

OFERTA CIBER PARA ESTUDIANTES.

Criptografía en la era de la computación cuántica.



La criptografía tiene un papel fundamental hoy en día. Protege nuestra información cuando viaja a través de Internet (data on-transit) y también cuando se almacena (at rest).

Los ordenadores cuánticos y su capacidad de cómputo mayor hacen peligrar la seguridad de la información / comunicación. Al ser más potentes pueden llegar a romper los algoritmos criptográficos existentes y comprometer los datos encriptados.

Por tanto, una nueva era de algoritmos criptográficos son necesarios, que sean lo suficientemente robustos ante las capacidades de los ordenadores cuánticos, i.e algoritmos criptográficos quantum-resistance.

En este proyecto se pretende investigar el estado del arte de estos algoritmos criptográficos post-quánticos, integrarlos en tecnologías actuales, y realizar un benchmarking de dichas tecnologías con algoritmos criptográficos actuales y con los post-cuánticos.

OBJETIVOS DEL PROYECTO:

- Conocimientos generales en criptografía
- Conocimientos en algoritmos criptográficos post-quantum
- Capacitación en tecnologías que usan criptografía

LAS FASES SERÁN:

- Análisis de algoritmos post-quánticos. Estado del arte de algoritmos propuestos por el NIST, beneficios, inconvenientes
- Selección y prueba de concepto de pilotos que implementen algoritmos quantum-resistance para servicios de VPN, TLS, y SSH
- Benchmarking para tecnologías que usen criptografía; comparativa de tecnologías usando algoritmos criptográficos actuales y los post-cuánticos. y sin algoritmos quantum-resistance.

TUTOR DE IKERLAN:

Leticia Montalvilla

Nuestra cultura Ikerlaniana.

- El mundo no se nos ha dado para contemplarlo sino para transformarlo.
- La tecnología, nuestra actitud.
- Un Proyecto cooperativo vivo de todos y para todos.
- Una filosofía de trabajo que apuesta por la excelencia, cercanía y autonomía.

**¡YA ERES PARTE
DE NUESTRO EQUIPO!**

Nacimos para mejorar y transformar nuestro entorno a través de la tecnología. Por eso, no es casualidad que seamos líderes en transferencia de tecnología a las empresas. Nos gusta soñar e imaginar el futuro. Pero sobre todo nos encanta crear tecnología útil para responder a los retos de las empresas y de la sociedad. Los retos de personas como tú.

En 45 años de historia, hemos conseguido ser pioneros en aplicar la robótica y la inteligencia artificial a la industria, colaborar con la NASA en mejorar sus experimentos en el espacio, aplicar con éxito tecnologías de inducción para mejorar las prestaciones de los aviones o desarrollar el primer tranvía sin catenaria y el primer sistema de almacenamiento de energía para parques fotovoltaicos del Estado.

Toda esta experiencia, junto a la capacidad de aplicación de la tecnología más innovadora, nos permite mejorar y facilitar tu vida, por ejemplo, desarrollando sistemas que consiguen que la energía que consumes sea cada vez más limpia, segura y económica o que el transporte que utilizas a diario sea más cómodo y sostenible. En definitiva, desarrollamos tecnología útil, que impacta en tu día a día y transforma nuestro futuro.

Trabajamos con las empresas líderes en retos que nos hacen crecer y desplegar nuestro mejor talento. Trabajamos en cooperación, en un entorno de aprendizaje continuo y superación y con un equipamiento singular. Y sobre todo disfrutamos creando la tecnología que transformará el futuro.

Si crees en el poder transformador de la tecnología y quieres ser protagonista en los retos tecnológicos del futuro, **IKERLAN es tu lugar.**