Experiencias de laboratorio híbridas (HyLab): Algoritmo ElGamal

Carmen **Caiseda**
Codirectora HyLab - UIPR-Bayamón
Puerto Rico
ccaiseda@bayamon.inter.edu
Alvaro **Lecompte**
Director HyLab – UIPR San Germán
Puerto Rico
alecompte@intersg.edu
Eddie **Arrieta-Arrieta**
Universidad Interamericana de Puerto Rico (UIPR)-Bayamón
Puerto Rico
earrieta@bayamon.inter.edu
Omayra **Rivera-Castro**
Coordinadora de Estudiantes HyLab-UIPR-Bayamón
Puerto Rico
oriverac@interbayamon.edu
Carlos **Martínez-Bonilla**
Coordinador de Currículo HyLab- UIPR- San Germán
Puerto Rico
cmartinez@intersg.edu

Resumen

El proyecto Experiencias de Laboratorio Híbridas (HyLab) es una "comunidad de práctica" que busca desarrollar un currículo híbrido innovador utilizando proyectos relevantes para educar estudiantes de nivel universitario. Las experiencias HyLab utilizan las herramientas virtuales y presenciales identificadas como mejores prácticas para cada equipo de trabajo. Estas experiencias son desarrolladas con el insumo de los estudiantes como diseñadores junto con la facultad proponiendo como grupo una mejor forma de enseñar y aprender.

Como ejemplo, usando aprendizaje basado en proyectos, presentamos la actividad del Algoritmo ElGamal, el equipo de estudiantes y profesores desarrollaron el proyecto por medio de aprendizaje híbrido, formato semiautomatizado y programación alfabetizada que provee oportunidades de aprender sobre estructuras algebraicas, algoritmos y su implementación en lenguajes de programación (MATLAB, Python, etc.).

Los resultados mostraron aumento en la identidad científica, pertenencia y autoeficacia de los estudiantes participantes.

Palabras clave: Aprendizaje basado en proyectos; Criptografía; Educación híbrida; Lenguajes de programación

Introducción

El proyecto de Experiencias de Laboratorio Híbridas (HyLab) de la Universidad Interamericana de Puerto Rico (UIPR) es una "comunidad de práctica" como lo define Lave & Wagner (1991) donde los miembros aprenden unos de otros para crecimiento personal y profesional. HyLab busca desarrollar currículo híbrido innovador utilizando proyectos/problemas relevantes para educar nuestra nueva población estudiantil de nivel superior. Las experiencias HyLab utilizan las herramientas virtuales y presenciales que mejor funcionan por disciplina basado en conversaciones de la facultad. Este proyecto une mentores expertos, facultad y estudiantes por medio de los Institutos de Verano que tienen como resultados facultad y estudiantes capacitados para desarrollar nuevo currículo y las experiencias de laboratorio que han sido diseñadas como mejores prácticas pedagógicas por disciplina. Lo innovador de este currículo es que estas experiencias híbridas de aprendizaje son desarrolladas con el insumo de los estudiantes como diseñadores, junto con la facultad, en un modelo que el grupo propone como una mejor forma de enseñar y aprender.

HyLab surge de la necesidad de ofrecer alternativas a la educación presencial tradicional, especialmente tras las experiencias vividas durante el cierre de instituciones educativas debido a la pandemia de COVID-19 y el consecuente aumento en la oferta de cursos a distancia o en modalidad híbrida en los años posteriores. Este cambio, que se percibe como permanente, invita a repensar los métodos de enseñanza sin comprometer la calidad educativa.

Las actividades de aprendizaje pueden desarrollarse parcialmente en laboratorios o salones de clase, y parcialmente en entornos virtuales o mediante comunicaciones asincrónicas en línea, fomentando el trabajo colaborativo entre los estudiantes. Se espera que los resultados de estas experiencias sean presentados y discutidos colectivamente como parte integral del proceso de aprendizaje.

En la revisión de Sandrone (2022) se discute la relación entre la auto-eficacia y la identidad científico-matemática. La auto-eficacia tiene un rol prominente en la capacidad sostenible del estudiante de hacer y utilizar las ciencias y Matemáticas. Se considera que la auto-eficacia promueve la identidad científico-matemática. El desarrollo de la auto-eficacia está ligado a una experiencia de dominio en la ejecución de una tarea específica y la interpretación del estudiante

de esta experiencia. El Instituto de Verano provee la oportunidad de tener esta experiencia transformadora.

El diseño lógico de la metodología de trabajo se resume en la Figura 1.

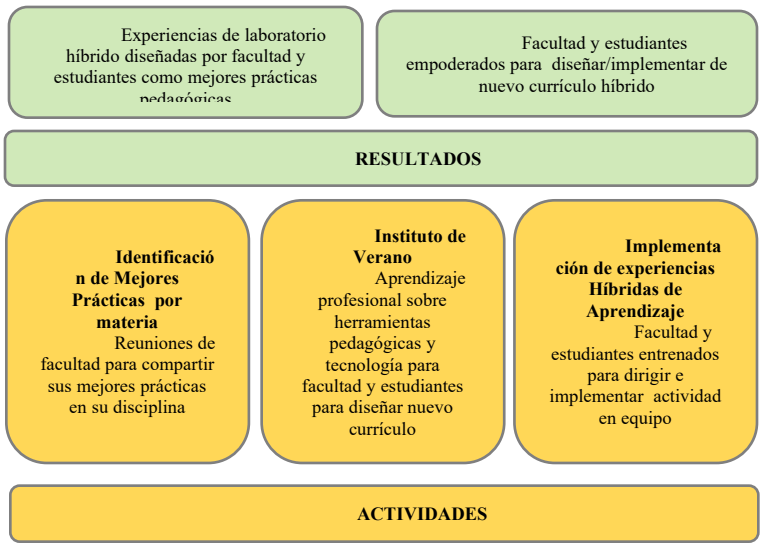

Figura 1. Resumen de las Actividades y resultados del proyecto INTER-HyLab

Este documento está organizado de la siguiente manera. En primer lugar, se presenta la metodología utilizada para el diseño de las actividades. En segundo lugar, a modo de ejemplo, se describe una experiencia basada en un algoritmo criptográfico de llave pública conocido como ElGamal. Esta experiencia puede integrarse en distintos niveles de varios cursos de Matemáticas o ciencias de computación, y demuestra las amplias aplicaciones de estas disciplinas en la vida moderna. En tercer lugar, se discuten los hallazgos obtenidos al emplear esta metodología, otras actividades que ya están disponibles, y los resultados de un estudio impacto de esta metodología realizado con los estudiantes participantes en el proyecto. Finalmente, se analiza la posible contribución de esta metodología y los desarrollos proyectados para el futuro.

Metodología

El Instituto de Verano HyLab 2023 contó con la participación de diez (10) profesores, cuatro (4) coordinadores HyLab y dieciocho (18) estudiantes provenientes de dos recintos geográficamente distantes de la Universidad Interamericana de Puerto Rico: San Germán y Bayamón. La facultad fue seleccionada por su especialidad en Matemáticas e ingeniería, con el objetivo de fomentar una participación significativa y con capacidad de transformar la enseñanza dentro de cada disciplina.

Durante el Instituto, se llevaron a cabo reuniones y conferencias tanto virtuales como presenciales, dirigidas por expertos invitados en herramientas pedagógicas y bienestar, así como por el personal de HyLab. Además, se organizaron sesiones de trabajo colaborativo entre facultad y estudiantes. Esta estructura permitió establecer múltiples niveles de mentoría, desde

expertos hasta estudiantes, fortaleciendo así la comunidad académica. La mentoría es clave para promover la auto-eficacia en los miembros de la comunidad.

Los equipos de trabajo estuvieron compuestos por dos profesores de la misma disciplina y cuatro estudiantes interdisciplinarios de ambos recintos. El Instituto incluyó dos semanas de talleres sincrónicos, dos reuniones presenciales, un mes de trabajo colaborativo (sincrónico y asincrónico), y culminó con un simposio en el que cada equipo presentó el currículo desarrollado, liderado por los propios estudiantes. En las conferencias se discutieron varias herramientas útiles como se indican abajo.

Existe un banco muy rico de herramientas pedagógicas para beneficio de la Educación Matemática a utilizarse al desarrollar actividades tanto en formato virtual como presencial. Parte de las herramientas para desarrollo del currículo que se presentaron en el Instituto de Verano HyLab 2023 se enumera a continuación.

- 4 C's - Pensamiento Crítico, Creatividad, Comunicación y Colaboración
- Raíz causal – los 5 por qué
- Estimación de Fermi
- 6-3-5: 6 personas -3 ideas – 5 minutos
- Específico, Medible, Alcanzable, Recursos y Tiempo (matriz SMART)
- 5-E: conectarse ("engage"), explorar, explicar, elaborar, evaluar
- Aprendizaje basado en problemas y proyectos
- Sustituir, aumentar, modificar, redefinir (SAMR)
- Modelo TPACK: Tecnología, Pedagogía, conocimiento de contenido
- Herramientas tecnológicas:
  - Tecnología para simulaciones en la educación de la física (PhET)
  - Plataforma común en línea para análisis de datos (CODAP)

Presentamos una de las experiencias desarrolladas por uno de los grupos de facultad y estudiantes como resultado de esta metodología de desarrollo de currículo y proyecto grupal.

Actividad sobre el Algoritmo ElGamal

La experiencia desarrollada con el Algoritmo ElGamal es una motivada por la necesidad de la ciberseguridad, de alta importancia en este tiempo. Tanto las transacciones financieras como la comunicación de información sensitiva en las redes deben ser altamente protegidas. El algoritmo ElGamal se caracteriza por su rápida ejecución ("throughput") y su uso en algoritmos de firmas digitales de documentos, conocido como DSA por sus siglas en inglés. Para más información referimos a los escritos de Anusha, R. et. al 2025, Arhin, et. Al. 2024 y Gómez, 2017.

La codificación del algoritmo ElGamal usa funciones inyectivas y es accesible bajo la Firma digital en el programado *GNU Privacy Guard*. El algoritmo tiene su soporte de seguridad en el concepto de funciones de una sola dirección, en este caso la función logaritmo discreto usada en clases residuales de números primos de más de 2048 bits. Dado que el algoritmo tiene tres pasos claves: 1. Creación de llave pública. 2. Cifrado y 3. Descifrado, se pueden diseñar actividades grupales donde se distribuye cada etapa en los integrantes. El primer paso de creación de la llave pública consiste en seleccionar de forma aleatoria un generador g del grupo

cíclico multiplicativo $(\mathbb{Z}_p)$, para un número primo *p,* un número aleatorio secreto $a \in \mathbb{Z}_p$ y el residuo $k = g^a \bmod p$. Esto produce la llave pública (p, g, k). No hay una única solución correcta al momento de crear la llave. La segunda parte conlleva generar un 2-tuplo $[y_1, y_2]$ a partir del mensaje *m*, para cifrar utilizando otro número aleatorio secreto $b \in \mathbb{Z}_p$ con las siguientes fórmulas: $y_1 = g^b \bmod p,\ y_2 = (k^b * m) \bmod p$. Finalmente en el tercer paso desciframos a partir del cifrado $[y_1, y_2]$ con las siguientes funciones:

$D_1 = \left(y_1^{p-a-1}\right) \bmod p,\ M = (D_1 \times y_2) \bmod p$, donde *M* es el mensaje original.

El usuario puede utilizar herramientas como MATLAB o Python entre otros que contienen funciones integradas para calcular números aleatorios y hacer cómputos de residuales $\mathbb{Z}_p$. Esta estrategia les permite comenzar a familiarizar a los estudiantes con estas operaciones. Sin embargo, un estudiante desarrolló herramientas en JAVA para calcular dos partes esenciales del algoritmo ElGamal: los generadores (*g*) del grupo cíclico multiplicativo de enteros módulo *p*-primo y el cómputo del residuo $k = g^a \bmod p$, donde *a* es un número entero aleatorio definido en el algoritmo. Los demás estudiantes utilizaron estas herramientas para cifrar y descifrar un mensaje usando ElGamal en forma semiautomatizada.

El proyecto del algoritmo de ElGamal produjo una experiencia curricular y una presentación dirigida por los estudiantes sobre su trabajo que sorprendió tanto a la facultad como a los propios estudiantes. Junto a sus profesores los cuatro estudiantes lograron trabajar efectivamente como equipo, superando los retos por medio de la comunicación, y aprendiendo sobre temas matemáticos previamente desconocidos, incentivados por el uso de la tecnología en el cifrado y descifrado de un mensaje. Los estudiantes son de programas de ingeniería y ciencia de cómputos con conocimiento matemático de nivel del curso de precálculo. No estaban familiarizados con Álgebra Lineal ni las operaciones en módulo *p.*

Principales Hallazgos

La facultad de Matemáticas participante de estos talleres identificó las mejores prácticas para el desarrollo de un currículo híbrido basado en proyectos. La práctica de mayor prioridad identificada es: **"Implementar tareas que *promuevan razonamiento y solución de problemas* e interesar a los estudiantes *en discusión de problemas que permitan variedad de puntos iniciales y estrategias.*"** La facultad contribuyó los siguientes comentarios referentes a la importancia del razonamiento, solución de problemas y comunicación por medio de la discusión de los problemas.

- Uso de lenguaje apropiado que promueve la hermenéutica matemática, pues conecta el proceso cognitivo y semiótico de la interpretación en Matemáticas
- Uso de foros de discusión: Aportación del estudiante sobre cómo explicar de acuerdo con lo que él/ella entendió del tema que se está estudiando
- Incentivar reuniones de grupos de aprendizaje fuera del horario de clases y poner por escrito sus ideas
- Conexión de estudiantes más avanzados con estudiantes nuevos
- Presentaciones orales
- Uso de representaciones múltiples: dibujos, tablas, diagramas

La práctica pedagógica de menor importancia identificada por la facultad participante es: "Apoyar la *lucha productiva:* proveer oportunidades a estudiantes individual y colectivamente para lidiar con ideas y relaciones matemáticas." Este tipo de enseñanza parece ser la menos conocida y/o practicada posiblemente por la incertidumbre del tiempo de clase que tome, y la meta de adelantar el contenido a cubrir en cada reunión. No obstante, la facultad aportó los siguientes comentarios asociados a la *lucha productiva.*

- Hay que recordarles a los estudiantes que *de los errores se aprende*
- *Validar el estrés* de los estudiantes nuevos
- Dar *múltiples oportunidades* para completar las actividades

El proyecto ha desarrollado cinco actividades producto del trabajo de los cinco equipos de facultad y estudiantes. Este material de formato híbrido incluye los siguientes temas:

1. Algoritmo ElGamal: Aplicaciones de Álgebra Lineal en la ciberseguridad
2. Jugando con cuerdas, masas y vectores: Estudio usando simulación y experimentación con cambios de dirección de cuerdas y masas
3. Análisis de datos para el curso de probabilidad – estudios de caso justificados con razonamiento estadístico
4. Logaritmos y pH- uso de una solución de repollo morado para medir y definir pH
5. Función Exponencial – modelos de crecimiento y decrecimiento

El impacto de esta metodología pedagógica fue evaluado mediante una encuesta ofrecida a los estudiantes antes y después del instituto de verano. Debido al tamaño de la muestra, 11 de 18 estudiantes, los resultados no pretenden ofrecer un análisis del valor estadístico de los resultados, sino una evaluación del Instituto. Los resultados de ambas encuestas (Pre y Pos) se presentan en la Tabla 1. Estos son alentadores, aunque la muestra no permite análisis inferencial. Observamos cambios positivos en tres constructos: Identidad científico-matemática, auto-eficacia y sentido de pertenencia. Es de destacar el cambio más alto que ocurre en el sentido de pertenencia. Esto está asociado con las mentorías facultad-estudiante, y entre pares que ocurre en la experienca de trabajo en equipo que se promueve como parte de la "comunidad de práctica" del Instituto HyLab.

Tabla 1
Resultados de Pre-Pos prueba para Instituto de Verano 2023

Constructo	**Media-Pre N = 9**	**Media-Pos N = 11**	**Cambio**
Identidad Científica-matemática	4.50	5.25	0.75
Auto-eficacia	8.54	9.15	0.61
Sentido de pertenencia	8.93	9.97	1.04
Bienestar	4.49	4.48	-0.01
Persistencia	4.67	4.65	-0.02

Además, hay una congruencia entre las actividades y las reflexiones que los estudiantes participantes compartieron sobre el impacto del programa. Incluimos comentarios de los estudiantes a la pregunta: ¿qué cosas claves obtuvieron de la experiencia? Citamos:

- "fue un reto, pero aprendí muchísimo"
- "aprendí a adaptarme y vencer ante los retos"
- "podemos hacer más de los que nos parecía posible, aún con pocos recursos"
- "un sentido de amistad y motivación"
- "he desarrollado destrezas de liderazgo, entusiasmo y creatividad"
- "descubrir oportunidades asombrosas para los estudiantes en nuestras disciplinas de estudio."

Contribución

El valor de esta experiencia HyLab se encuentra en la riqueza del lenguaje matemático y sus métodos que han sido obtenidos por los estudiantes al construir sus funciones y programas en lugar de utilizar un programado obtenido y utilizarlo sin consciencia de su contenido, como una "caja negra". Esto es una oportunidad que se puede reproducir hoy más que ayer con el uso de los asistentes de Inteligencia Artificial (IA) para facilitar la programación en diversos lenguajes de interés para el estudiante. Un futuro impacto mayor de este tipo de actividad es el uso de la programación alfabetizada (literate programming) de Knuth (1984) que actualmente se integra en sistemas como R-markdown, y Jupyter Notebooks que permitir incluir explicaciones tipo libro de texto que redactan los conceptos matemáticos seguidos por pedazos de código. Este formato provee al estudiante la explicación y la herramienta para que explore y modifique aprendiendo destrezas del pensamiento lógico-matemático y tecnológico. De esta manera como educadores de Matemáticas estamos posicionados para aprovechar esta oportunidad provista por los avances tecnológicos y enseñar el lenguaje del desarrollo de las ideas que la misma tecnología utiliza: las Matemáticas.

Agradecimiento

Este proyecto ha sido subvencionado por el programa MSEIP (Programa de mejoramiento de las ciencias e ingeniería para minorías) del Departamento de Educación de E.U, bajo la dirección de la Dra. Bernadette Hence. El equipo de trabajo del proyecto INTER-HyLab agradece la contribución de la evaluadora externa Dra. Gabriele Haynes.

Referencias y bibliografía

Anusha, R., & Saravanan, R. (2025). Revolutionizing signature scheme: the enhanced Edward Elgamal extreme performance accumulate signature approach for IoT and blockchain applications. *Soft Computing*, 1-24.

Arhin, P., & Aggrey, G. Enhancement of Elgamal Cryptosystem (Noviembre 2024); A Review, recuperado el 15 de febrero de 2025, de https://icaiit.org/proceedings/12th_ICAIIT_2/1-9-ICAIIT_2024_12(2).pdf

Bravo, A., & Olga, M. (2018). Selección e implementación de librería Java de algoritmo para E-Voting.

Gómez Olvera, M. D. (2017). Las Matemáticas y las comunicaciones seguras Algoritmo de Elgamal.

Hernandez, F., Algebra Lineal, recuperado el 15 de febrero de 2025, de https://sites.google.com/unal.edu.co/fohernandezr/docencia/materias/%C3%A1lgebra-lineal

Lave, J., and Wenger, E. (1991). Situated Learning: Legitimate Peripheral Participation. New York, NY: Cambridge University Press. doi:10.1017/CBO9780511815355

Knuth, D. E. (1984), Literate Programming, *The Computer Journal*, Vol. 27: 2, (pp.97 111), https://doi.org/10.1093/comjnl/27.2.97.

Sandrone, S. (2022) Science dentity and Its "Identity Crisis": On Science Identity and Strategies to Foster Self-Efficacy and Sense of Belonging in STEM, MINI REVIEW article, Front. Educ., 21 July 2022, Sec. STEM Education. Volume 7 - 2022 | https://doi.org/10.3389/feduc.2022.871869

Tsiounis, Y., & Yung, M. (1998, February). On the security of ElGamal based encryption. In International Workshop on Public Key Cryptography (pp. 117-134). Berlin, Heidelberg: Springer Berlin Heidelberg.