# CRIPTOGRAFÍA LIGERA APLICADA A IOT

El objetivo de este trabajo es poner en valor algunos de los algoritmos de criptografía ligera que existen en la actualidad y cómo su uso puede solventar muchos de los problemas de seguridad que normalmente acarrean muchos de los dispositivos IoT que utilizamos en nuestro día a día.

Los dispositivos IoT son cada vez una parte más importante de nuestra vida diaria, y muchos de ellos realizan funciones tan básicas que en muchos casos las empresas no se preocupan por protegerlos correctamente.

Es por esto que, en los últimos años, han tenido lugar una serie de sucesos derivados de estas fallas de seguridad que han llevado a puntos tan serios como poder atacar a un vehículo a través de un ataque de fuerza bruta que permite manejar incluso la dirección y los frenos de este mismo.

En el trabajo se tratan algunos de estos eventos, así como se explican varios de los algoritmos de criptografía ligera más relevantes en la actualidad y cómo su correcta implementación puede servirnos para proteger estos dispositivos y hacerlos más seguros sin tener que renunciar al rendimiento y la velocidad que se espera de estos dispositivos.

También se ha desarrollado una aplicación web llamada LightCipher, que puede utilizarse tanto de forma online como desplegada en una instancia local, y que nos permite utilizar algunos de estos algoritmos con todas sus variaciones posibles para cifrar y descifrar cadenas de texto.

Esta herramienta está programada en Java, usando el framework Spring, e incluye funciones de cifrado y descifrado para las familias de algoritmos de criptografía ligera Simon y Speck. Está basada en las implementaciones de dichos algoritmos y sus variantes realizadas en el proyecto SAWScript. LightCipher es accesible de forma online en <http://lightcipher2022.herokuapp.com>, y su código se encuentra subido a GitHub en <https://github.com/joscarboz/lightCipher>

En resumen, en este trabajo se trata de concienciar sobre los problemas de seguridad que suelen ir de la mano con muchos de los dispositivos IoT que utilizamos en nuestra vida cotidiana, así como explicar por qué ocurren estos problemas, y las formas en las que la comunidad de expertos en ciberseguridad están desarrollando nuevos algoritmos, englobados dentro del paradigma de criptografía ligera, que permitan asegurar la seguridad de estos dispositivos, teniendo en cuenta que sus procesadores necesitan ser rápidos para ser útiles y al mismo tiempo, para mantener sus costes bajos, deben funcionar en procesadores con poca potencia.

El objetivo de la aplicación desarrollada para este TFM ha sido, sobre todo, crear una primera herramienta con la que poder probar el funcionamiento de algunos de estos algoritmos mediante una interfaz gráfica y darlos a conocer, demostrando que ya existen soluciones para muchos de los problemas de seguridad de los dispositivos IoT. Así como animar a conocerlos y a implementarlos en futuros dispositivos y herramientas tanto a nivel doméstico como industrial. Ya que, actualmente, es muy difícil encontrar herramientas que implementen algoritmos de criptografía ligera.