Propuestas de trabajos de diplomas del Instituto de Criptografía

* Tecnología Blockchain

1. **Tutor**: Magdiel Vicet Morejón

**Tema:** Diseño e implementación de una arquitectura básica para el desarrollo de una blockchain genérica.

**Problema a resolver:** Desarrollar una blockchain propia, que sea lo más genérica posible para que pueda ser utilizada en la solución de la mayor cantidad de problemas posibles.

**Objetivo general:** Desarrollar una arquitectura básica de una blockchain genérica que aglutine lo mejor de las blockchains existentes en la actualidad.

**Objetivos específicos:** Definir:

* Los participantes, activos y transacciones.
* Tipos de nodos de la red, así como las características de cada uno.
* Algoritmos de consenso.
* Estructura de los bloques de la cadena de bloques.
* Protocolo de comunicación.
* Lenguaje de programación a utilizar para implementar los contratos inteligentes.
* Estructura de una Billetera.
* Elementos criptográficos necesarios para proteger la información que se procese, intercambie, y almacene en la blockchain.

1. **Tutor:** Alexi Massó Muñoz

**Tema:** Implementación de aplicación de acceso (wallet) para el sistema descentralizado para la transferencia de propiedad de medicamentos en Cuba.  
**Problema a resolver:** El Instituto de Criptografía desarrolla el sistema descentralizado para la transferencia de la propiedad de medicamentos en Cuba para BioCubaFarma. Este sistema será desplegado sobre la plataforma quórum y hará uso de estándares de tokens fungibles (erc20) para modelar los diferentes medicamentos y las transferencias que pueden ser realizadas. Los usuarios necesitarán una wallet para interactuar con el sistema y al usarse estándar es posible utilizar wallet genéricas para las funciones básicas del sistema. A pesar de lo planeado es imprescindible la creación de una wallet a medida para el sistema.  
**Objetivo general:** Desarrollar una aplicación web y Mobile para la interacción con el sistema descentralizado para la transferencia de propiedad de medicamentos en Cuba.  
**Objetivos específicos:**

* Estudio del API web3.
* Estudio de la plataforma go quórum.
* Análisis y diseño de aplicación web y Mobile.
* Implementación de aplicación web y Mobile.

1. **Tutor:** Jesús A. López Borges

**Tema:** Chaincode para la Supply Chain

**Problema a resolver:** ¿Cómo convertir el proceso de negocio de la Supply Chain en un Chaincode para Hyperledger Fabric?

**Objetivo general:** Diseñar e implementar un Chaincode para la Suply Chain según arquitectura de Hyperledger Fabric

1. **Tutor:** Jesús A. López Borges

**Tema:** Despliegue en Producción de una Red de Hyperledger Fabric

**Problema a resolver:** ¿Cómo sistematizar el despliegue en producción de una red de Hyperledger Fabric?

**Objetivo general:** Diseñar una metodología para el despliegue en producción de un consorcio con Hyperledger Fabric

1. **Tutores:** Miguel Katrib Mora, Camilo Denis González y Daniel Mena Frías

**Tema**: Herramienta para desarrollar contratos inteligentes para HLF desde C#.

**Problema a resolver:** Poder programar contratos en C# que interactúen con una Blockchain en HLF

**Objetivo general:** Integrar la lógica de los contratos inteligentes programados en C# dentro de la arquitectura de una blockchain HLF. Facilitar el entrenamiento docente en la concepción de contratos inteligentes

**Objetivos específicos:** Diseño e implementación del SDK. Desarrollo de un repositorio de contratos reutilizables. Evaluar características de Solidity que se puedan emular o mejorar como bibliotecas C#

1. **Tutor:** Daniel Mena Frías

**Tema**: Módulo fabric-network del Fabric-SDK para el lenguaje C#:

**Descripción:** Este módulo proporcionara una API de alto nivel para interactuar con contratos inteligentes usando C# en una red de blockchain de Hyperledger Fabric. Esta primera versión de la API no proporcionará capacidades administrativas, como instalar e iniciar contratos inteligentes, solo permitirá consultar e invocar contratos inteligentes.

**Problema a resolver:** Interactuar con la red blockchain de Hyperledger Fabric usando el lenguaje de programación C#.

**Objetivo general:** Diseñar e implementar un módulo fabric-network para interactuar con la red blockchain de Fabric empleando C#

1. **Tutor**: Camilo Denis González

**Tema:** Módulo fabric-ca-client del Fabric-SDK para el lenguaje C#:

**Descripción:** Este paquete encapsula las API para interactuar con Fabric CA y administrar el ciclo de vida de los certificados de usuario, como el registro, la inscripción, la renovación y la revocación.

**Problema a resolver:** Interactuar con la Autoridad Certificadora de Fabric (Fabric-CA) a través de su REST-API, para administrar el ciclo de vida de los certificados de usuario, como el registro, la inscripción, la renovación y la revocación.

**Objetivo general:** Diseñar e implementar un módulo fabric-ca-client para interactuar con el Fabric-CA empleando C#

1. **Tutores**: Camilo Denis González y Jesús A. López Borges

**Tema:** Configuraciones de red blockchain óptimas basada en el análisis de las configuraciones de bloque para mejorar el rendimiento de Hyperledger Fabric

**Problema a resolver:** Cuando se trata de configuraciones, Hyperledger Fabric (HF) brinda un alto grado de libertad a los operadores de red, existen parámetros para configurar el rendimiento y latencia de las transacciones, estos parámetros se pueden ajustar para escenarios donde se ejecuten una gran cantidad de transacciones por segundos (TPS) o donde ocurra todo lo contrario, y es en dependencia de la configuración de estos parámetros que se puede mejorar el rendimiento de redes blockchain usando HF.

Por lo que el problema consiste en definir uno o varias configuraciones de bloques para HF donde se obtenga buen rendimiento de la red y que estas configuraciones estén en dependencia del escenario de negocio a implementar.

**Objetivo general:** Determinar parámetros de configuración de bloques en varios escenarios para redes blockchain de HF

**Objetivos específicos:**

* Configuración y despliegue de redes de HF variando configuraciones de bloques
* Medición de rendimiento de las redes desplegadas
* Obtención y análisis de los reportes de indicadores de rendimientos
* Presentación de parámetros de configuración ideal para varios escenarios basados en los resultados experimentales.

1. **Tutores:** Camilo Denis González, Miguel Katrib Mora y Alexi Massó Muñoz

**Tema:** Implementación de la Interfaz de Usuario (IU) de una plataforma de credenciales digitales usando Blockchain

**Problema a resolver:** Las credenciales digitales son certificados digitales emitidos por una institución: diplomas, habilidades, expedientes académicos, certificaciones de grado, etc. La blockchain es una base de datos descentralizada y a prueba de falsificaciones que hace posible proteger y almacenar estos documentos. Los estudiantes tienen así un suministro de por vida de credenciales en línea con valor probatorio.

El problema a resolver consiste en diseñar e implementar una Interfaz de usuario de una plataforma de credenciales digitales que de acceso a un certificado a prueba de manipulaciones y directamente verificable.  
Donde cualquiera pueda utilizar libremente y verificar el certificado con un solo clic, sin ninguna necesidad técnica particular: su autenticidad está garantizada por naturaleza.

**Objetivo general:** Implementar una Interfaz de Usuario (IU) de una plataforma de credenciales digitales

1. **Tutor**: Yaidir Mustelier Ruiz

**Tema:** Sistema de votación representativa sobre Quórum

**Problema a resolver:** Llamaremos sistema de votación representativa, aquel que permite a los votantes ceder su derecho al voto a otro votante para asumir como suya la decisión de aquel. Este tipo de votaciones es frecuente durante la elección de juntas directivas de empresas, o toma de decisiones por un grupo de personas.

La relación entre votantes y representantes se modela por un grafo orientado, que pueden presentar ciclos que impidan el feliz término del proceso de votación.

La tecnología *Blockchain* facilita el desarrollo de sistemas de votaciones pues posee mecanismos para evitar el fraude, garantizar la confidencialidad e integridad de los datos; sin embargo**, no se cuenta con un algoritmo apropiado para llevar a cabo votaciones representativas**.

**Objetivo general:** Diseño de algoritmos para el Desarrollo de sistemas de votaciones representativas sobre Quórum.

1. **Tutor**: Yaidir Mustelier Ruiz

# **Tema:** Sistema de subasta a ciegas sobre Quórum

**Problema a resolver:** Los métodos de subasta de valores son muy populares en los mercados financieros. Estas subastas pueden realizarse a la vista, donde cada uno de los participantes conoce las ofertas que hacen los pujadores. Cuando se realiza a ciegas los participantes conocen quien está ganando la subasta, pero no con que oferta.

En el Instituto de Criptografía se desarrolla una plataforma para el Mercado de deuda pública en Cuba, basada en Quórum. Esto implica el desarrollo de contratos inteligentes para la subasta de bonos y títulos de valores. La implementación de subastas a ciegas sobre blockchain presupone una dificultad pues toda información que se almacena es pública y verificable por cualquiera que esté conectado a la red de nodos. La solución a esto podría ser el cifrado de las ofertas que realizan los pujadores. Por tanto, el **problema** consiste en la selección de un esquema de cifrado adecuado para el desarrollo de un sistema de subasta a ciegas sobre Quorum.

**Objetivo general:** Diseño e implementación de un esquema de cifrados que permita el Desarrollo de subastas a ciegas sobre Quorum.

1. **Tutor:** Miguel Katrib Mora + (Camilo y/o Dani)

**Tema**: Herramienta para desarrollar contratos inteligentes para HLF desde Python.

**Problema a resolver:** Poder programar contratos en Python que interactúen con una Blockchain en HLF

**Objetivo general:** Integrar la lógica de los contratos inteligentes programados en Python dentro de la arquitectura de una blockchain HLF. Facilitar el entrenamiento docente en la concepción de contratos inteligentes

**Objetivos específicos:** Diseño e implementación del SDK. Desarrollo de un repositorio de contratos reutilizables. Evaluar características de Solidity que se puedan emular o mejorar como bibliotecas Python

* Método de multiplicación de números enteros grandes

1. Tutor: Magdiel Vicet Morejón

Tema: Método de representación para la multiplicación de números enteros grandes utilizando el algoritmo de Strassen.

Problema a resolver: Representar la multiplicación de dos operandos en una matriz, de manera tal que los coeficientes estén organizados por niveles, posibilitando el uso del algoritmo de Strassen eficientemente

Objetivo general: Obtener un método de representación matricial para la multiplicación que permita utilizar el algoritmo de Strassen y obtener el resultado final a través un algoritmo computacional haciendo uso del overflow.

Objetivos específicos:

* Representar la multiplicación de dos operandos en una matriz donde los coeficientes estén organizados por niveles.
* Aplicar el algoritmo de multiplicación de matrices de Strassen para obtener el resultado de la multiplicación.
* Al resultado de la multiplicación que está almacenado en una matriz aplicarle el algoritmo computacional para obtener el resultado final.
* Calcular el tiempo de procesamiento en cada caso.
* Determinar el consumo de memoria del algoritmo en general.
* Comparar los resultados obtenidos con los obtenidos en las librerías GNU o gmp, MIRACL
* Criptografía Simétrica y Aleatoriedad

1. Tutor: Evaristo Madarro

Tema: Implementación del criterio de propagación en s-cajas de gran dimensión.

Resumen:El criterio de propagación es una de las propiedades criptográficas que deben cumplir las s-cajas para ser utilizadas en algoritmos de cifrado. No obstante, a medida que la dimensión de las s-cajas aumenta, la evaluación de esta propiedad se convierte en un problema práctico. Esto debido al tamaño del espacio de trabajo y por consiguiente del considerable tiempo de ejecución. Por consiguiente, es necesario plantear la utilización de elementos de selección aleatoria o paralelismo para mejorar el tiempo de ejecución de la evaluación de esta propiedad.

1. Tutor: Evaristo Madarro

Tema: Fuentes de aleatoriedad en Blockchain

Resumen:La aleatoriedad es imprescindible en todo proceso digital en que intervenga de algún modo la criptografía. Algunas tecnologías como blockchain están basadas en la utilización de métodos criptográficos, lo cual implica la necesidad de aleatoriedad. En este trabajo se pretende determinar las fuentes de aleatoriedad en blockchain, así como, su importancia en el proceso de construcción de la cadena de bloques. Además, de describir y analizar experimentalmente los métodos de código abierto que se utilicen como fuente de aleatoriedad en blockchain.

1. Tutor: Evaristo Madarro

Tema: Comparación experimental de métodos (preferentemente frecuenciales) para la detección de aleatoriedad en sucesiones de bits (entropía, chi-cuadrado, frecuency test (NIST), otros que se te ocurran o busque el estudiante)

Resumen:En criptografía medir la aleatoriedad de sucesiones de bits aleatorios es indispensable, es un entorno donde se utilizan frecuentemente números aleatorios. En la actualidad existen variados métodos para la evaluar la aleatoriedad existente entre sucesiones de bits. La ausencia de aleatoria, implica una posible debilidad en este entorno y por consiguiente la posible aplicación de un ataque. Por otro lado, evaluar aleatoriedad en sucesiones cortas de bits no es tirvial y muchos de los métodos existentes fallan. La prueba de aleatoriedad basada en el criterio estricto de avalancha (SAC) necesita de un método de este tipo en su funcionamiento, así contar con el método más efectivo para este entorno resulta de vital importancia.

1. Tutor: Evaristo Madarro

Tema: Comparación experimental de métodos para la detección de correlación entre variables binarias (IM, el método que utilizamos en BIC, Pearson, otros clásicos, y otros que se te ocurran o busque el estudiante)

Resumen:En la actualidad existen variados métodos para la evaluar la correlación existente entre variables numéricas discretas. La existencia de correlación entre variables indica la ausencia de aleatoria, lo cual implica en ámbitos criptográficos una posible debilidad en el entorno donde se encuentre esta variable. En dependencia de los valores numéricos de esta variable, el tamaño de muestra o simplemente el tipo de correlación se hace un problema seleccionar cual método utilizar. La prueba de aleatoriedad basada en el criterio de independencia de bits (BIC) necesita de un método de este tipo en su funcionamiento, así contar con el método más efectivo para este entorno resulta de vital importancia.

1. Tutor: Evaristo Madarro

Tema: Algoritmo para la medir la fortaleza de contraseñas basado en la entropía

Resumen:Hoy en día, casi la totalidad de los sistemas actuales basa su seguridad en el uso de contraseñas alfanuméricas. Es conocido, que muchas de estas contraseñas son débiles debido a las propias decisiones de los usuarios al seleccionarlas. De esta manera, es muy importante contar con una herramienta que permita determinar la fortaleza de las contraseñas que seleccionan lo usuarios. Y sobre todo que esta herramienta permita ser embebida en los sistemas informáticas.

1. Tutor: Evaristo Madarro

Tema: Utilización de la entropía (índice de coincidencia, Tsallis, Renyi, Shannon, min entropía y la guess entropy) en la detección de malware y virus.

Resumen:Frecuentemente son informados, por la comunidad internacional, la aparición de virus y malwares que son distribuidos por dispositivos extraíble, emails o elementos de redes sociales. Existen variadas herramientas para la detección de este tipo de archivos que pueden dañar nuestros dispositivos, pero la mayoría son de costosos o no cumplen con los estándares que se necesitan. Varios resultados apuntan al uso de varias herramientas estadísticas para la detección de virus y malware, así que contar con un estudio y comparación experimental de estas herramientas proporciona un resultado práctico significativo.

1. Tutor: Evaristo Madarro

Tema: Comparación experimental entre la entropía y las propiedades algebraicas de las s-cajas

Resumen:La evaluación de propiedades criptográficas en s-cajas se ha convertido en un requisito indispensable para su utilización en algoritmos de cifrado. Hoy en día, existen diversas propiedades que deben cumplir, muchas algebraicas y otras estadísticas. Teóricamente, se han establecido relaciones entre estas propiedades que permiten la evaluación de una forma u otro de ciertas propiedades. Es muy difundido la implementación de las propiedades algebraicas, donde en muchos casos calcularlas en la práctica puede tomar un tiempo considerable. De esta manera, contar con la aplicación práctica de las propiedades basada específicamente en la teoría de la información (estadística) podría permitir reducir los costos en tiempo de ejecución de la evaluación de estas propiedades.

1. Tutor: Evaristo Madarro

Tema: Implementación del estimador NSB de la entropía

Resumen:La entropía es una de las herramientas más utilizadas en la criptografía para la detección de aleatoriedad dentro de algoritmos de cifrado. En la práctica, es necesario estimar la entropía para que puede ser aplicada a la evaluación de estos algoritmos, debido a su carácter probabilístico. Hoy por hoy, existen muchos estimadores de la entropía, algunos de ellos muy difícil de implementar debido a la teoría en que se basan. Uno de estos lo constituye el estimador NSB, que por ser de uno de los más efectivos resultado de gran importancia contar con una implementación propia que permita utilizarlo en la práctica.

1. Tutor: Evaristo Madarro

Tema: Prueba de aleatoriedad basada en la entropía y el índice de coincidencia.

Resumen:La entropía es una de las herramientas de la teoría de la información que más se utilizan en la criptografía para detectar aleatoriedad. En la actualidad existen muchas pruebas estadísticas para medir aleatoriedad, muchas de estas fallan cuando se trabaja en muestra cortas. Y prácticamente, no existe ninguna prueba basada en la utilización del conocido índice de coincidencia. El índice de coincidencia es una de las herramientas utilizas en el criptoanálisis estadístico de algoritmos de cifrado. Así, en este trabajo se propone una nueva prueba estadística basada en la relación entre la entropía y el índice de coincidencia para la evaluación de aleatoriedad en sucesiones de bits.

* Secreto compartido

1. Tutor: José Rodríguez Tito

Estudiante: Gretel Hernández Garbey (C-4)

Tema: Secreto compartido

Objetivo General:Obtener un software que resuelva el uso de los Polinomios en el Cuerpo donde **p** sea primo, para el uso de protocolos criptográficos del tipo esquemas de compartición-reparto de secretos (contraseñas, claves, ficheros, etc.).

Objetivos específicos:

1. Investigar los Protocolos de Secreto Compartido y su fundamentación matemática.
2. Establecer los modelos a usar para un colectivo de N entidades, con vistas a que la recuperación de dicho secreto implique la presencia de K (K<N) entidades y que con sólo (K-1) no se pueda recuperar, ni si quiera poder inferir algo de información. Definir los polinomios a usar para cada caso, en el proceso directo.
3. Utilizando la interpolación polinómica de Lagrange para un número de puntos específicos, modelar la determinación del polinomio original.
4. Implementar el Software.