**Análisis DES**

A lo largo de la historia la criptografía ha sido un área de estudio que ha evolucionado constantemente por su gran utilidad en numerosas áreas, ya sea para lo militar como lo civil. Debido a las diversas aplicaciones de la criptografía, tanto empresas privadas como gobiernos enteros han destinado esfuerzos a desarrollar algoritmos de cifrado cada vez más sofisticados y difíciles de romper.

Esta constante evolución ha dado paso a estándares que garanticen la seguridad de los sistemas, sin embargo, éstos se han visto vulnerados en varias ocasiones, por lo que también los estándares han cambiado con el paso del tiempo, debido a las pérdidas millonarias que supondrían violar la seguridad de un sistema que usan los estándares que garantizan que esto no pase.

La capacidad computacional es otro factor que también ha aumentado en los últimos años, sin embargo, es un arma de doble filo, ya que si bien implementar algoritmos que pueden tardar mucho tiempo se ha vuelto una tarea sencilla, de igual manera se ha facilitado el desarrollo de algoritmos que puedan romper las claves de cifrado.

El criptoanálisis es un área que ha evolucionado a la par que la criptografía. Su principal objetivo es encontrar la lleva con la cual se ha cifrado un mensaje, sin embargo, la mayoría de los métodos para hallar la llave de cifrado al final terminando usando fuerza bruta, por lo que el costo computacional sigue siendo determinante en estos casos.

Con el paso del tiempo, el costo computacional ha disminuido y también el costo del hardware para construir máquinas capaces de descifrar claves, es por ello que se apuesta en la seguridad a nivel de hardware. Implementar un módulo en el sistema que se encargue del cifrado a bajo nivel sería lo más óptimo, ya que si los estándares cambian debido a brechas de seguridad, entonces sería menos costoso sólo cambiar el módulo destino a esto que toda la arquitectura completa.

El principal objetivo del criptoanálisis es encontrar la llave con la que fueron cifrados los datos, dependiendo de la longitud de la llave, el espacio de búsqueda aumenta exponencialmente conforme la llave es más grande. Construir una máquina capaz de verificar todos esos espacios de búsqueda requiere esfuerzos enormes y además el costo sería muy elevado.

Dentro de los aspectos a considerar para construir una máquina con las características antes descritas se encuentran:

* Tamaño: una máquina con estas características requiere millones de chips para el procesamiento de la información, lo cual se traduce a un espacio muy amplio
* Potencia: Tener a trabajando a muchos procesadores requiere de mucho consumo energético
* Costo monetario: El costo de cada chip varía dependiendo de sus capacidades de procesamiento
* Diseño: El diseño de algoritmos distribuidos capaces de ejecutar las operaciones sin perder consistencia en la información
* Tamaño de la llave: Dependiendo del tamaño de la llave es el tiempo que requerirá el sistema para poder descifrarla
* Cambios: Si se descifra una llave, se debe tomar en cuenta que ésta puede cambiar
* Solución única: No se garantiza que sólo exista una llave como solución para un texto cifrado

**Conclusión**

En la actualidad, la seguridad de los sistemas que implementan algoritmos de cifrado está basada sólo en la llave. Constantemente diversas organizaciones, así como gobiernos, han invertidos dinero y esfuerzo en desarrollar nuevos métodos de cifrado, así como probar los que ya se tienen, para garantizar la solidez de estos.

El avance que se ha dado a lo largo de los años ha sido impresionante, tanto algoritmos de cifrado como técnicas para romperlos han ido evolucionando y los organismos han diseñado estrategias para probar estos algoritmos; premios a quien logre romperlos, competencias o incentivos para aquellas personas que mejores o encuentren vulnerabilidades.

Uno de los factores determinantes ha sido el mejoramiento de los procesadores que ha permitido disminuir el costo computacional de los algoritmos y esto también trae consigo un riesgo, ya que los atacantes tienen mayor acceso a máquinas capaces de realizar muchas operaciones.

A pesar de todo esto, ningún sistema es completamente seguro, siempre habrá brechas de las cuales se pueden aprovechar los atacantes y la principal y más vulnerable es el usuario.