- Cryptographic Attack Possibilities over RSA Algorithm through Classical and Quantum Computation

El sistema criptográfico RSA es usado para el diseño de cifrado, su protocolo de seguridad funciona según el principio de factorización de enteros grandes que descompone el número compuesto en un producto de números primos. En dicho survey se describe un ataque por fuerza bruta, en la que tiene como objetivo encontrar la clave secreta consultando la función de cifrado sucesivamente con todas las posibles claves. Por otro lado, para vulnerar el algoritmo RSA es necesario la factorización de números enteros grandes, actualmente no existe un algoritmo en tiempo polinomial que pueda realizarlo en una computadora clásica, sin embargo en dicho survey se propone el Algoritmo Shor logra factorizar números enteros grandes en tiempo polinomial, pero este algoritmo sólo puede ejecutarse en una computadora cuántica. [Cryptographic Attack Possibilities over RSA Algorithm through Classical and Quantum Computation]

https://ieeexplore.ieee.org/document/8748675

```
@INPROCEEDINGS{8748675,
  author={Soni, Kapil Kumar and Rasool, Akhtar},
  booktitle={2018 International Conference on Smart Systems and Inventive Technology (ICSSIT)},
  title={Cryptographic Attack Possibilities over RSA Algorithm through Classical and Quantum Computation},
  year={2018},
  volume={},
  number={},
  pages={11-15},
  doi={10.1109/ICSSIT.2018.8748675}}
```

- Quantum Algorithm for Attacking RSA Based on Fourier Transform and Fixed-Point

Shor diseña un algoritmo cuántico de tiempo polinomial para encontrar el orden r de un elemento a en el grupo multiplicativo Z_n^* , que es usado para factorizar el entero positivo n y lograr así romper el famoso sistema criptográfico RSA, pero está sujeto a una condición, donde se requiere que r sea par, sin embargo dicho survey propone un ataque de punto fijo basado en la transformada inversa cuántica de Fourier y la estimación de fase, este algoritmo se ejecuta en tiempo polinomial cuántico y no necesita factorizar explícitamente el módulo n y además no requiere que r sea par, esta propuesta asegura que la probabilidad de éxito sea mayor frente al algoritmo Shor, pero la complejidad del tiempo es la misma para ambos. [Quantum Algorithm for Attacking RSA Based on Fourier Transform and Fixed-Point], [Quantum Polynomial-Time Fixed-Point Attack for RSA]

https://www.researchgate.net/publication/357840113_Quantum_Algorithm_for_Attacking_RSA_Based_on_Fourier_Transform_and_Fixed-Point

@article{ refId0,
	author = {{WANG, Yahui} and {ZHANG, Huanguo}},
	title = {Quantum Algorithm for Attacking RSA Based on Fourier Transform and Fixed-Point},
	DOI= "10.1051/wujns/2021266489",
	url= "https://doi.org/10.1051/wujns/2021266489",
	journal = {Wuhan Univ. J. Nat. Sci.},
	year = 2021,
	volume = 26,
	number = 6,
	pages = "489-494",
}

- Experimental Analysis of Attacks on RSA & Rabin Cryptosystems using Quantum Shor's Algorithm

  Este survey propone, cómo el algoritmo de Shor puede romper los algoritmos de de criptografía que se basan en factorización como el RSA y los algoritmos de Rabin usando IBM Quantum Experience, pero dicho experimento se hará con no más de 7 bits, puesto que IBM ofrece solo 32 qubits. El enfoque de dicho survey está en demostrar que el algoritmo de Quantum Shor representa un peligro para los criptosistemas asimétricos que utilizan productos de números primos grandes para la generación de claves. [Experimental Analysis of Attacks on RSA & Rabin Cryptosystems using Quantum Shor's Algorithm]

  https://www.researchgate.net/publication/352181318_Experimental_Analysis_of_Attacks_on_RSA_Rabin_Cryptosystems_using_Quantum_Shor's_Algorithm

  @inproceedings{inproceedings,
  author = {Jajodia, Babita and Thombre, Ritu},
  year = {2021},
  month = {04},
  pages = {},
  title = {Experimental Analysis of Attacks on RSA & Rabin Cryptosystems using Quantum Shor's Algorithm},
  doi = {10.21467/proceedings.114.74}
  }

- Quantum Grover Attack on the Simplified-AES

  Este survey presenta la forma de atacar el algoritmo estándar de cifrado avanzado simplificado (S-AES) usando el algoritmo de Grover, donde se construyen circuitos cuánticos para los componentes principales de S-AES para luego juntarlos y formar una versión cuántica de dicho algoritmo; de esta forma el S-AES se integra en una

caja negra que pasara por el algoritmo de Grover y así recuperar la clave secreta en aceleración cuadrática. [Quantum Grover Attack on the Simplified-AES]

https://doi.org/10.1145/3185089.3185122

```
@inproceedings{10.1145/3185089.3185122,
author = {Almazrooie, Mishal and Abdullah, Rosni and Samsudin, Azman and
Mutter, Kussay N.},
title = {Quantum Grover Attack on the Simplified-AES},
year = {2018},
isbn = {9781450354141},
publisher = {Association for Computing Machinery},
address = {New York, NY, USA},
url = {https://doi.org/10.1145/3185089.3185122},
doi = {10.1145/3185089.3185122},
abstract = {In this work, a quantum design for the Simplified-Advanced
Encryption Standard (S-AES) algorithm is presented. Also, a quantum Grover
attack is modeled on the proposed quantum S-AES. First, quantum circuits for
the main components of S-AES in the finite field F2[x]/(x4 + x + 1), are
constructed. Then, the constructed circuits are put together to form a
quantum version of S-AES. A C-NOT synthesis is used to decompose some of the
functions to reduce the number of the needed qubits. The quantum S-AES is
integrated into a black-box queried by Grover's algorithm. A new approach is
proposed to uniquely recover the secret key when Grover attack is applied.
The entire work is simulated and tested on a quantum mechanics simulator.
The complexity analysis shows that a block cipher can be designed as a
quantum circuit with a polynomial cost. In addition, the secret key is
recovered in quadratic speedup as promised by Grover's algorithm.},
booktitle = {Proceedings of the 2018 7th International Conference on
Software and Computer Applications},
pages = {204–211},
numpages = {8},
keywords = {Symmetric cryptography, Quantum cryptanalysis, Block cipher,
Quantum simulation, Grover attack},
location = {Kuantan, Malaysia},
series = {ICSCA 2018}
}
```

- Variational quantum attacks threaten advanced encryption standard based symmetric cryptography

  Este survey propone un Variational Quantum Attack Algorithm (VQAA) para la criptografía simétrica AES (Advanced Encryption Standard), a su vez muestra cómo en ocasiones el VQAA es mucho más rápido que el algoritmo de Grover utilizando el mismo orden de consultas de espacio de búsqueda, así como también muestran la relación entre la entropía de entrelazamiento, la concurrencia y la función de costo.[Variational quantum attacks threaten advanced encryption standard based symmetric cryptography]

  https://www.researchgate.net/publication/362163448_Variational_quantum_attacks_threaten_advanced_encryption_standard_based_symmetric_cryptography

  @article{article,
  author = {Wang, Zeguo and Wei, Shijie and Long, Gui and Hanzo, L.},

year = {2022},
month = {10},
pages = {200503},
title = {Variational quantum attacks threaten advanced encryption standard based symmetric cryptography},
volume = {65},
journal = {Science China Information Sciences},
doi = {10.1007/s11432-022-3511-5}
}

TAXONOMÍA
https://miro.com/app/board/uXjVPKAdrqE=/

Asimétrica:

- Propuesta 1
  - RSA
  - Algoritmo Shor
    - Factorización de enteros
  - Transformada cuántica de fourier
  - Algoritmo de fuerza bruta
- Propuesta 2
  - RSA
  - Algoritmo shor
    - Factorización de enteros
  - Punto fijo
    - Transformada Inversa Cuántica de Fourier
- propuesta 3
  - RSA
  - Algoritmos Rabin
  - Algoritmo Shor
    - Factorización de enteros
    - Computadoras cuánticas de 32 qubits
    - Números de 7 bits

Simétrica:

- propuesta 1
  - AES
  - S-AES
  - Algoritmo Grover
    - Recuperación de clave secreta
- propuesta 2
  - AES
  - S-AES
  - DES
  - Variational Quantum Attack Algorithm
  - Relación
    - Entropía de entrelazamiento
    - Concurrencia

- Función de costo