Ejercicios de Criptografía Cuántica

Ejercicio I: El Algoritmo de Shor y su Repercusión en la Criptografía Actual

Introducción

El algoritmo de Shor, desarrollado por el matemático Peter Shor en 1994, es un algoritmo cuántico que revolucionó el campo de la criptografía. Está diseñado para factorizar números enteros grandes de manera exponencialmente más rápida que cualquier algoritmo clásico conocido. Esto representa una amenaza directa para sistemas criptográficos ampliamente utilizados, como RSA, que basan su seguridad en la dificultad de la factorización.

Fundamento del Algoritmo

El algoritmo de Shor se basa en la idea de transformar el problema de la factorización en un problema de búsqueda de períodos, específicamente el período de la función $f(x) = a^x \bmod N$. La parte clásica del algoritmo se complementa con una parte cuántica que utiliza la transformada de Fourier cuántica (QFT) para encontrar ese período de forma eficiente.

El proceso se puede dividir en dos partes:

1. Parte clásica: se elige un número aleatorio $a < N$ y se verifica si es coprimo con N.
2. Parte cuántica: se busca el período r de la función $f(x) = a^x \bmod N$. Con este período, se pueden hallar los factores de N utilizando el MCD entre $a^{(r/2)} \pm 1$ y N.

Ejemplo Ilustrativo (versión simplificada)

Supongamos que queremos factorizar N = 15.

1. Elegimos a = 2 (aleatoriamente).
2. Calculamos potencias: $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16 \bmod 15 = 1$. Entonces, r = 4.
3. Calculamos $MCD(2^{(r/2)} - 1, 15) = MCD(3, 15) = 3$.
   $MCD(2^{(r/2)} + 1, 15) = MCD(5, 15) = 5$.

Por tanto, 3 y 5 son factores de 15.

Aunque este ejemplo es con números pequeños, el principio es el mismo para números grandes.

Complejidad y Ventaja Cuántica

Mientras los algoritmos clásicos tienen complejidad subexponencial, el algoritmo de Shor es polinómico: O((log N)^3). Esto implica que podría romper claves de RSA-2048 en horas o minutos si se dispone de un ordenador cuántico con suficientes qubits estables y corrección de errores.

Aplicaciones prácticas actuales

IBM, Google y otras empresas han desarrollado ordenadores cuánticos de hasta 100 qubits. Aunque aún están lejos de poder ejecutar Shor a gran escala, ya han realizado factorizaciones de números pequeños como 21, 35 o 56153. Se espera que en 10-20 años se alcance la capacidad necesaria para atacar claves modernas.

Impacto en la Criptografía Actual

Los algoritmos afectados directamente incluyen:

- RSA: basada en factorización.
- DSA/Diffie-Hellman: basada en logaritmo discreto.
- ECC: logaritmo discreto en curvas elípticas.

Todos estos algoritmos quedarían obsoletos con la llegada de un ordenador cuántico funcional y estable.

Conclusión

El algoritmo de Shor representa tanto una amenaza como una oportunidad: nos obliga a replantear la seguridad criptográfica moderna y avanzar hacia soluciones resistentes a la computación cuántica. La migración debe comenzar antes de que los ordenadores cuánticos sean una realidad masiva, ya que los datos cifrados hoy podrían ser descifrados mañana.

Avances recientes y perspectivas futuras

Grandes empresas tecnológicas y laboratorios de investigación están compitiendo para construir ordenadores cuánticos escalables. IBM ha lanzado su hoja de ruta hacia ordenadores con más de 4.000 qubits para 2025. Google, por su parte, alcanzó en 2019 la llamada "supremacía cuántica", resolviendo un problema específico que sería casi imposible para un

ordenador clásico. Aunque estas máquinas aún no pueden ejecutar el algoritmo de Shor contra claves reales, los avances son constantes.

La investigación en corrección de errores cuánticos y estabilidad de qubits es clave. Se estima que un ordenador cuántico capaz de romper RSA-2048 necesitaría entre 4.000 y 10.000 qubits con bajo nivel de error y capacidad de mantener la coherencia cuántica durante los miles de operaciones necesarias para ejecutar el algoritmo. Aunque técnicamente desafiante, muchos expertos coinciden en que este escenario podría materializarse entre 2030 y 2040.

Consecuencias prácticas para organizaciones

Aunque los ataques cuánticos aún no son una realidad práctica, ya existe el riesgo de los llamados ataques "store now, decrypt later": los datos cifrados con RSA pueden ser capturados hoy y descifrados en el futuro. Esto es especialmente grave para organizaciones que manejan información que debe mantenerse confidencial durante décadas: entidades gubernamentales, sistemas de defensa, servicios de salud o registros legales.

Por tanto, es imprescindible comenzar desde ahora con auditorías internas de sistemas criptográficos y evaluación del riesgo cuántico, adoptando políticas de transición hacia criptografía resistente a esta amenaza.

Alternativas criptográficas seguras frente a Shor

Como respuesta al algoritmo de Shor, se están desarrollando algoritmos post-cuánticos basados en problemas matemáticos que se consideran resistentes a los ordenadores cuánticos, como:

- Problemas de retículos (lattice-based cryptography).
- Códigos de corrección de errores (code-based).
- Funciones hash y multivariables.
- Isogenias de curvas elípticas (aunque algunos esquemas fueron vulnerados recientemente).

Conclusión ampliada

El algoritmo de Shor es el principal motor que impulsa la migración global hacia la criptografía post-cuántica. Su impacto teórico es suficiente para considerar obsoletos, en el mediano plazo, los sistemas actuales de cifrado y firma digital. Si bien no representa una amenaza inmediata, su poder disruptivo requiere acción preventiva y proactiva por parte de gobiernos, instituciones educativas, empresas tecnológicas y organismos internacionales. El futuro de la seguridad digital depende de cómo se gestione esta transición en la próxima década.

Ejercicio II: El Teorema de Mosca y la Necesidad de una Transición hacia Criptografía Quantum-Safe

Introducción

El Teorema de Mosca, formulado por Michele Mosca, matemático canadiense experto en computación cuántica, plantea una reflexión crítica sobre el tiempo disponible para migrar a sistemas criptográficos seguros frente a la amenaza cuántica. Se basa en una simple desigualdad temporal: si el tiempo que tarda en desarrollarse un ordenador cuántico capaz de romper la criptografía actual (x) más el tiempo necesario para migrar a sistemas seguros (y) es mayor que el tiempo que los datos necesitan mantenerse seguros (z), entonces hay un riesgo real de exposición.

El Teorema

Formalmente, se expresa como:

Si x + y > z, entonces estamos en problemas.

Esto significa que, si no iniciamos la transición a tiempo, los datos cifrados hoy podrían ser vulnerables en el futuro, ya que podrían ser almacenados ahora y descifrados posteriormente cuando la tecnología cuántica lo permita.

Implicaciones

El teorema resalta la importancia de no esperar a que el ordenador cuántico exista para comenzar a adoptar criptografía post-cuántica. Algunos datos, como expedientes médicos, secretos industriales o información gubernamental, necesitan ser protegidos por décadas. Si

se capturan ahora bajo esquemas como RSA y se almacenan, podrían ser descifrados más adelante.

Transición Necesaria

Por todo ello, organizaciones, gobiernos y empresas deben comenzar **desde ya** la transición hacia la criptografía quantum-safe (basada en problemas difíciles para ordenadores cuánticos como redes euclidianas o códigos de corrección). NIST ya ha seleccionado algoritmos finalistas en este campo, como CRYSTALS-Kyber y CRYSTALS-Dilithium.

Conclusión

El Teorema de Mosca no es una predicción científica del futuro, sino un llamado a la acción: si esperamos demasiado, el daño será inevitable. La migración a sistemas resistentes a la computación cuántica debe empezar hoy para asegurar el mañana.

Ejercicio III: Recomendaciones para Mejorar la Seguridad Criptográfica Frente a la Amenaza de un Ordenador Cuántico

Introducción

Los ordenadores cuánticos representan una amenaza directa para los sistemas criptográficos actuales. Por ello, es esencial establecer una estrategia organizacional que permita transitar hacia algoritmos resistentes a ataques cuánticos. A continuación, se presentan recomendaciones concretas para organizaciones públicas y privadas.

1. Inventario y clasificación de activos criptográficos
   - Registrar todos los sistemas que usan criptografía (servidores, apps, VPN, dispositivos IoT).
   - Clasificarlos según nivel de criticidad y tiempo de vida de los datos.
   - Referencia: ISO/IEC 27005.

2. Evaluación de riesgos específicos del entorno cuántico
   - Determinar la probabilidad e impacto de que los datos sean capturados hoy y desencriptados en el futuro.
   - Aplicar el Teorema de Mosca como marco temporal.

- Referencia: ENISA Post-Quantum Security Guidelines.

3. Transición progresiva a algoritmos post-cuánticos
- Empezar pruebas piloto con algoritmos como CRYSTALS-Kyber y Dilithium.
- Aplicar primero en servicios de correo seguro, autenticación y almacenamiento.
- Usar TLS híbrido (clásico + post-cuántico).
- Referencia: NIST PQC Standardization Process.

4. Desarrollar una estrategia de Crypto Agility
- Garantizar que los sistemas permitan reemplazar algoritmos criptográficos sin rediseñar toda la arquitectura.
- Evitar el uso de algoritmos embebidos (hardcoded).
- Referencia: Microsoft Quantum Whitepaper (2022).

5. Capacitación continua y concienciación
- Realizar cursos internos sobre computación cuántica y sus riesgos.
- Incluir al personal no técnico en procesos de concienciación.
- Referencia: ETSI TR 103 619.

6. Integración con proveedores
- Exigir a proveedores tecnológicos que implementen esquemas post-cuánticos en sus productos y servicios.
- Incluir cláusulas específicas en los contratos.
- Establecer auditorías conjuntas.

7. Plan de migración específico por sector
- En sector salud: proteger historiales médicos durante décadas.
- En banca: asegurar comunicaciones y firmas digitales.
- En sector público: cifrado de documentos oficiales, identidad digital y procesos judiciales.
- Referencia: EU Cybersecurity Act.

8. Seguimiento de avances tecnológicos y normativos
- Vigilar publicaciones de NIST, ETSI, ISO, ENISA.
- Participar en foros especializados para estar a la vanguardia.

Conclusión

La adopción de criptografía post-cuántica es una necesidad estratégica, no una opción. Actuar ahora garantiza una ventaja competitiva, cumplimiento normativo y protección futura. La resistencia cuántica debe integrarse al ADN de la ciberseguridad organizacional.

9. Incorporar soluciones híbridas como medida transitoria

Muchas organizaciones no pueden sustituir de inmediato toda su infraestructura criptográfica. Por ello, se recomienda adoptar esquemas híbridos, combinando algoritmos tradicionales (como RSA o ECC) con esquemas post-cuánticos. De esta forma se obtiene un nivel de seguridad inmediato, pero preparado para el futuro.

Ejemplo: en el protocolo TLS 1.3, se puede usar una clave híbrida generada por ECDH (curvas elípticas) y CRYSTALS-Kyber. Esta combinación asegura compatibilidad y resistencia.

10. Realizar simulaciones de ciberataques cuánticos

Para comprobar la preparación ante amenazas cuánticas, se pueden simular escenarios donde un atacante tenga acceso a capacidad de factorización cuántica. Esto ayuda a:

- Detectar sistemas vulnerables.
- Evaluar tiempos de respuesta.
- Mejorar protocolos internos de gestión de incidentes.

11. Integrar la resistencia cuántica en políticas corporativas

Es necesario que los comités de seguridad de la información incluyan explícitamente la resistencia cuántica en sus políticas de seguridad. Esto afecta directamente la adquisición de tecnología, la redacción de contratos, el diseño de productos y la capacitación del personal.

12. Casos reales de migración

Organizaciones como Microsoft, IBM, Cloudflare, Google y AWS ya están probando o integrando algoritmos post-cuánticos en sus plataformas. Por ejemplo, Google ha implementado versiones de Chrome con pruebas de Kyber en TLS. Estas iniciativas muestran que la industria ya está avanzando en esa dirección.

13. Consideraciones para pequeñas y medianas empresas (PYMES)

Las PYMES también deben actuar, aunque su nivel de exposición sea menor:
- Evaluar servicios de terceros que ya ofrezcan cifrado post-cuántico.
- Formarse en normativas emergentes (como los estándares del NIST).
- Integrar medidas de crypto-agility al desarrollar software.

Bibliografía

Cyber chiefs unveil new roadmap for post-quantum cryptography migration. (s. f.). https://www.ncsc.gov.uk/news/pqc-migration-roadmap-unveiled

Martello, D. (2024, 24 octubre). *Algoritmo de Shor: como las computadoras cuánticas pueden romper los cimientos de la criptografía actual*. Blog de Divulgación Científica y Tecnológica. https://divulgando-ciencia.blog/algoritmo-de-shor-o-como-las-computadoras-cuanticas-pueden-romper-la-base-de-la-criptografia-actual/

Normativa ISO/IEC 27005. (s. f.).