CIENCIA DE LA COMPUTACIÓN

INFORME CRIPTOGRAFÍA

ALGEBRA ABSTRACTA

ANDRES CUSIRRAMOS
MARQUEZ MARES

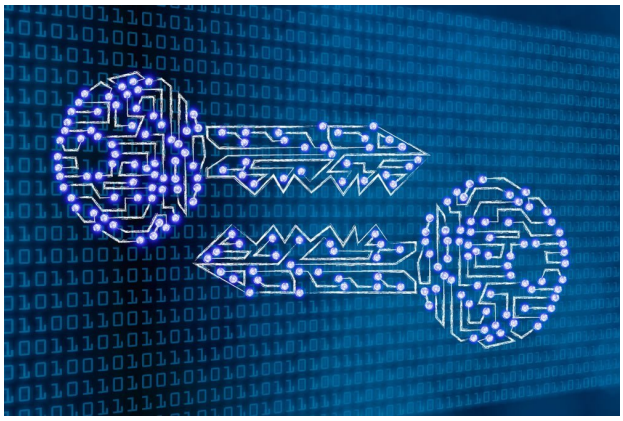
TERCER SEMESTRE
2019

"El alumno declara haber realizado el presente trabajo de acuerdo a las normas de la Universidad Católica San Pablo"

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

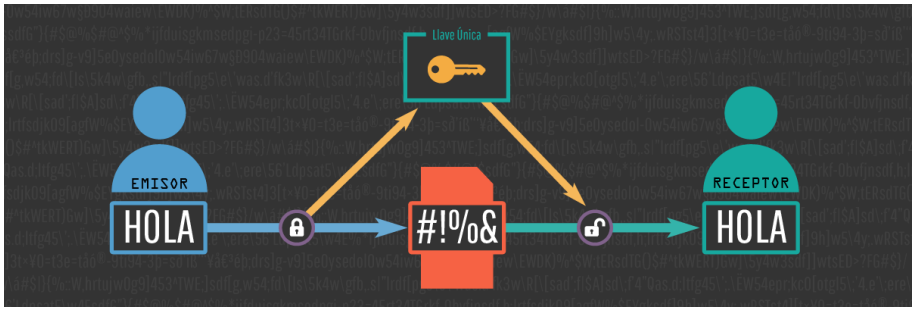
Introducción:

Primero vamos a dar una pequeña definición de lo que se puede entender como criptografía , Se le puede decir a la criptografía el arte y técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quién sepa descifrarlo. A lo largo de la historia de la computacion y desde antes incluso se usaban técnicas de encriptación para poder mandar mensajes sin que sean descubiertos por terceros en este informe vamos a profundizar sobre unos temas en concreto ya que en estos días la criptografia es algo común mas que nuevo pero se pueden dar ciertas ramas de esta que son nuevas o tienen muy poco tiempo como la criptografia ligera. Cabe resaltar que esta ramas de la criptografía es grande y complejas lo que intentare plasmar es un resumen en cual se pueda entender su funcionamiento, su uso y su visión a futuro.



Criptografía Ligera:

En estos días los dispositivos móviles están muy conectados en todo, se tienen dispositivos muy pequeños los cuales pueden contener mucha información privada y que debe estar segura pueden ser datos de salud o hasta bancarios y al ser dispositivos pequeños no pueden tener algoritmos de encriptación muy grandes como un RSA que tiene una exponenciación modular la cual hace que el algoritmo sea muy costoso y hasta lento para un dispositivo pequeño del cual se busca el mejor rendimiento. En concepto internet de las cosas promete un cambio en varias áreas como los cuidados médicos, manufactura, uso de la energía y todo eso apoyaría a los dispositivos en consumo de energía ,almacenamiento en memoria y capacidad de memoria.



Para esto se están usando algoritmos criptográficos livianos, Simon y Speck son familias de cifrados de bloques livianos, lo que significa que son algoritmos criptográficos diseñados para dispositivos de bajos recursos, con memoria y poder de procesamiento limitado. Aunque ambos algoritmos son versátiles en hardware y software, Simon es óptimo en hardware mientras que Speck es óptimo en software. La información detallada sobre las familias de Simon y Speck es compilada por la NSA en su repositorio oficial de Github.

En 2014, se propuso que se incluyeran Simon y Speck (documento IACR) en la norma ISO que especifica los requisitos para la criptografía liviana y con un cifrado adecuado. Publicado en 2012, este estándar ya cubre dos cifras de bloques livianos, Present y Clefia. Además, hay dos "Anteproyectos de enmiendas" registrados sin ninguna información de contenido. Pueden referirse a los códigos de bloque de la NSA propuestos.

En conclusión a pesar que la criptograma es algo ya de muchos años en la raza humana se esta mejorando con el fin de ser mas efectiva y segura y mas pequeña si todos los dispositivos móviles que tienden a ser mas pequeños puedan tener una seguridad de alto nivel para proteger los datos y información privada.