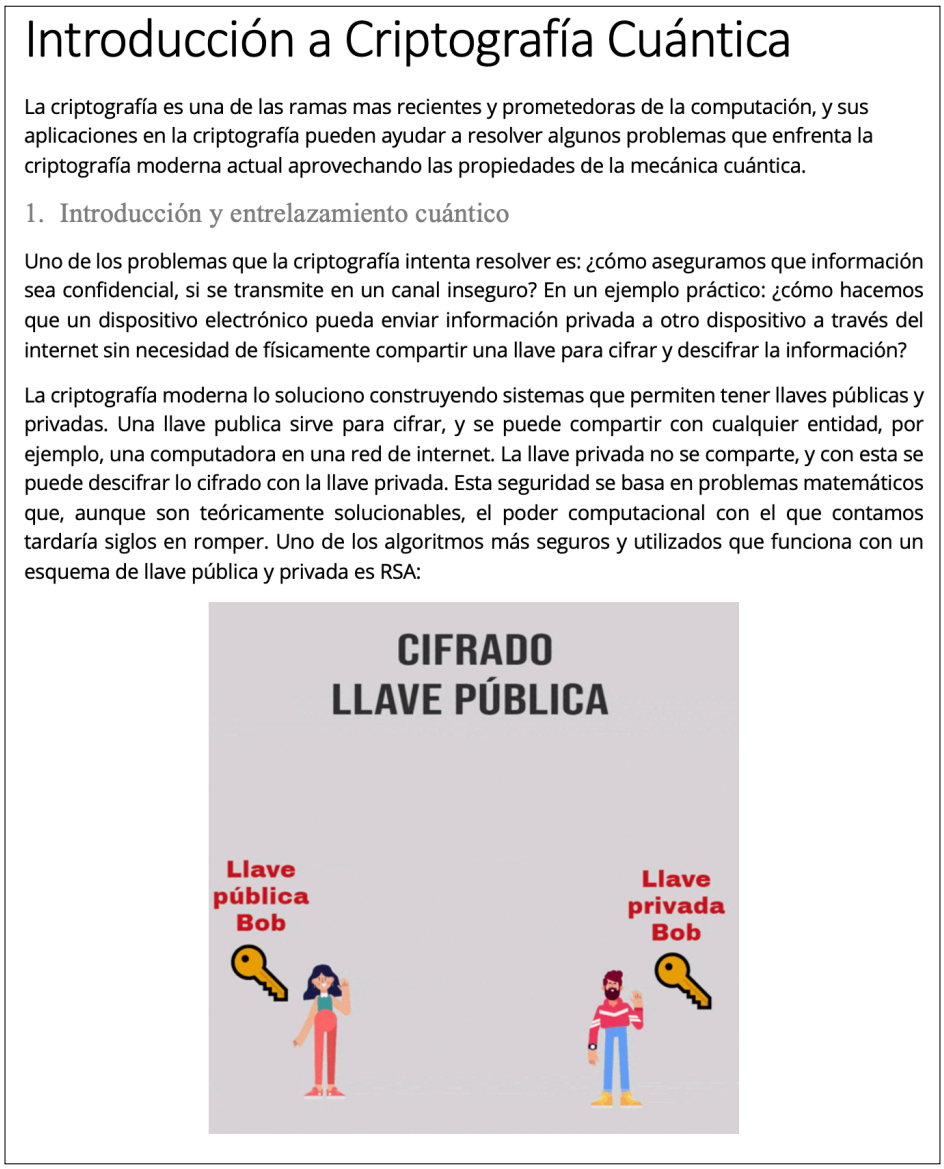


Figura 4.4. Captura de pantalla de la UAPA "Introducción a la Criptografía Cuántica"

Al ser destinados a ser distribuidos de forma individual, fue necesario agregarles antecedentes de temas anteriores, en cuanto al orden de los temas en el plan de estudios. Cabe

mencionar que las UAPA al ser de alcance general tienen autoevaluaciones propias del tema, a comparación de los demás temas del material que no cuentan con una. Esto con el objetivo de que cualquiera que consulte el material pueda evaluar su aprendizaje sobre el contenido específico de esa UAPA. En la Figura 4.5 se observa una sección de la actividad de autoevaluada de la UAPA Introducción a la Criptografía Cuántica.

COMPONENTE	DESARROLLO
Actividad 1	Completa las oraciones con las opciones disponibles, se pueden utilizar más de una vez: **Qubit** **Distribución de llave** **Spin** **Entrelazamiento** 1. El _____ es una partícula elemental utilizada en la criptografía cuántica para representar información. **Qubit:** Correcto **Cualquier otra respuesta:** Incorrecto. Es una partícula fundamental, como el fotón. 2. La criptografía cuántica permitió solucionar algunos problemas de seguridad en la _____, aunque sigue siendo necesario más herramientas como la autenticación. **Distribución de llave:** Correcto **Cualquier otra respuesta:** Incorrecto. En este proceso es necesario para poder establecer un secreto compartido de forma segura, y poder establecer una comunicación cifrada con el secreto. 3. El _____ es el movimiento constante de un ____, y puede ser en cualquier sentido y es afectado muy fácilmente por fenómenos externos. **Spin (1) y qubit (2):** Correcto **Cualquier otra respuesta:** Incorrecto. Este movimiento es característico de este tipo de partículas, y dependiendo de su posición se puede interpretar como valor para transmitir información. 4. El ____ es una propiedad física que permite que dos o más _____ estén conectados y se puedan predecir el estado de un elemento del par, observando otro. **Entrelazamiento (1) y qubit (2):** Correcto **Cualquier otra respuesta:** Incorrecto. En este fenómeno, dos partículas se ligan y se comportan igual ante los mismos estímulos externos. Es utilizado en el protocolo E91.

Figura 4.5. Actividad de evaluación 1, UAPA: "Introducción a la Criptografía Cuántica"

Tanto las actividades como las autoevaluaciones en las UAPA deben ser auto gestionables, es decir, el consultante debe poder evaluarse sin necesidad de la intervención de un docente, por lo que se optó por el uso de cuestionarios con preguntas de opción múltiple, elección de verdadero falso y completar columnas y frases. Estos ejercicios pueden ser implementados en diversas plataformas educativas y ofrecen una retroalimentación inmediata para todas las respuestas correctas e incorrectas, cumpliendo con el requerimiento de ser auto gestionables. En la Figura 4.6 se observa una sección del cuestionario de autoevaluación de la UAPA Introducción a la Criptografía Cuántica.

Autoevaluación	Responde verdadero o falso 1. La principal diferencia entre un bit y un qubit es que un bit se forma a partir de la medición de un voltaje y un qubit dependiendo del spin que tiene una partícula cuántica elemental. **Falso**: Incorrecto *Para darle valor a un bit se lee un voltaje, el valor de un qubit se determina con la posición de su spin, cada que se toma lectura, el estado del qubit se altera.* **VERDADERO**: Correcto. *Para darle valor a un bit se lee un voltaje, el valor de un qubit se determina con la posición de su spin, cada que se toma lectura, el estado del qubit se altera.* 2. La criptografía cuántica se utiliza principalmente para la distribución de llaves **Falso**: Incorrecto *Un servidor o un tercero genera una serie de qubits que se utilizan para generar una llave que se utilizará para tener una comunicación segura entre el servidor y el cliente.* **VERDADERO:** Correcto. *Un servidor genera un conjunto de qubits a un cliente, después de un proceso de validación exitoso se utilizan los estados de los qubits para poder generar una llave utilizable para establecer una comunicación segura.* 3. El entrelazamiento cuántico se da entre dos o más qubits y permite saber el comportamiento de los qubits sin observarlos. **Falso**: Incorrecto *Los qubits entrelazados no pueden ser controlados a distancia modificando alguno de los pares. Más bien, es posible determinar el estado de un qubit sin observar su par entrelazado en vez de hacerlo directamente.* **VERDADERO**: Correcto. *Los qubits entrelazados no pueden ser controlados a distancia modificando alguno de los pares. Más bien, es posible determinar el estado de un qubit sin observar su par entrelazado en vez de hacerlo directamente.*

Figura 4.6. Extracto de Autoevaluación de UAPA: "Introducción a la Criptografía Cuántica"

4.3. Evaluaciones

El proceso de evaluación es importante, ya que les permite saber tanto a alumnos como a docentes si se ha cumplido con el objetivo de la unidad o actividad. A continuación, se describen los diversos instrumentos de evaluación usados en cada módulo.

4.3.1. Evaluación de módulo

Al finalizar, todos los módulos tienen una evaluación auto gestionable compuesta de 7 a 15 preguntas de opción múltiple con retroalimentación para todas las respuestas correctas e incorrectas. El objetivo que se tuvo en mente al redactar las preguntas fue que el estudiante reforzara los conocimientos más importantes de ese módulo y que fueran de relevancia para los módulos posteriores y en general importantes para la aplicación de la criptografía en el ámbito profesional o especialización. La Figura 4.7 muestra una sección de la Autoevaluación de la unidad 4 Introducción a la Criptografía Simétrica.

Autoevaluación	Selecciona la respuesta correcta Función matemática que es fácil de calcular directamente, pero realizar su inversa es muy complejo: **Función directa:** Incorrecto La función trampa es normalmente muy difícil de invertir, debido a la complejidad matemática, que se traduce en necesidad de procesamiento. Haciendo que sean excelentes funciones para fines criptográficos. **Factorización de primos:** Incorrecto La factorización de primos es el proceso inverso del producto de primos, que sí es función trampa, ya que la cantidad de capacidad de procesamiento que se necesita para resolverla es sumamente alta y tomaría años. **Función trampa:** Correcto La función trampa es normalmente muy difícil de invertir, debido a la complejidad matemática, que se traduce en necesidad de procesamiento. Haciendo que sean excelentes funciones para fines criptográficos. **Función indeterminada:** Incorrecto La función trampa es normalmente muy difícil de invertir, debido a la complejidad matemática, que se traduce en necesidad de procesamiento. Haciendo que sean excelentes funciones para fines criptográficos.
	Selecciona la respuesta correcta ¿Qué problema resuelve la criptografía cuántica respecto a la criptografía moderna? **Mejora la distribución de llaves:** Correcto Los estándares actuales de criptografía cuántica permiten realizar la distribución de llaves a través de un canal destinado únicamente a comunicar información por medio de *qubits*, En este canal se transmiten los mensajes necesarios para generar las llaves con las cuales se puede realizar una comunicación segura. Sin embargo, sólo resuelve la distribución de llaves, aún es necesario implementar otros métodos para garantizar la autenticación, integridad de datos y confidencialidad. **Garantiza la confidencialidad de los mensajes enviados en un canal inseguro:** Incorrecto Los estándares actuales de criptografía cuántica permiten realizar la distribución de llaves a través de un canal destinado únicamente a comunicar información por medio de *qubits*, La forma en la que esta llave es utilizada está fuera de estos estándares, por lo que no puede garantizar la confidencialidad de los mensajes. **Hace innecesaria la autenticación:** Incorrecto Los estándares actuales de criptografía cuántica permiten realizar la distribución de llaves a través de un canal destinado únicamente a comunicar información por medio de *qubits*, Si se llegara a personificar a una entidad para obtener la llave a través de este proceso, se podría compartir información entre cliente personificado y servidor. **Garantiza confidencialidad en la comunicación:** Incorrecto Los estándares actuales de criptografía cuántica permiten realizar la distribución de llaves a través de un canal destinado únicamente a comunicar información por medio de *qubits*, En este canal se transmiten los mensajes necesarios para generar las llaves con las cuales se puede realizar una comunicación segura. Sin embargo, sólo resuelve la distribución de llaves, aún es necesario implementar otros métodos para garantizar la autenticación, integridad de datos y confidencialidad.

Figura 4.7. Extracto de autoevaluación de Unidad 4: "Criptografía Asimétrica o de llave pública".

4.3.2. Examen

Los exámenes son evaluaciones que engloban el contenido más importante de varias unidades, para fines de este curso se plantearon dos exámenes divididos de la siguiente forma:

- Examen 1:
    - Unidad 1

- Unidad 2
- Unidad 3

- Examen 2:
  - Unidad 4
  - Unidad 5
  - Unidad 6

Al igual que las autoevaluaciones de módulo, las preguntas de estos exámenes están pensadas de forma que sean auto gestionables, por lo que todas las respuestas tienen retroalimentación. Se introdujo mayor variedad de ejercicios con el fin de presentar mayor reto y de evaluar de forma más integral los conocimientos de os estudiantes. A continuación, se muestran algunos de los ejercicios introducidos para exámenes. En las Figuras 4.8. 4.9. y 4.10. se muestran ejemplos de ejercicios incluidos en el Examen Parcial 1.

3- Clasifica los siguientes ataques entre Pasivo y Activo: (4 puntos)

Ataque	Tipo (Activo/Pasivo)
Suplantación de identidad	**Activo**
Distribución de información no autorizada	**Pasivo**
Retraso de mensaje	**Activo**
Bloqueo de mensajes	**Activo**
Distribución de datos	**Pasivo**
Reproducción de mensaje	**Activo**
Análisis de tráfico de datos	**Pasivo**
Negación de servicio	**Activo**
Destrucción de mensajes	**Activo**
Modificación de mensaje	**Activo**
Copia de mensaje	**Activo**

Pasivo	Activo
¡Correcto! Los ataques pasivos son aquellos que solo observan datos en una comunicación.	**¡Correcto! Los ataques activos son aquellos que buscan causar la modificación o alteración de datos.**
¡Incorrecto! Recuerda que los ataques pasivos son aquellos que solo observan datos en una comunicación, como es el caso de la intercepción, distribución de datos, etc.	**¡Incorrecto! Recuerda que los ataques activos son aquellos que buscan causar la modificación o alteración de datos, como es el caso de la suplantación, modificación, interrupción, etc.**

Figura 4.8. Ejercicio de clasificación de ataques, Examen 1.

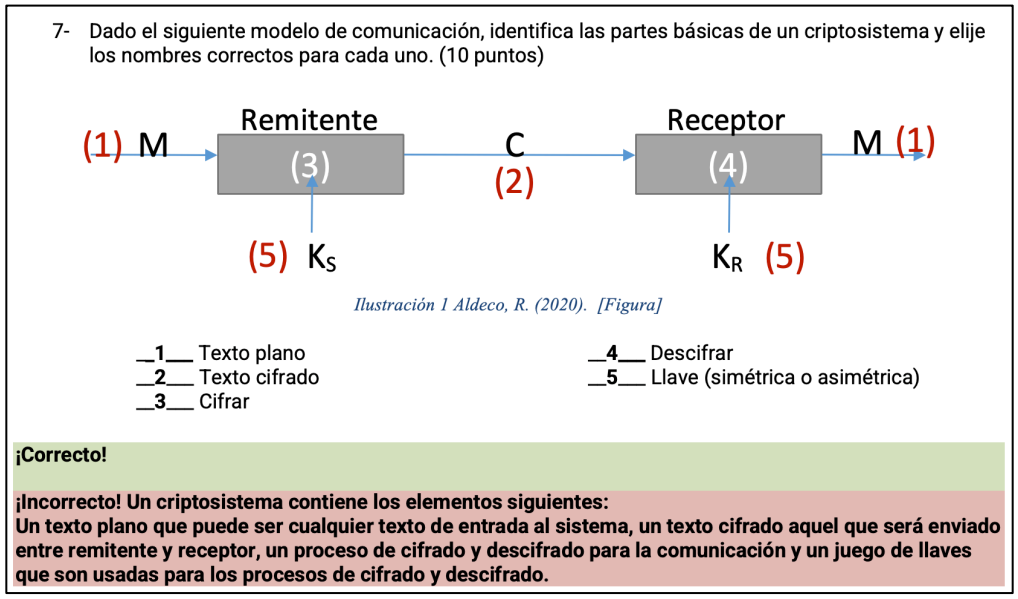


Figura 4.9. Ejercicio relación de conceptos en un diagrama, Examen 1.

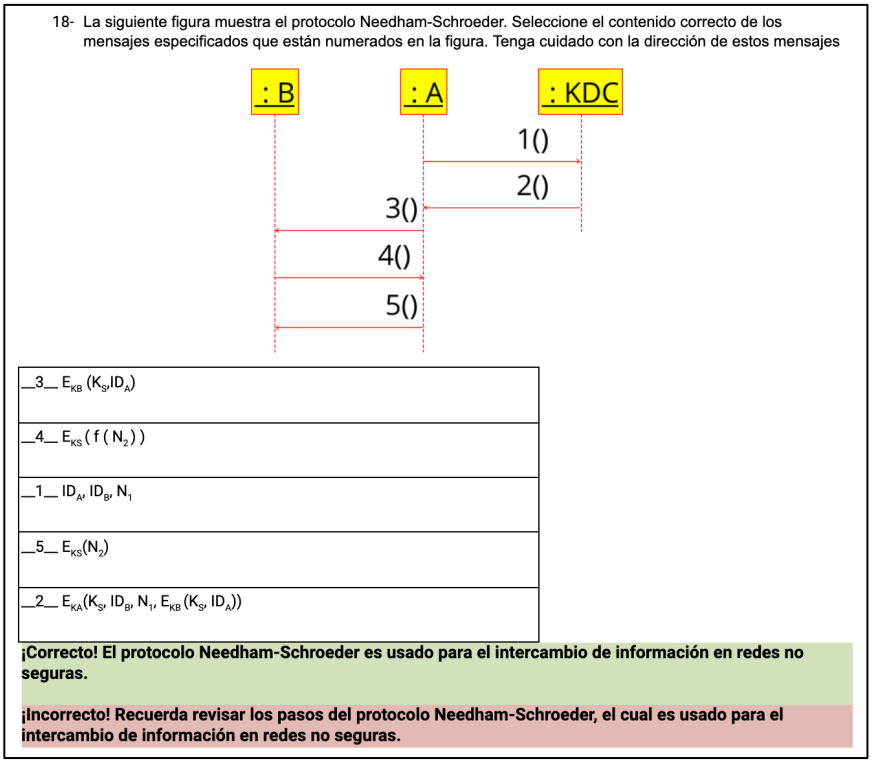


Figura 4.10. Ejercicio de identificación de orden de mensajes en protocolo, Examen 2.

4.4. Actividades

Existen dos tipos de actividades o tareas a lo largo del curso: (1) lectura e (2) investigación. Ambos tipos tienen como objetivo reforzar los conocimientos adquiridos en los temas permitiéndole al estudiante conocer más ya sea a través de lecturas que profundizan más en

el tema o realizando investigaciones propias. A continuación, una descripción mas detallada de las actividades y la evaluación de estas. Cabe mencionar que, a diferencia de los exámenes y evaluaciones de módulo, las actividades fueron diseñadas para ser evaluadas por un docente por lo que se anexaron rúbricas como guía de evaluación, por lo tanto, no son auto gestionables.

Las lecturas se propusieron como actividades para complementar el conocimiento adquirido en clase, ya que en ellas se abordan temas a mayor detalle. Al ser publicaciones académicas y de investigación, le permiten al estudiante tener un contexto real sobre la criptografía, la seguridad informática y la investigación de algoritmos, protocolos y criptosistemas nuevos y su seguridad. Como entregable se deberá enviar una síntesis de la lectura, por lo que este ejercicio no está destinado a ser auto gestionable. Se generó una rúbrica única para todas las lecturas, de forma que el estudiante pueda autoevaluarse antes de entregar la actividad y que el profesor evalúe de forma ágil y consistente a lo largo del curso. La rúbrica generada para la evaluación de las lecturas se muestra en la Figura 4.11.

Criterios	**Escala de calificación**					
Presentación Excelente formato que contiene los elementos visuales y organizativos descritos en las plantillas dadas.	2.5 Excelente	2.25 Muy bien	2 Bien	1.75 Satisfactorio	1.5 Necesita mejorar	0 No presento
Contenido y estructura El contenido y la estructura siguen los descritos en la plantilla, incluida una solución clara al problema dado.	2.5 Excelente	2.25 Muy bien	2 Bien	1.75 Satisfactorio	1.5 Necesita mejorar	0 No presento
Escritura Describe de forma clara y concisa los objetivos del trabajo.	2.5 Excelente	2.25 Muy bien	2 Bien	1.75 Satisfactorio	1.5 Necesita mejorar	0 No presento
Claridad Discutir de forma clara y concisa las conclusiones de la etapa correspondiente del proyecto.	2.5 Excelente	2.25 Muy bien	2 Bien	1.75 Satisfactorio	1.5 Necesita mejorar	0 No presento

Figura 4.11. Rúbrica para actividades de lectura.

Las actividades de investigación requieren que el estudiante busque información para contestar preguntas o resolver actividades. Al igual que las lecturas, no son actividades auto gestionables. Todas las investigaciones se evalúan con un entregable escrito con los resultados solicitados en la actividad. La rúbrica generada para la evaluación de las actividades se muestra en la Figura 4.12., mientras que en la Figura 4.13. se muestra la actividad de la unidad 5 “Investigación de gestión de llaves”

Criterios	**Escala de calificación**					
Presentación Excelente formato que contiene los elementos visuales organizados y legibles.	2 Excelente	1.75 Muy bien	1.5 Bien	1.25 Satisfactorio	1 Necesita mejorar	0 No presento
Contenido y estructura El contenido y la estructura siguen los descritos en las instrucciones y el docente, incluida una solución clara al problema dado.	3 Excelente	2.5 Muy bien	2 Bien	1.5 Satisfactorio	1 Necesita mejorar	0 No presento
Escritura Describe de forma clara y concisa los objetivos de la investigación.	2 Excelente	1.75 Muy bien	1.5 Bien	1.25 Satisfactorio	1 Necesita mejorar	0 No presento
Claridad Discutir de forma clara y concisa las conclusiones de la investigación..	3 Excelente	2.5 Muy bien	2 Bien	1.5 Satisfactorio	1 Necesita mejorar	0 No presento

Figura 4.12. Rúbrica para actividades de investigación.

Actividad 3: Investigación de Gestión de llaves

1- Siguiendo los pasos mostrados a continuación, realizar un certificado digital:
   a. Ingresar a: Free SSL Digital Certificate Tools (getacert.com)
   b. Hacer clic en Create your Free Digital Certificate instantly (getacert.com) para crear un certificado.
   c. Descarga los archivos generados.
   d. Subir el certificado creado en Submit your CSR and Create free Digital Certificate instantly (getacert.com)
   e. Abre el documento generado y revisa la información dentro de él.
2- Sube capturas de pantalla del certificado generado que tenga tu nombre completo en él.

Figura 4.13. Ejercicio "Generación de Gestión de Llaves", Unidad 5.

4.5. Actividades de programación

Las actividades de programación forman parte de las actividades prácticas y son pequeños laboratorios que presentan un reto al estudiante que debe resolver por medio de la programación. Todas las actividades de programación están basadas en algoritmos o versiones simplificadas de los algoritmos que se ven a lo largo del curso. El formato de ejercicios es el siguiente:

- Explicación breve del algoritmo.
- Explicación del proceso del algoritmo.
- Ejemplos de entrada salida del algoritmo (pruebas unitarias).
- Preguntas sobre el algoritmo.

Las explicaciones tienen como objetivo introducir al estudiante con el algoritmo seguido de explicación paso a paso de como funciona el algoritmo. De esta forma el estudiante entiende qué es lo que debe resolver al momento de programar. Después de la explicación se ofrecerán ejemplos de entrada y salida que el estudiante podrá utilizar para evaluar su código (pruebas unitarias). Finalmente, el estudiante deberá contestar unas preguntas sobre el algoritmo que resolvió, estás preguntas tienen un enfoque analítico que permitan evaluar la compresión del problema que resolvió. Estas actividades tienen su propia rúbrica con la que los docentes pueden evaluar las entregas de los estudiantes. En la Figura 4.14. se muestra la rúbrica utilizada para evaluar las actividades de programación y sus entregables, mientras que en la Figura 4.15. y 4.16. se muestra una sección de la práctica "*Kyd Crypto*" de la unidad 4, junto con las pruebas unitarias propuestas.

Criterios	Escala de calificación					
Ejecución del programa La ejecución del programa se realiza con éxito (sin problemas de ejecución o compilación).	3.4 Excelente	3 Muy bien	2.666 Bien	2.333 Satisfactorio	2 Necesita mejorar	0 No presento
Explicación del programa El alumno demuestra conocimiento del código presentado y es capaz de explicarlo correctamente.	3.3 Excelente	3 Muy bien	2.666 Bien	2.333 Satisfactorio	2 Necesita mejorar	0 No presento
Implementación de programa El programa implementa la técnica solicitada, el lenguaje de programación o cualquier otro requisito indicado en la descripción del trabajo.	3.3 Excelente	3 Muy bien	2.666 Bien	2.333 Satisfactorio	2 Necesita mejorar	0 No presento

Figura 4.14. Rúbrica de actividades de programación.

Práctica 4. Kid Krypto

Kid Krypto

"Kid Krypto" (Fellows, M. & Koblitz, N.) es una familia de criptosistemas desarrollada por Michael Fellows y Neal Koblitz para la enseñanza de la criptografía sin utilizar las matemáticas avanzadas.

Kid Krypto usa dos claves diferentes pero relacionadas para el cifrado y descifrado. Para configurar *Kid Krypto*, Ana elige cuatro enteros aleatorios *a, b, A* y *B*. Luego calcula:

$$M = ab - 1$$
$$e = AM + a$$
$$d = BM + b$$
$$n = \frac{ed - 1}{M}$$

Ella hace que el par ***(n, e)*** esté disponible como su llave pública y mantiene **d** como su llave privada. Todos los otros números pueden ser descartados; pero en ningún momento deberían ser revelados. Los mensajes en este sistema son enteros ***x < n***.

Supongamos que Beto desea enviar el mensaje **x** a Ana. Lo cifra multiplicando primero ***x*** por ***e*** y dividiendo el producto ***xe* entre *n***. El resto de esta división es el texto cifrado **y**. Ana descifra multiplicando por ***d*** para obtener ***yd*** y luego divide este producto entre ***n***. El resto de esta división es el texto plano.

Para ver esto en acción, supongamos que Ana elige

$$a = 3, b = 4, A = 5, B = 6$$

Entonces es fácil determinar

$$M = 11, e = 58, d = 70, n = 369$$

Su llave pública es *(369,58)* y su llave privada es *70*.

Supón que Beto quiere cifrar $x=200$. Lo multiplica por $e=58$ para obtener $xe= 11600$. Divide entre $n=369$ dejando como residuo 161. Este es el texto cifrado *y* que le envía a Ana.

Figura 4.25. Extracto de explicación de la actividad de programación "Práctica 4 Kid Crypto".

Vectores de Prueba					
a	**b**	**A**	**B**	**Texto plano**	**Texto cifrado**
3	4	5	6	200	161
3	4	5	6	650	62
9	11	5	8	1028	572
9	11	5	8	54	2546
47	22	11	5	12223	13268
47	22	11	5	4356	28929

Pasos

1. Usa *Kid Krypto* con valores a = 10, b = 2, A = 15, B = 5 para cifrar x = 112.
2. Responde las siguientes preguntas.
    a. ¿Se pueden elegir todos los enteros para configurar *Kid Krypto*? ¿Por qué?
    b. Si respondes no en la pregunta anterior, di qué números no se pueden usar y por qué.

Figura 4.16. Ejemplos de pruebas y preguntas de actividad práctica "Práctica 4: Kid Crypto".

4.6. Estructura de curso y material generado

La estructura de temas, actividades, actividades prácticas, autoevaluaciones y exámenes se mantiene como se mencionó en el capítulo *4.7 Descripción de material completo*. La totalidad del material teórico y práctico generado podrá ser consultado en *Google Drive* en la siguiente dirección:

https://drive.google.com/drive/folders/1CP2YCaq2EfEkWdK349Y_yyMbOWCVREUy

Para la presentación de este trabajo se habilitó una plataforma ***Moodle*** como demo con el material teórico en la siguiente dirección*:*

http://45.33.120.30/moodle/course/view.php?id=3#section-1

A continuación, una breve descripción de la organización del material en cada una de las plataformas:

- **Material en Google Drive**

  El material se encuentra ordenado por unidades, las rubricas y exámenes se encuentran en carpetas separadas ya que son documentos globales no dependientes de cada unidad. Esto se puede ver en la Figura 4.17.

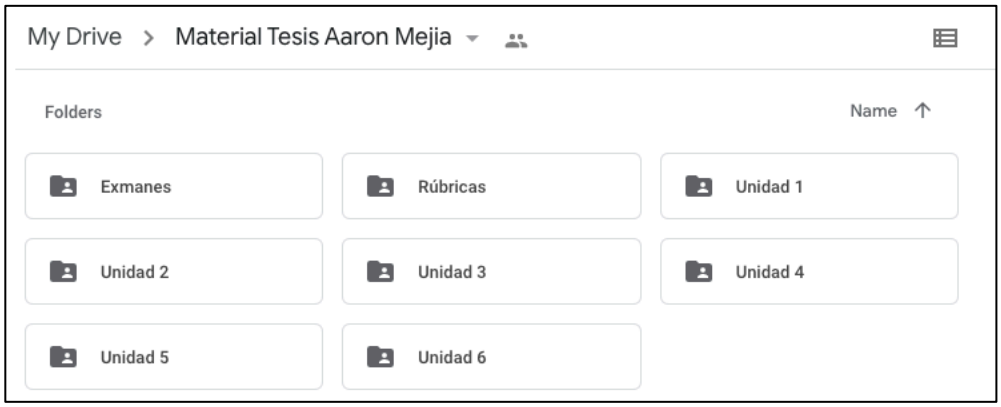


Figura 4.17. Material generado y almacenado en Google Drive.

Dentro de cada unidad se encuentran los temas (temas del curso y UAPA), actividades, actividades prácticas y autoevaluaciones correspondientes a ella como se muestra en la Figura 4.18.

Figura 4.18. Contenido de la Unidad 4 en Google Drive.

- **Material en Moodle**

Dentro de Moodle se encuentra todo el material teórico generado ordenado de forma secuencial, dividido en unidades y por temas de unidad como se muestra en la Figura 4.19. En esta plataforma se pueden dar de alta profesores y alumnos para que puedan interactuar con el material de manera autogestiva.

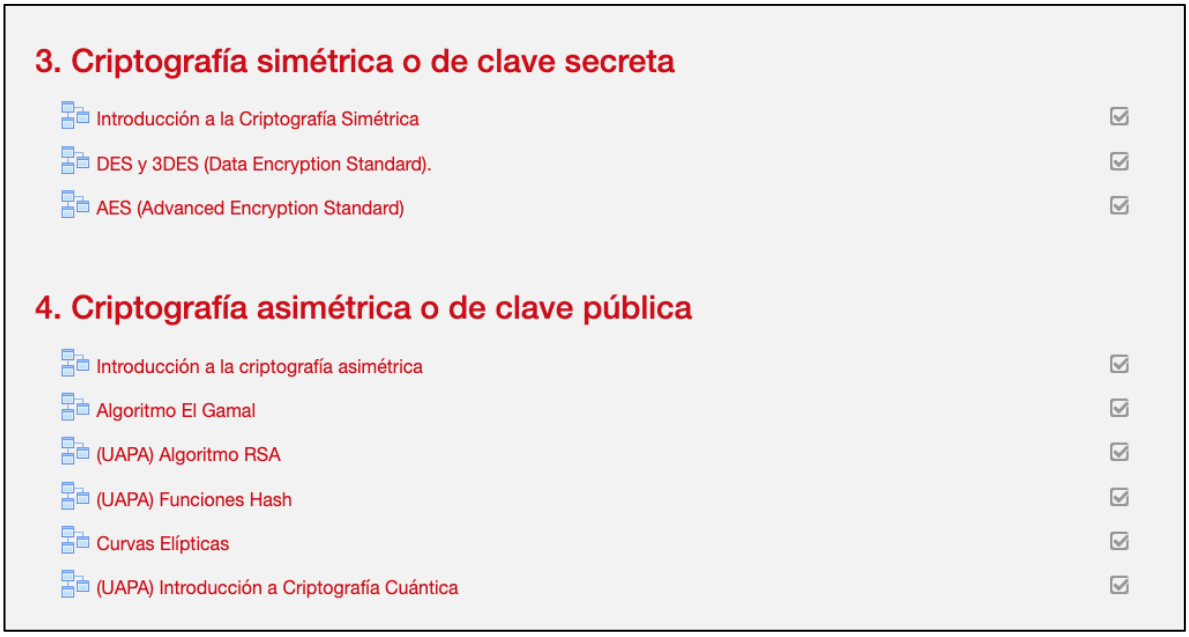


Figura 4.19. Orden del contenido teórico en Moodle.

- **Material en CUAIEED**

De la misma manera, este material se envío a la CUAIEED para su revisión en la plataforma que tiene a su cargo. En este momento se encuentra en proceso de revisión de estilo para posteriormente estar a disposición de los alumnos y profesores de la UNAM. En las Figura 4.20, 4.21, 4.22, 4.23 y 4.24 se muestran algunos avances de este trabajo. Este continuará hasta tener las actividades completas en dicha plataforma.

Figura 4.20. Unidad 1 Antecedentes de la Criptografía en la plataforma CUAED

Figura 4.21. Unidad 2 Técnicas Clásicas de Cifrado en la plataforma CUAED

Figura 4.22. Unidad 3 Criptografía Simétrica o de Clave Secreta en la plataforma CUAED

Figura 4.23. Unidad 4 Criptografía Asimétrica o de clave pública en la plataforma CUAED

Figura 4.24. Unidad 5 Gestión de llaves en la plataforma CUAED

Capítulo 5

5. Conclusiones y trabajo futuro

Durante la realización de este trabajo se generó el material teórico necesario para cubrir los temas propuestos en el temario de la materia de criptografía en el plan de estudios para la carrera de Ingeniería en Computación 2016. Esto incluye actividades teóricas, actividades de programación y evaluaciones con sus correspondientes rúbricas. Todos estos complementan los conocimientos y habilidades adquiridas por los estudiantes durante el curso teórico; además de brindar las herramientas necesarias a los profesores para impartir y evaluar la materia en línea con el material generado.

La necesidad de habilitar nuevas formas de transmitir el conocimiento por medios no tradicionales se evidenció con la llegada de la pandemia, por lo que este material aprovecha esta área de oportunidad. Además, ayudará a los estudiantes que se vean en la necesidad de presentar exámenes extraordinarios o aquellos que tomen curso presencial y necesiten o quieran consultar más material para complementar su aprendizaje o reforzar lo adquirido en su curso presencial.

Para elaborar el material se tomó como base el plan de estudios para la carrera de Ingeniería en Computación 2016, siguiendo la estructura y temas propuestos en él. El diseño del curso se realizo con base en la investigación de técnicas de aprendizaje basada en retos y la construcción del material se realizo por medio de la investigación de los temas en diversas fuentes, en conjunto con las actividades teóricas y prácticas propuestas.

Cómo resultado del esfuerzo en conjunto, se logró elaborar el material teórico, práctico y de apoyo para un curso de criptografía de distribución electrónica y como material de consulta para cursos presenciales. Evidencia de esto son los repositorios y el material presentado en el espacio de *Moodle* que han sido revisados y retroalimentados por la CUAIEED.

Queda como trabajo futuro el dar acceso a los diversos estudiantes, ya sea a través de Moodle o del sitio de CUAIEED, para en un futuro evaluar el impacto que estos materiales tendrán en los estudiantes y profesores que decidan hacer uso de él. Además de funcionar como cimiento para la implementación de una materia totalmente en línea formal por parte de la Facultad de Ingeniería.

Bibliografía

Monterrey, E. I. (Ed.). (2016). Introducción: El Aprendizaje Basado en Retos desde la perspectiva del Aprendizaje Vivencial. *Edu Trends: Aprendizaje Basado en Retos*, 6-13.

Edu Trends: Educación Basada en Competencias. (2015). Editorial Instituto Tecnológico y de Estudios Superiores de Monterrey.

Coordinación de Universidad Abierta, I. E. (8 de octubre de 2021). Obtenido de CUAIEED: https://cuaieed.unam.mx/index.php

Universidad Nacional Autónoma de México. (8 de octubre de 2021). Obtenido de Sistema Universidad Abierta y Educación a Distancia : https://www.unamenlinea.unam.mx/recurso/suayed-unam-abierta-y-a-distancia

Facultad de Ineniería UNAM. (9 de octubre de 2021). *Mapa curricular ingeniería en computación 2016*. Obtenido de Facultad de Ingniería: https://www.ingenieria.unam.mx/programas_academicos/licenciatura/computacion_plan2016.php

Sáenz, R. (2021). *Plataforma educativa en línea para la asignatura de Criptografía.* UNAM.

Global, G. (2021). *Educación virtual: ¿Qué es la educación virtual?* Obtenido de GCF Global: https://edu.gcfglobal.org/es/educacion-virtual/que-es-la-educacion-virtual/1/

Information security and cryptography. (1996). En A. J. Menezes, P. C. Van Oorschot, & S. A. Vanstone, *Handbook of Applied Cryptography* (pág. 4).

Aldeco, R., Gallegos, G., & Rodríguez, L. M. (2020). *Introducción a la Ciberseguridad y sus aplicaciones en México.* Academia Mexicana de Computación, A. C.

Barrón, H. (Marzo de 2024). Obtenido de La educación en línea en México: http://www.uib.es/depart/ gte/edutec-e/revelec18/barron_18.pdf 17/09/13

Ordoñez, H., & Lopez, H. (2013). *"La educación en línea.*

Ibáñez, F. (20 de Noviembre de 2020). *Observatorio Instituto para el futuro de la educación*. Obtenido de Educación en línea, Virtual, a Distancia y Remota de Emergencia, ¿cuáles son sus características y diferencias?: https://observatorio.tec.mx/edu-news/diferencias-educacion-online-virtual-a-distancia-remota

6 cursos online GRATUITOS DE criptografía. (2019). Obtenido de WeLiveSecurity: https://www.welivesecurity.com/la-es/2019/03/15/cursos-online-gratuitos-criptografia/

Cursos de formación para criptografía: Aprende criptografía en línea hoy mismo. (s.f.). Obtenido de Udemy: https://www.udemy.com/es/topic/cryptography/?p=2

About us. (s.f.). Obtenido de edX: https://www.edx.org/about-us

Criptografía. (s.f.). Obtenido de Coursera: https://es.coursera.org/lecture/seguridad-informatica/criptografia-rIYxA

Universidad Autónoma de Barcelona. (s.f.). Obtenido de ¿Qué ES Un curso MOOC? ¿Qué es un curso MOOC?: https://www.uab.cat/web/estudiar/mooc/-que-es-un-curso-mooc-1345668281247.html

Ángel, J. (s.f.). *Historia de la criptografía, en México.* Recuperado el abril de 2020, de https://www.researchgate.net/profile/Jose_Angel-Angel/publication/339199155_Historia_de_la_criptografia_en_Mexico/links/5e43683892851c7f7f30bd59/Historia-de-la-criptografia-en-Mexico.pdf

Ángel, Á., J., J., & G., M. L. (10 de marzo de 2018). *BREVE DESCRIPCIÓN DE LA CRIPTOGRAFÍA EN LA REVOLUCIÓN MEXICANA.* Recuperado el 2020 de abril, de http://ru.tic.unam.mx/bitstream/handle/123456789/1362/art18_2008.pdf?sequence=1&isAllowed=y

Fernández, S. (abril de 2004). *La Criptografía Clásica.* Recuperado el 2020 de abril, de http://www.hezkuntza.ejgv.euskadi.eus/r43-573/es/contenidos/informacion/dia6_sigma/es_sigma/adjuntos/sigma_24/9_Criptografia_clasica.pdf

Mifsud, E. (marzo de 2012). *MONOGRÁFICO: Introducción a la seguridad informática.* Recuperado el 2020 de abril, de http://recursostic.educacion.es/observatorio/web/fr/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=5

Sidhpurwala, H. (agosto de 2013). *A Brief History of Cryptography.* Obtenido de Red Hat: Customer Portal: https://access.redhat.com/blogs/766093/posts/1976023

Skala., V., Hrádek, J., & Kuchař, M. (2010). *New Hash Function Construction for Textual and Geometric Data Retrieval.* Obtenido de NAUM Confu: https://dspace5.zcu.cz/bitstream/11025/11784/1/Skala_2010_Corfu-NAUN-Hash.pdf

Aung, T. M., Naing, H. H., & Hla, N. N. (2019). A Complex Transformation of Monoalphabetic Cipher to Polyalphabetic Cipher: (Vigenère-Affine Cipher). *International Journal of Machine Learning and Computing*(doi: 10.18178/ijmlc.2019.9.3.801), 296-303. Obtenido de International Journal of Machine Learning and Computing.

Alba, M. E. (2018). *Criptografía y Criptoanálisis. Desde los cifrados clásicos hasta la actualidad.* Recuperado el abril de 2020, de http://tesismatematica.ucoz.es/_ld/0/30_Tesis-Maximilia.pdf

L., T. J. (s.f.). *Criptografía Clásica.* Recuperado el abril de 2020, de https://legacy.gitbook.com/book/joseluistabaracarbajo/criptografia-clasica/details

Ramió-Aguirre, J. (s.f.). *Introducción a la seguridad informática y criptografía clásica.* Recuperado el mayo de 2020, de http://www.criptored.upm.es/crypt4you/temas/criptografiaclasica/leccion7.html

Barría Huidobro, C. D. (2018). *Aplicaciones del álgebra matricial en los cifrados por transposición.* Recuperado el mayo de 2020, de https://www.researchgate.net/profile/Alvaro_Toledo_San_Martin/publication/340570294_Aplicaciones_del_algebra_matricial_en_los_cifrados_por_transposicion/links/5e9115ba4585150839d22e6e/Aplicaciones-del-algebra-matricial-en-los-cifrados-por-transposicion.pd

Armando, F. F., & Omar, R. J. (octubre de 2011). *U.N.A.M Criptografía.* Recuperado el octubre de 2020, de https://unamcriptografia.wordpress.com/

Lucena-López, M. J. (2001). *Criptografía y Seguridad en Computadores.* España.

Menezes, A., Oorshot, P., & Vanstone, S. (2001). En *Handbook of Applied Cryptography* (págs. 223-254, 332).

Matsui, M. (1993). *Linear Cryptanalysis Method for DES Cipher. Advances in Cryptology.* .

Biham, E., & Biryukov, A. (1997). An Improvement of Davies' Attack on DES. *Journal of Cryptology*, 195-205.

Computerphile. (2019). *AES Explained (Advanced Encryption Standard) - Computerphile*. (M. Dr. Pound, Productor) Obtenido de https://www.youtube.com/watch?v=O4xNJsjtN6E

Diffie, W., & Hellman, M. (1976). Multiuser Cryptographic Techniques. *National Computer Conference*, 7-10.

T., E. (1985). El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *In Proceedings of CRYPTO 84 on Advances in cryptology*, 10-18.

Santamaría, J., & & Sadornil, D. (2013). *El logaritmo discreto y sus aplicaciones en Criptografía.* Universidad de Cantabria.

Boer, B. d. (1988). Diffie-Hellman is as strong as discrete log for certain primers. *Advance in cryptography- CRYPTO '88*, 13-15, 17-18.

Tsiounis, Y., & Yung, M. (1998). On the security of ElGamal based encryption, Public Key Cryptography. 117-134.

Digital Signature Algorithm. (octubre de 2020). Obtenido de https://en.wikipedia.org/w/index.php?title=Digital_Signature_Algorithm&oldid=981973635

Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 120-126.

Wang, X., & Yu, H. (mayo de 2005). *How to Break MD5 and Other Hash Function.* Obtenido de Shandong University: https://www.researchgate.net/publication/225230142_How_to_Break_MD5_and_Other_Hash_Functions

Dams, J. (2012). *An introduction to elliptic curve cryptography.* Recuperado el septimbre de 2020, de https://www.embedded.com/an-introduction-to-elliptic-curve-cryptography/

Barker, E., Chen, L., Roginsky, A., Vassilev, A., & R., D. (2018). *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography.* Obtenido de https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final

Katz, J., & Lindell, Y. (2014). *Introduction to Modern Cryptography.* (C. &. Hall/CRC., Ed.)

José, L. L. (2001). *Criptografía y seguridad en computadores.*

B., B. E., K., B. D., & E., S. M. (2015). A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS). *NIST Special Publication*, 800-1052.

Barker, E. (2020). Recommendation for Key Management: Part 1 – General. *NIST Special Publication*.

Educación a distancia. Modelo generador de mitos. (2011). Obtenido de http://www.rieoei.org/deloslectores/482Almenara.pdf 15/09/13

J., Y. (2015). Key Distribution for Symmetric Key Cryptography: A Review. *International Journal of Innovative Research in Computer and Communication Engineering*.

Khan, R., & Challa, R. (2017). A review on key distribution protocols to achieve secure secret key distribution and mutual authentication. .

Rescorla, E. (2018). *The Transport Layer Security (TLS) Protocol Version 1.3.* Recuperado el noviembre de 2020, de https://tools.ietf.org/html/rfc8446

Diffie, W., & Hellman, M. E. (6 de boviembre de 1976). *New Directions in Cryptography.* Obtenido de https://ee.stanford.edu/~hellman/publications/24.pdf

WPA3 SpecificationVersion 3.0. (s.f.). Obtenido de WI-FI ALLIANCE PROPRIETARY: https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Specification_v3.0.pdf

IEEE 802.11 WIRELESS LOCAL AREA NETWORKS. (s.f.). Obtenido de The Working Group for WLAN Standards: https://www.ieee802.org/11/

IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amen. (2004). Obtenido de https://standards.ieee.org/standard/802_11i-2004.html

Wolford, B. (2020). *What is PGP encryption and How does it work?* Recuperado el 2021, de https://protonmail.com/blog/what-is-pgp-encryption/

OpenPGP. . (29 de octubre de 2020). Obtenido de https://www.openpgp.org/about/standard/

J., C., L., D., H., F., D., S., & R., T. (2007). *RFC 4880. Openpgp message format .* Obtenido de https://tools.ietf.org/html/rfc4880

C., D., & T., C. (2015). *RFC 7466. An Optimization for the Mobile Ad Hoc Network (MANET), Neighborhood Discovery Protocol (NHDP).* Obtenido de https://tools.ietf.org/html/rfc7466

Raeburn, K. (2005). *RFC 3961. Encryption and Checksum Specifications for Kerberos 5.* Obtenido de https://curl.se/rfc/rfc3961.txt

Vanhoef, M., & Ronen, E. (2019). *Dragonblood: Analyzing the Dragonfly handshake of WPA3 AND EAP-PWD.* Obtenido de https://eprint.iacr.org/2019/383

L., F., & R., C. (s.f.). *Sensus: A Security-Conscious Electronic Polling System for the Internet.* Recuperado el octubre de 2020, de http://lorrie.cranor.org/pubs/hicss/hicss.html

Lin, M. H., & C., C. (2013). Security enhancement for anonymous secure e-voting over a network. *Comput. Stand. Interfaces* , 131-139.

S., H., H., W., & T., H. (2005). On the security enhancement for anonymous secure e-voting over computer network. *Comput. Stand. Interfaces* , 163-168.

Adams, C., Cain, P., D., P., & Zuccherato, R. (2001). Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). *IETF*.

Takura, A., Ono, S., & Naito, S. (1999). A secure and trusted time stamping authority. *Internet Workshop*, 88-93.

Chaum, D., Fiat, A., & Naor, M. (1990). Untraceable electronic cash. In Proceedings on Advances in cryptology . *Advances in cryptology* , 319-327.

R., B. (s.f.). *Cryptography: Authentication, Blind Signatures, and Digital Cash*. Obtenido de http://wwwf.imperial.ac.uk/~rbellovi/writings/chaum.pdf

Bitcoin Wiki . (s.f.). Obtenido de https://en.bitcoin.it/wiki/Main_Page

Nakamoto, S. (s.f.). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Obtenido de https://bitcoin.org/bitcoin.pdf

Aublin, P. L., Guerraoui, R., Knezevic, N., Quéma, V., & Vukolic, M. (2015). The Next 700 BFT Protocols. *ACM TOCS*.

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. *IEEE S&P*.

Cachin, C., Kursawe, K., Petzold, F., & Shoup, V. (2001). Secure and Efficient Asynchronous Broadcast Protocols. *CRYPTO*.

Cachin, C., Guerraoui, R., & Rodrigues, L. (2011). *Introduction to Reliable and Secure Distributed Programming.* Springer.

Cachin, C., Schubert, S., & Vukolic, M. (2016). *Non-determinism in Byzantine Fault-Tolerant Replication.* OPODIS.

Castro, M., & Liskov, B. (2002). *Practical Byzantine fault tolerance and proactive recovery.* ACM TOCS.

Decker, C., Seidel, J., & Wattenhofer, R. (20016). *Bitcoin meets strong consistency.* ICDCN.

Eyal, I., Gencer, A., Sirer, E., & Van Renesse, R. (2026). *Bitcoin-NG: A Scalable Blockchain Protocol.* NSDI.

Requisitos que deben observarse para la conservación de mensajes de datos y digitalizacion de documentos. (2017). Obtenido de http://dof.gob.mx/nota_detalle.php?codigo=5478024&fecha=30%2F03%2F2017

Anexos

A. Ligas de acceso a los materiales

Tema	Nombre	Liga Google Drive	Liga Moodle
1	***Panorama general***		
1.2	Historia de la criptografía	Documento	Moodle
1.3	Servicios y mecanismos de seguridad	Documento	Moodle
	Actividades Prácticas	-	-
	Actividades	-	-
	Evaluaciones	Documento	-
2	***Técnicas clásicas de cifrado***		
2.1	Introducción y clasificación de los sistemas de cifrado	Documento	Moodle
2.2	Algoritmos de sustitución	Documento	Moodle
2.3	Algoritmos de transposición	Documento	Moodle
	Actividades Prácticas	-	-
	Actividades	-	-
	Evaluaciones	Documento	-
3	***Criptografía simétrica o de clave secreta***		
3.1	Introducción a la criptografía simétrica	Documento	Moodle
3.2	DES y 3DES (Data Encryption Standard)	Documento	Moodle
3.3	AES (Advanced Encryption Standard)	Documento	Moodle
	Actividades Prácticas	Carpeta	-
	Actividades	Carpeta	-
	Evaluaciones	Documento	-
Examen 1		**Documento**	**-**
4	***Criptografía asimétrica o de clave pública***		
4.1	Introducción a la criptografía asimétrica	Documento	Moodle
4.2	Algoritmo El Gamal	Documento	Moodle
4.3	Algoritmo RSA	Documento	Moodle
4.4	Funciones Hash	Documento	Moodle
4.5	Curvas Elípticas	Documento	Moodle
4.6	Introducción a Criptografía Cuántica	Documento	Moodle
	Actividades Prácticas	Carpeta	-

	Actividades	Carpeta	-
	Evaluaciones	Documento	-
5	**Gestión de claves**		
5.1	Políticas y gestión de claves	Documento	Moodle
5.2	Tipos de claves	Documento	Moodle
5.3	Generadores y distribución de claves	Documento	Moodle
5.4	Protocolos de Distribución de Llaves	Documento	Moodle
	Actividades Prácticas	-	-
	Actividades	Carpeta	-
	Evaluaciones	Documento	-
6	***Aplicaciones criptográficas***		
6.1	Firmas Digitales	Documento	Moodle
6.2	Certificados Digitales	Documento	Moodle
6.3	Aplicaciones Descentralizadas	Documento	Moodle
	Actividades Prácticas	-	-
	Actividades	Carpeta	-
	Evaluaciones	Documento	-
Examen 2		**Documento**	**-**