Retos para la seguridad en un futuro cercano
¿está la Criptografía preparada?

Luis Hernández Encinas

Jornadas Técnicas de RedIRIS, 2019

Sevilla, 29 de mayo

Instituto de Tecnologías Físicas y de la Información (ITEFI)
Consejo Superior de Investigaciones Científicas (CSIC)
C/ Serrano 144, Madrid, España

luis@iec.csic.es

http://www.itefi.csic.es/es/personal/hernandez-encinas-luis

Criptografía – Criptoanálisis

Criptografía: Diseña protocolos que permitan el intercambio de mensajes de forma confidencial, íntegra y autenticada, utilizando canales inseguros.

Se utilizan claves y algoritmos para cifrar/descifrar y firmar/verificar mensajes.

Criptoanálisis: Estudia las posibles debilidades de los protocolos criptográficos con el fin de garantizar su seguridad.

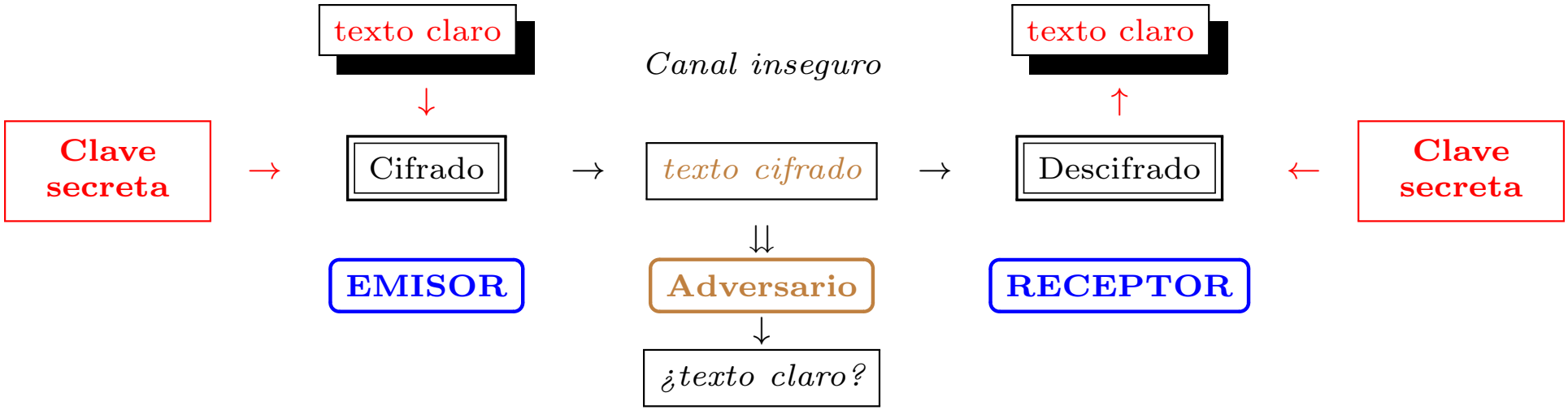
Encontrar las claves empleadas o resolver el algoritmo utilizado.

Uso de técnicas y herramientas:

matemáticas, físicas, computacionales y de comunicación.

Esquema de Cifrado/Descifrado simétrico

Los criptosistemas simétricos emplean la misma clave para cifrar y para descifrar. Su seguridad se basa en mantener la clave en secreto, con un tamaño adecuado.

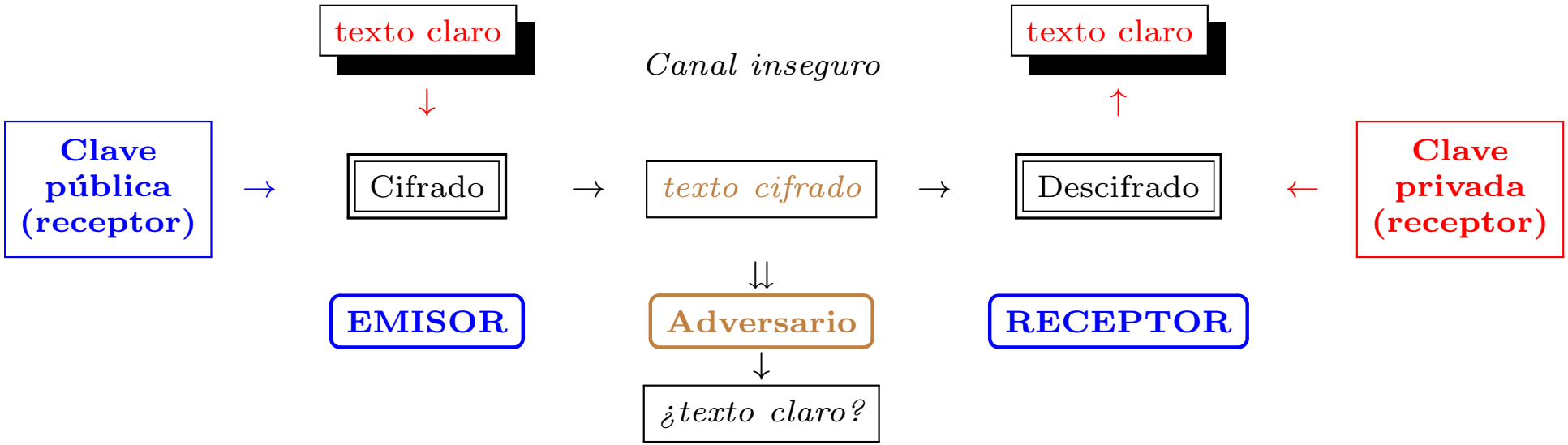


Ejemplos: Triple-DES, AES, Blowfish, etc.

Problema de la distribución de claves $\rightsquigarrow$ *Quantum Key Distribution.*

Esquema de Cifrado/Descifrado asimétrico

Los criptosistemas asimétricos usan una clave para cifrar y otra distinta para descifrar. Su seguridad se basa en la dificultad computacional de resolver un problema matemático considerado difícil: IFF, DLP, ECDLP, etc.



Ejemplos: RSA, ElGamal, ECC, etc.

Ataques a la Criptografía simétrica actual

En 1997, K.L. Grover publicó un algoritmo (*Quantum mechanics helps in searching for a needle in a haystack*, Phys. Rev. Lett. 79, 1997, 325–328) por el que la computación cuántica reduciría el tiempo necesario para romper la criptografía simétrica a la raíz cuadrada del tiempo actual.

Si un PC necesita $\mathcal{O}(n)$ operaciones bit para romper un algoritmo, con este algoritmo cuántico harían falta $\mathcal{O}\left(\sqrt{n}\right)$ operaciones y una memoria de $\mathcal{O}(\log n)$.

Es decir, un ordenador cuántico tardaría el mismo tiempo en realizar una búsqueda exhaustiva de claves de 256 bits (2^{256} claves) que un PC actual con claves de 128 bits (2^{128} claves).

Recientes publicaciones (Naya-Plasencia, 2016) demuestran que la criptografía simétrica puede no estar tan preparada para resistir la computación cuántica dado que se han encontrado aceleraciones exponenciales en ataques a sistemas criptográficos simétricos.

Ataques a la Criptografía asimétrica actual

En 1997 (1994/95), P.W. Shor publicó un artículo (*Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J. Computing 5, 26, 1997, 1484–1509) proponiendo dos algoritmos cuánticos que pueden romper en tiempo polinómico los problemas de la factorización de enteros y del logaritmo discreto.

Si con un PC actual un algoritmo precisara de $\mathcal{O}\left(2^{\sqrt[3]{\log n}}\right)$ operaciones bit para ser roto, con un ordenador cuántico y el algoritmo de Shor, este tiempo se reduciría a $\mathcal{O}\left(\log^3 n\right)$ operaciones bit y una memoria de $\mathcal{O}(\log n)$.

Esto es, un ordenador cuántico sería capaz de romper en tiempo polinómico la mayoría de los criptosistemas asimétricos actuales.

¿Qué hacen los criptográfos actualmente?

Dado que la llegada del ordenador cuántico supondrá la desaparición de la criptografía asimétrica actual (RSA, ECC, DH, ECDH, DSA, ECDSA, HTTPS, TLS, PGP, GPG, etc.), los criptógrafos están investigando nuevos/viejos problemas matemáticos para proponer criptosistemas asimétricos resistentes a la computación cuántica (*quantum resistant*).

Los nuevos problemas matemáticos están basados en:

- Teoría de Códigos (*Coding theory*).
- Funciones Resumen (*Hash functions*).
- Sistemas de ecuaciones polinómicas cuadráticas en varias variables (*Multivariate Quadratic*).
- Retículos (*Lattices*).
- Isogenias entre Curvas Elípticas (*Isogenies*).

Llamada del NIST

El NIST ha puesto el interés en los criptosistemas asimétricos (se olvida de los simétricos) haciendo una llamada internacional para elegir futuros estándares resistentes a la computación cuántica (proceso similar a la elección de AES y SHA-3).

24-26/02/2016	Presentación del NIST en el PQCrypto 2016
28/04/2016	El NIST lanza el NISTIR 8105
20/12/2016	Llamada formal para propuestas
30/11/2017	Fecha límite para envío de propuestas
04/12/2017	Presentación del NIST en el AsiaCrypt 2017
21/12/2017	Anuncio de los algoritmos incluidos en la Ronda 1
11/04/2018	Presentación del NIST en el PQCrypto 2018
11-13/04/2018	Primera PQC Standardization Conference
2018/2019	Inicio de la Ronda 2
August 2019	Segunda PQC Standardization Conference
2020/2021	Inicio de la Ronda 3 o algoritmos seleccionados
2022/2024	Publicación del primer Draft Standards

Estado actual

Se aceptaron 69 algoritmos en la Ronda 1 (11/2017) y muy pronto se retiraron 5 después de numerosos comentarios abiertos.

https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions

En enero de 2019 se ha publicado la lista de los algoritmos que se mantienen en la Ronda 2.

Los 26 algoritmos que aún se mantienen en esta competición corresponden a 17 criptosistemas de clave pública y protocolos de acuerdo de clave (Classic McEliece, NTRU, Newhope, etc.) y a 9 de firma electrónica (Rainbow, SPHINCS+, etc.)

https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions

Muchas gracias por su atención