PUCE Virtual

CLASE

1

MÉTODOS NUMÉRICOS

Introducción a los Métodos Numéricos

QS WORLD UNIVERSITY RANKINGS

Educación de calidad

INTRODUCCIÓN DE LA CLASE

GRADO / POSGRADO / TECNOLOGÍAS

Estudia a tu tiempo
son interrupciones

EDUCACIÓN EN LÍNEA DE CALIDAD

En esta clase se introduce de manera integral a los métodos numéricos como herramientas fundamentales para resolver de forma aproximada problemas matemáticos en ingeniería y ciencias, entendiéndolos como procedimientos algorítmicos que permiten obtener soluciones cuando el enfoque analítico no es viable o resulta demasiado complejo, destacando su evolución junto con la computación digital y su importancia en el análisis moderno al transformar problemas continuos en procesos discretos aplicables en computadora, mientras se presentan conceptos clave como aproximación, iteración y convergencia y se exploran aplicaciones en áreas como mecánica, electrónica, economía y biología, además de establecer una comparación clara con los métodos analíticos resaltando tanto su flexibilidad y alcance como sus limitaciones en estabilidad, errores y costo computacional, cerrando con una visión general de los principales tipos de problemas que abordan como ecuaciones no lineales, sistemas lineales, interpolación, integración y ecuaciones diferenciales.

De forma complementaria se estudia el manejo y análisis de errores como parte esencial del cálculo numérico, considerando que toda aproximación implica diferencias entre el valor exacto y el calculado, introduciendo los conceptos de error absoluto y relativo para medir precisión y evaluar resultados, analizando cómo estos errores afectan la confiabilidad especialmente en procesos iterativos y de gran escala, identificando sus principales fuentes como el redondeo por la representación finita de números y el truncamiento al aproximar procesos infinitos, y explicando cómo se propagan a lo largo de los cálculos pudiendo amplificarse si no se controlan, con el objetivo de que el estudiante desarrolle criterio para interpretar resultados y gestionar la precisión en aplicaciones reales.

Resultado o resultados de aprendizaje que será abordado con el contenido de la clase.
Analizar problemas matemáticos y computacionales utilizando métodos numéricos adecuados para su solución aproximada.

Introducción a los Métodos Numéricos

Los métodos numéricos son técnicas matemáticas que nos ayudan a encontrar soluciones aproximadas a problemas que no pueden resolverse de manera exacta o que resultan demasiado complejos para resolver directamente. Se utilizan mucho en campos como la ingeniería y las ciencias, donde las ecuaciones que describen fenómenos físicos, estructuras o sistemas dinámicos no siempre tienen soluciones claras o fáciles de calcular.

Por ejemplo, en ingeniería civil, al analizar una estructura, o en ingeniería mecánica, al simular el flujo de un fluido, es necesario recurrir a aproximaciones numéricas para obtener resultados útiles. Aunque algunos problemas se pueden resolver con métodos exactos, muchas veces las ecuaciones son demasiado complejas, y aquí es donde los métodos numéricos se vuelven esenciales. Estos métodos no ofrecen soluciones exactas, pero sí resultados suficientemente precisos para la mayoría de los fines prácticos, y permiten abordar problemas grandes o complicados que de otra manera serían imposibles de resolver.

Una de las grandes ventajas de los métodos numéricos es su flexibilidad: se pueden aplicar a muchísimos tipos de problemas, incluso cuando no existen soluciones analíticas. Sin embargo, su precisión depende del método que se utilice, del tamaño de los pasos de cálculo y de la estabilidad del algoritmo. Esto quiere decir que, aunque sean herramientas poderosas, siempre hay un margen de error, y es importante elegir bien el método para evitar resultados incorrectos o inestables. Además, hay que considerar que los problemas muy grandes o complejos pueden requerir mucho tiempo de cálculo y memoria, lo que también limita su uso si no se gestionan adecuadamente.

A pesar de estas limitaciones, los métodos numéricos han transformado la ingeniería y la ciencia, permitiendo simular y analizar situaciones que antes eran inaccesibles. Por eso, se clasifican en distintos tipos: desde métodos para resolver ecuaciones algebraicas, hasta técnicas para ecuaciones diferenciales, optimización o integración numérica. Todos ellos son herramientas clave para enfrentar los desafíos reales en distintas disciplinas científicas y tecnológicas.

Definición de métodos numéricos

Piensa en cómo es tu día a día como profesional de seguridad informática: a veces estás analizando trazas de potencia para extraer una clave AES mediante ataques diferenciales, otras veces estás factorizando un módulo RSA débil con métodos numéricos avanzados, y en otras ocasiones entrenas un modelo que detecta anomalías en el tráfico de red, capaz de procesar millones de paquetes por segundo. Cada día trae un nuevo desafío. La mayoría de estos problemas no tienen soluciones analíticas exactas o si las tienen, son imprácticas por el tamaño de los números involucrados o la complejidad computacional.

Los métodos numéricos te dan el poder de obtener aproximaciones extremadamente precisas y controladas mediante algoritmos repetitivos que corren en computadoras, permitiendo romper sistemas criptográficos, detectar amenazas en tiempo real o simular riesgos de brechas con alta fiabilidad. En esta asignatura de 8 clases exploraremos desde los errores inherentes hasta métodos avanzados de optimización y ecuaciones diferenciales aplicadas a modelado de ataques, pasando por aritmética modular y lattices. Al finalizar, podrás seleccionar, implementar y evaluar métodos numéricos en escenarios reales de ciberseguridad, estimar errores críticos, mitigar vulnerabilidades numéricas y entender cómo un pequeño error de aproximación o precisión puede comprometer un sistema entero.

En el mundo de la computación y la ciberseguridad, los problemas matemáticos que enfrentamos diariamente son enormes y complejos: números de cientos de dígitos en criptografía asimétrica, matrices de alta dimensión en análisis de lattices para post-cuántica, o distribuciones probabilísticas en detección de malware mediante machine learning. Rara vez existe una fórmula cerrada que resuelva estos problemas de manera exacta y eficiente.

En ciberseguridad, los métodos numéricos transforman problemas teóricos en ataques viables o defensas robustas: permiten factorizar claves RSA, correlacionar trazas en side-channel attacks o optimizar hiperparámetros en modelos de detección de intrusiones.

Ejemplo práctico: para romper un cifrado RSA con módulo $N = p * q$ (donde p y q son primos grandes), no hay fórmula directa; usamos métodos numéricos como el de Pollard rho o el Number Field Sieve (NFS), que aproximan factores mediante iteraciones y pruebas probabilísticas. Otro caso: en ataques de timing, aproximamos distribuciones de tiempo de ejecución con métodos estadísticos numéricos para inferir bits de clave.

Figura 1: Diagrama de clasificación general de métodos numéricos aplicados a problemas de computación y ciberseguridad.

Creación propia.

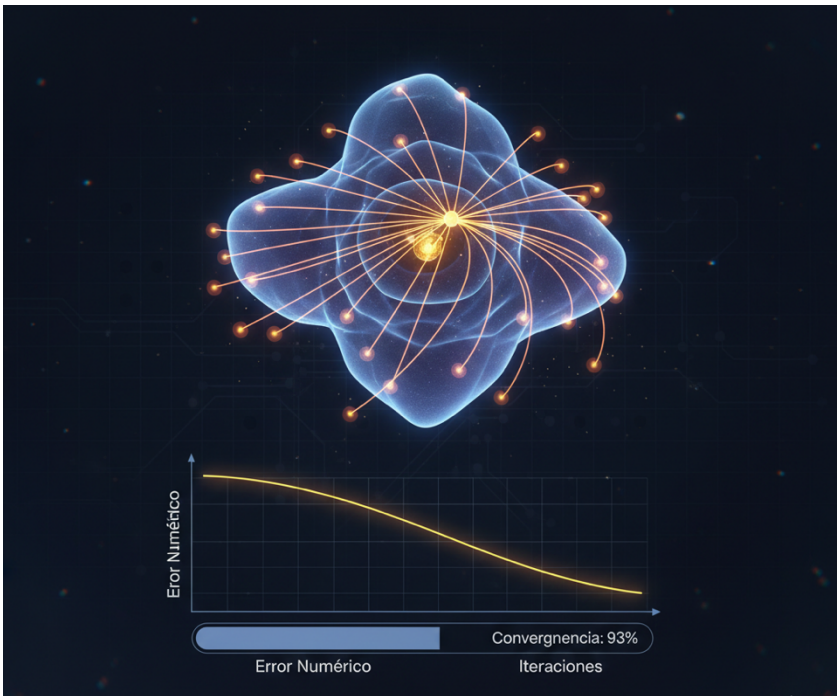

Figura 2: Representación visual de la convergencia numérica en un ataque de aproximación a una clave criptográfica mediante iteraciones.

Creación propia.

Enlace 1: https://www.youtube.com/watch?v=Pc2D7BQj9mA Ver en YouTube: Floating Point Errors in Cryptography – Why Precision Matters Este video analiza casos reales donde errores de punto flotante han creado vulnerabilidades explotables en algoritmos criptográficos.

Desde el punto de vista de la ciberseguridad, la figura puede interpretarse como una abstracción de ciertos ataques teóricos en los que se modela la recuperación de una clave como un problema de optimización numérica, en el cual se define una función objetivo que mide la discrepancia entre la salida criptográfica producida por una clave candidata y la salida esperada, permitiendo que el atacante ajuste sistemáticamente los parámetros hasta minimizar dicha función, siempre que existan vulnerabilidades estructurales que introduzcan correlaciones explotables.

Asimismo, la gráfica pone de manifiesto la importancia de la estabilidad numérica y la tasa de convergencia, ya que un descenso rápido del error indica un método con convergencia de orden superior o con buena elección de condiciones iniciales, mientras que una disminución lenta, oscilatoria o estancada puede revelar la presencia de mínimos locales, mal condicionamiento del problema o resistencia inherente del esquema criptográfico frente a técnicas de aproximación iterativa.

Importancia de los métodos numéricos

La ciberseguridad moderna depende completamente de cálculos numéricos precisos y eficientes. Los algoritmos criptográficos (RSA, ECC, Kyber, AES) se basan en problemas matemáticos duros que solo se resuelven (o atacan) mediante aproximaciones numéricas.

Criptoanálisis: Factorización de enteros grandes (GNFS, ECM), resolución de ecuaciones logarítmicas discretas (Pollard rho, index calculus), ataques a lattices (LLL, BKZ con aproximaciones numéricas).

Side-channel y fault attacks: Correlación numérica (Pearson) en Differential Power Analysis (DPA), regresión lineal para extraer claves de trazas de potencia o timing.

Sin métodos numéricos, herramientas como John the Ripper (para cracking de hashes), Hashcat (optimización GPU), o SageMath/Magma (criptoanálisis) no existirían en su forma actual. Son la base para pasar de la teoría a la práctica en red teaming, blue teaming y desarrollo de criptografía segura.

Enlace 2: https://www.youtube.com/watch?v=tS2LP5voIm4 Ver en YouTube: Numerical Stability in Side-Channel Analysis and Cryptographic Implementations Este recurso explica

cómo la estabilidad numérica afecta directamente la efectividad de ataques DPA y CPA, con ejemplos prácticos.

Figura 3: Infografía sobre aplicaciones de métodos numéricos en áreas clave de ciberseguridad y computación.

Creación propia.

Ventajas y limitaciones frente a métodos analíticos

- **Ventajas en ciberseguridad:**
  - Manejan números arbitrariamente grandes con librerías como GMP, OpenSSL o mpmath.
  - Resuelven problemas no lineales y de alta dimensión típicos en ECC, lattices y ML para seguridad.
  - Permiten ataques prácticos en tiempo finito (e.g., side-channel en minutos vs. años teóricos).

- Facilitan cuantificación de seguridad (bits de entropía, complejidad numérica).
- Integran datos reales (trazas, logs, paquetes) para análisis forense numérico.

- **Limitaciones críticas:**
  - Errores de redondeo pueden crear vulnerabilidades (e.g., ataques de rounding en implementaciones de curva elíptica).
  - Inestabilidad numérica genera falsos positivos/negativos en detección de anomalías.
  - Alto costo computacional en ataques avanzados (NFS requiere supercomputadoras).
  - Aproximaciones pueden subestimar riesgos (e.g., Monte Carlo con pocas iteraciones).

Requieren validación extrema: un resultado numérico "correcto" puede ocultar una puerta trasera.

En ciberseguridad, elegir entre exactitud analítica (limitada) y aproximación numérica (práctica pero riesgosa) define si un sistema resiste o cae ante un atacante real.

Clasificación general de los métodos numéricos

- **Clasificación adaptada:**
  - Raíces de ecuaciones no lineales: Newton-Raphson, secante → recuperación de claves parciales, ataques polinómicos a RSA.
  - Aritmética modular y factorización: Exponenciación rápida, GCD extendido, Pollard rho, ECM, NFS → criptoanálisis de RSA/DH.
  - Sistemas lineales y lattices: Gauss, BKZ, LLL → ataques a NTRU, Kyber, Dilithium.
  - Interpolación y curve fitting: Lagrange, mínimos cuadrados → reconstrucción en side-channel, timing analysis.
  - Optimización: Gradiente descendente, quasi-Newton → entrenamiento ML para detección malware, optimización en ataques.
  - Integración y Monte Carlo: Estimación probabilística de éxito de exploits, simulación side-channel.
  - Métodos estocásticos: Generación pseudoaleatoria segura, pruebas Miller-Rabin.

Figura 4: Diagrama de clasificación de métodos numéricos relevantes para criptografía, criptoanálisis y ciberseguridad computacional.

Creación propia.

Manejo y Análisis de Errores

En la Clase 1 exploramos cómo los métodos numéricos permiten resolver problemas complejos en computación y ciberseguridad cuando las soluciones analíticas no son viables. Sin embargo, todo cálculo numérico introduce errores inevitables debido a la precisión finita de las computadoras. Estos errores pueden ser pequeños en teoría, pero en la práctica de la seguridad informática —donde se manejan claves criptográficas, trazas de potencia o datasets masivos de red— un error minúsculo puede generar vulnerabilidades reales, falsos negativos en detección de amenazas o subestimaciones de riesgos.

En esta clase profundizaremos en el concepto de error numérico, sus tipos principales, cómo se miden y, especialmente, cómo se propagan a través de algoritmos. Al finalizar, podrás

identificar fuentes de error en implementaciones criptográficas, evaluar su impacto en ataques side-channel o sistemas de machine learning para seguridad, y aplicar técnicas para controlarlos en código real.

Concepto de error numérico

El error numérico es la diferencia entre el valor matemático exacto (ideal) y el valor obtenido en una computadora debido a limitaciones inherentes como la representación finita de números y la aproximación de operaciones infinitas.

Las computadoras usan el estándar IEEE 754 para aritmética de punto flotante: doble precisión ofrece alrededor de 15-16 dígitos decimales confiables, pero números como 0.1 no se representan exactamente en binario, generando errores desde el inicio. En ciberseguridad, estos errores afectan directamente la fiabilidad de cálculos en criptografía modular, análisis de canales laterales o entrenamiento de modelos de detección.

Los errores se clasifican en dos grandes categorías: inherentes al problema (condicionamiento) y introducidos por el algoritmo (estabilidad).

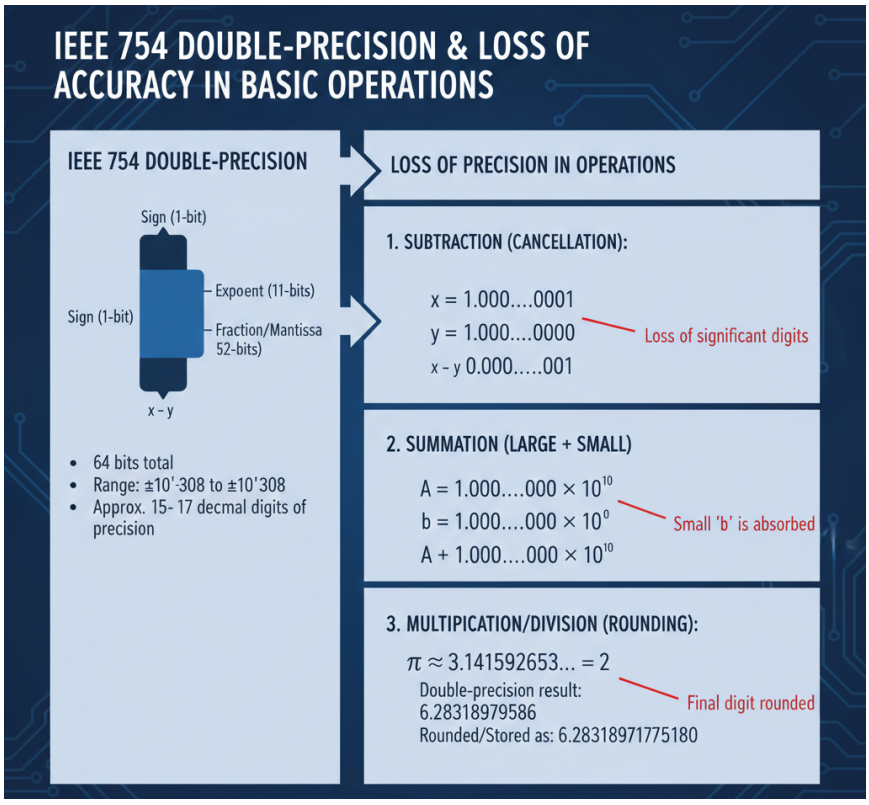

Figura 5: Representación IEEE 754 en doble precisión y pérdida de precisión en operaciones básicas.

Creación propia.

El concepto de pérdida de precisión en este contexto está relacionado con la imposibilidad de representar de manera exacta ciertos números decimales en su forma binaria correspondiente debido a la limitación en el número de bits disponibles para la mantisa. En una serie de operaciones, la acumulación de estos pequeños errores puede dar lugar a resultados imprecisos o, incluso, a una propagación de errores a través de las iteraciones, lo que podría comprometer la seguridad de un sistema criptográfico si no se maneja adecuadamente. Esta imprecisión es aún más relevante cuando se realizan cálculos iterativos en métodos de ataque como búsquedas de claves o fuerza bruta, donde las pequeñas variaciones pueden alterar significativamente los resultados finales si no se toman en cuenta las posibles pérdidas de precisión en las representaciones numéricas.

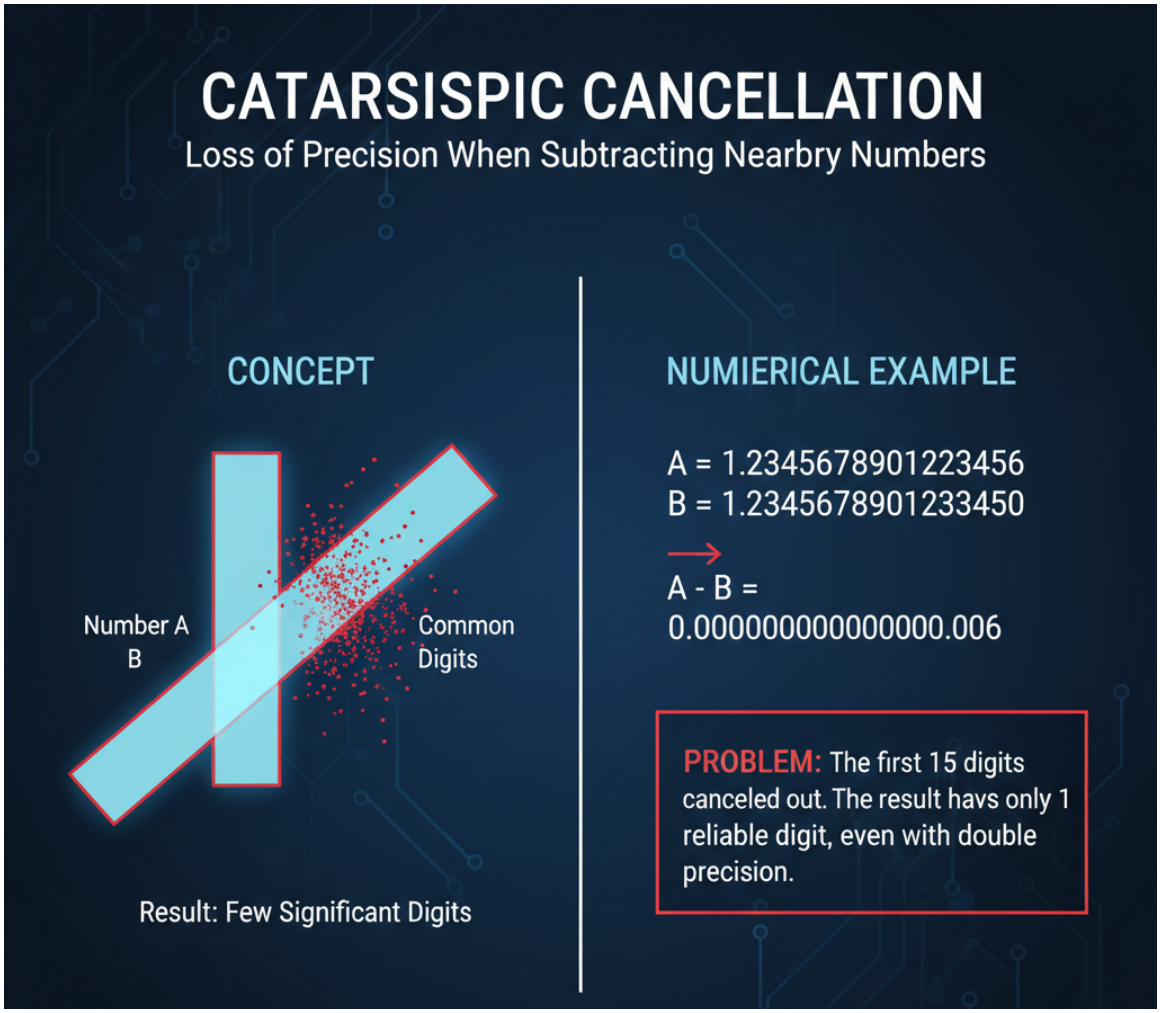

Figura 6: Ilustración visual del fenómeno de cancelación catastrófica al restar números muy cercanos.

Creación propia.

El fenómeno de la cancelación catastrófica ocurre cuando se restan dos números que son extremadamente cercanos entre sí, y debido a las limitaciones inherentes a la

representación numérica en punto flotante (como la que se utiliza en el estándar IEEE 754 de doble precisión), se produce una pérdida de precisión considerable. Este problema se debe a que la finita cantidad de bits disponibles para almacenar números en punto flotante no es suficiente para representar con exactitud las pequeñas diferencias entre números muy cercanos. Así, al realizar la resta de dos valores como, por ejemplo, ($\mathbf{a} = \mathbf{1.23456789012345}$) y ($\mathbf{b} = \mathbf{1.23456789012344}$), el resultado de la operación debería ser 0.00000000000001, un valor muy pequeño. Sin embargo, debido a la representación en binario de los números en doble precisión, esta diferencia tan pequeña no puede ser representada con la exactitud necesaria, lo que genera un error de redondeo que afecta seriamente al cálculo final.

Este fenómeno tiene implicaciones serias en el análisis numérico y la ciberseguridad, especialmente en criptoanálisis y en la aproximación de claves criptográficas. Cuando se realizan cálculos iterativos para, por ejemplo, aproximarse a una clave en un ataque de fuerza bruta o en una técnica de análisis diferencial, pequeños errores debido a la cancelación catastrófica pueden alterar el resultado de manera drástica. En estos casos, la correcta interpretación y manejo de los cálculos numéricos es crucial, ya que cualquier error de redondeo puede dar lugar a una propagación de imprecisiones que distorsiona la búsqueda de la clave correcta. Un atacante que no considere estos errores podría perder la pista de su objetivo debido a los fallos de precisión introducidos por la cancelación catastrófica, lo que lo llevaría a conclusiones incorrectas y a un análisis ineficaz.

Error absoluto y error relativo

El error absoluto se define como la diferencia directa entre el valor verdadero y el aproximado:

$$\boldsymbol{Error\ absoluto} = |\boldsymbol{valor\ verdadero} - \boldsymbol{valor\ aproximado}|$$

El error relativo normaliza este valor respecto a la magnitud del verdadero, siendo más útil cuando se trabajan con números grandes (como módulos RSA de 2048 bits):

$$\boldsymbol{Error\ relativo} = |\boldsymbol{error\ absoluto}| \ / \ |\boldsymbol{valor\ verdadero}|$$

Figura 7: Comparación gráfica entre error absoluto y error relativo en cálculos con números grandes típicos de criptografía.

Creación propia.

Error de redondeo y error de truncamiento

El error de redondeo surge al representar un número real en la precisión finita de la máquina. Ocurre en cada operación aritmética (suma, multiplicación) cuando el resultado excede los bits disponibles y se redondea (hacia cero, al más cercano, etc.).

Ejemplo: en implementaciones de exponenciación modular rápida (usada en RSA o Diffie-Hellman), acumulaciones de redondeo en reducciones intermedias pueden introducir sesgos explotables vía timing attacks.

El error de truncamiento aparece al aproximar procesos infinitos con finitos: series de Taylor cortadas, diferencias finitas para derivadas o reglas de integración numérica.

En ciberseguridad: truncamiento en aproximaciones polinómicas (ataques Coppersmith) puede fallar en encontrar raíces cortas, o en Monte Carlo para estimación de riesgos, truncar iteraciones tempranamente subestima la probabilidad de éxito de un exploit.

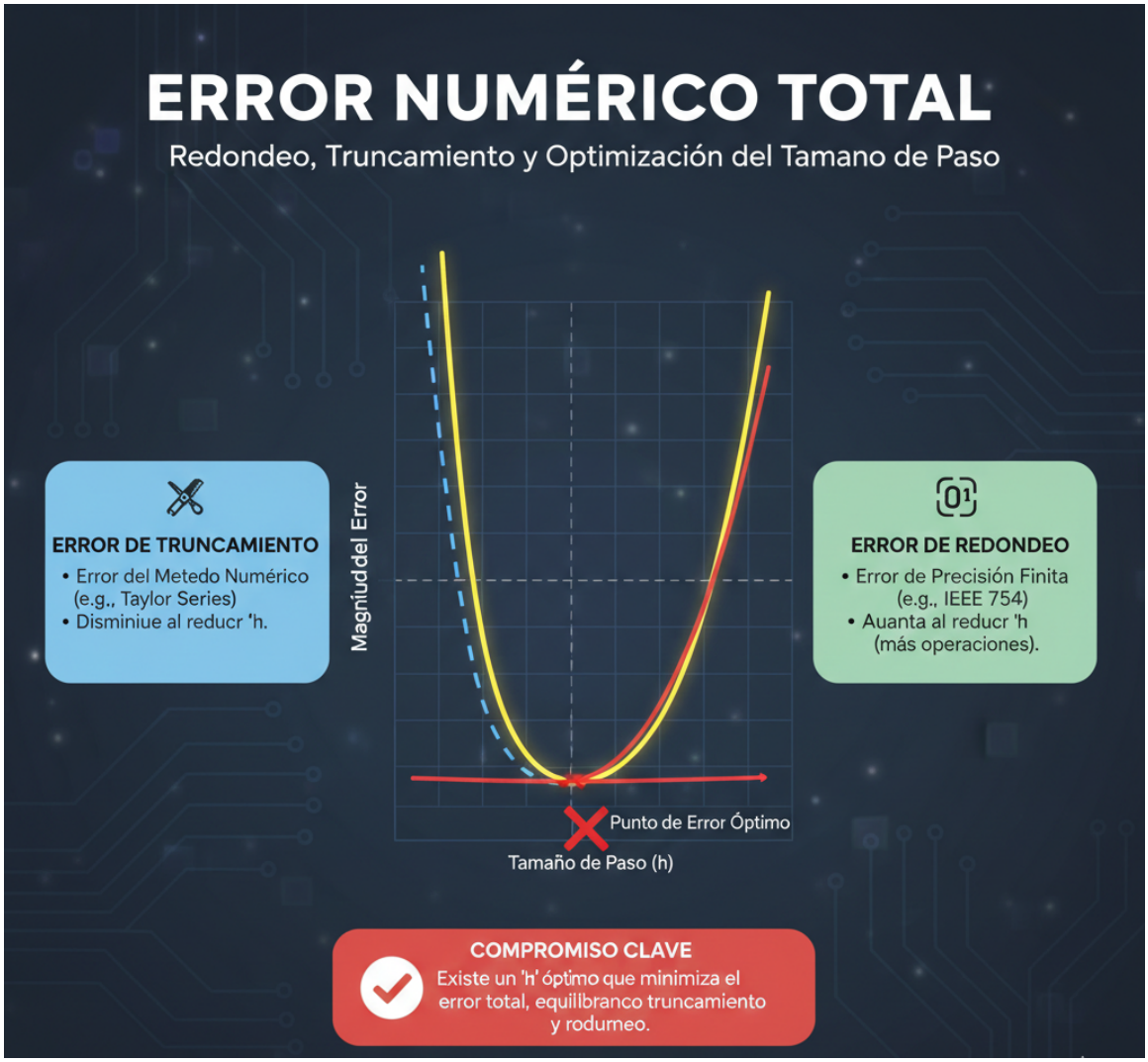

Figura 8: Diagrama de error de redondeo vs truncamiento y error total en función del tamaño de paso.

Creación propia.

Propagación del error

La propagación del error describe cómo los errores pequeños en entradas o pasos intermedios se amplifican en la salida final. Depende del condicionamiento del problema (número de condición κ) y la estabilidad del algoritmo.

El número de condición κ mide la sensibilidad: κ ≈ 1 → bien condicionado (errores no se amplifican mucho) κ >> 1 → mal condicionado (pequeños errores de entrada causan grandes errores de salida)

En ciberseguridad:

- En lattices (NTRU, Kyber), matrices mal condicionadas amplifican errores numéricos, fallando en reducción BKZ o recuperación de claves.
- En side-channel: propagación en acumulaciones de correlación puede diluir picos.

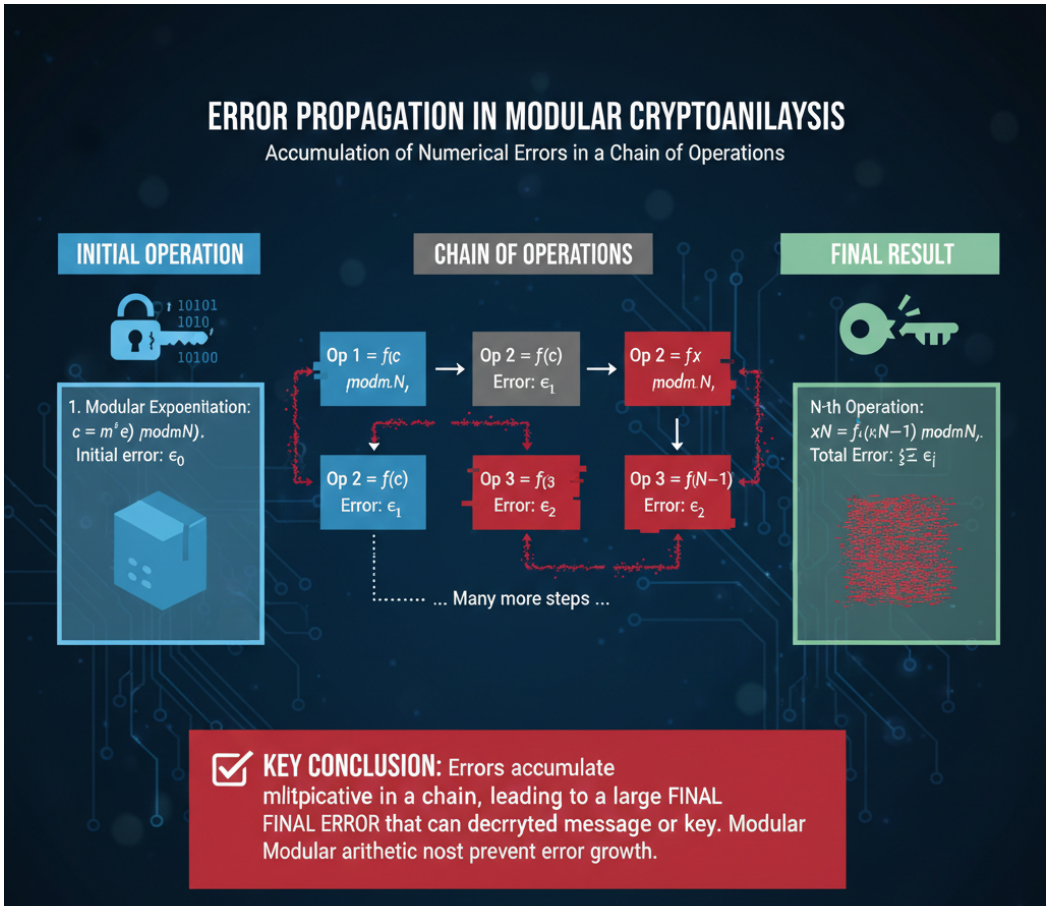

Figura 9: Diagrama de propagación de errores a lo largo de una cadena de operaciones en criptoanálisis modular.

Creación propia.

REFERENCIAS

• **Boneh, D., & Shoup, V. (2020).** A graduate course in applied cryptography. https://toc.cryptobook.us

• **Higham, N. J. (2002).** Accuracy and stability of numerical algorithms (2ª ed.). SIAM.

• **Kocher, P., Jaffe, J., & Jun, B. (1999).** Differential power analysis. Advances in Cryptology — CRYPTO ’99. Springer.

• **Overton, M. L. (2001).** Numerical computing with IEEE floating point arithmetic. SIAM.

• **Paar, C., & Pelzl, J. (2010).** Understanding cryptography: A textbook for students and practitioners. Springer.

PUCE Virtual

síguenos en:

www.pucevirtual.puce.edu.ec