FACULTAD DE CIENCIAS

DEPARTAMENTO DE...

PHD THESIS:

EL TÍTULO DE LA TESIS ES MUY IMPORTANTE, ASÍ QUE, NO OLVIDES PONER UNO QUE SEA INTERESANTE Y ADECUADO PARA TU TESIS

A Thesis submitted by Amy Wong for the degree of Doctor of Philosophy
in the Mars University

Supervised by:
Hubert J. Farnsworth

Índice general

Índice de figuras

1 Resumen

Hace décadas comunicarse mediante un dispositivo que estuviera conectado a una red cableada y tras mucha espera resultaba algo fantástico. Hoy en día tenemos la posibilidad de realizar un gesto en cualquier lugar y ponernos en contacto con alguien a cientos o miles de kilómetros. En este sentido, las comunicaciones han evolucionado de una forma increíble. La seguridad en estas comunicaciones basada en la criptografía es un elemento primordial para salvaguardar la privacidad de los usuarios y la del contenido.

La criptografía no se ha quedado atrás y durante el último siglo su devenir ha seguido el mismo camino. Desde los métodos más primitivos basados en cambiar una letra por la anexa; hasta complejos sistemas criptológicos (criptosistemas) que aprovechan ciertas propiedades matemáticas para preservar niveles de seguridad elevados con la necesidad de menos recursos (computacionales y de almacenamiento). Optimizar los recursos es esencial para ser competitivo y para ello la metodología de criptografía basada en curvas elípticas reduce exponencialmente la cantidad de almacenamiento necesaria respecto a otros algoritmos. De la mano va la tecnología NFC (*Near Field Comunication*), la cual ha simplificado los dispositivos de comunicación a algo tan pequeño y barato que ha conquistado el planeta en forma de multitud de aplicaciones.

En este Trabajo Fin de Grado (TFG a partir de ahora), comprenderemos la posibilidad de elaborar sistemas seguros con dispositivos de comunicación de bajo coste y criptología avanzada. A su vez, se implementará una aplicación para *smartphones* que, gracias a algorítmos avanzados de criptografía, permitirán a un usuario crear y utilizar un *tag* NFC como dispositivo de autenticación de alta seguridad en un sistema ficticio.

2
Abstract

Hace décadas comunicarse mediante un dispositivo que estuviera conectado a una red cableada y tras mucha espera resultaba algo fantástico. Hoy en día tenemos la posibilidad de realizar un gesto en cualquier lugar y ponernos en contacto con alguien a cientos o miles de kilómetros. En este sentido, las comunicaciones han evolucionado de una forma increíble. La seguridad en estas comunicaciones basada en la criptografía es un elemento primordial para salvaguardar la privacidad de los usuarios y la del contenido.

La criptografía no se ha quedado atrás y durante el último siglo su devenir ha seguido el mismo camino. Desde los métodos más primitivos basados en cambiar una letra por la anexa; hasta complejos sistemas criptológicos (criptosistemas) que aprovechan ciertas propiedades matemáticas para preservar niveles de seguridad elevados con la necesidad de menos recursos (computacionales y de almacenamiento). Optimizar los recursos es esencial para ser competitivo y para ello la metodología de criptografía basada en curvas elípticas reduce exponencialmente la cantidad de almacenamiento necesaria respecto a otros algoritmos. De la mano va la tecnología NFC (*Near Field Comunication*), la cual ha simplificado los dispositivos de comunicación a algo tan pequeño y barato que ha conquistado el planeta en forma de multitud de aplicaciones.

En este Trabajo Fin de Grado (TFG a partir de ahora), comprenderemos la posibilidad de elaborar sistemas seguros con dispositivos de comunicación de bajo coste y criptología avanzada. A su vez, se implementará una aplicación para *smartphones* que, gracias a algorítmos avanzados de criptografía, permitirán a un usuario crear y utilizar un *tag* NFC como dispositivo de autenticación de alta seguridad en un sistema ficticio.

3
Introducción

Cuando una persona envía un mensaje a un destinatario con información que considera comprometida o personal, pretende realizarlo con el mínimo riesgo de que dicho mensaje llegue de forma alterada y que sea al destinatario indicado. Además, éste quiere que el canal sea seguro y que nadie más intercepte la información; y si ocurriese tal caso, que personas ajenas no sean capaces de interpretar el mensaje y usarlo en su contra de forma perjudicial -o simplemente no desea difundir la información a alguien que no sea el destinatario-. También es evidente la necesidad de sistemas que eviten de la mejor forma posible la suplantación de usuarios; apoyándose en la criptografía, la autentificación resulta indespensable.

Existe la consideración generalizada que aquellos elementos más seguros a la hora de identificar y autenticar a un usuario de un sistema son aquellos que implican el uso de parámetros biométricos. Por ejemplo, el algoritmo para el reconocimiento del iris patentado por el investigador de la universidad de Cambridge, John Daugman, se basa en el iris como elemento único e intransferible para cada persona[**??**]. De forma análoga se utilizan algoritmos basados en la estructura facial o huellas dactilares. Por otra parte, Manuel Lucena López, doctor en informática de la universidad de Jaén, asegura en su publicación [**??**] que esta clase de 'requerimientos biométricos' se pueden reducir a problemas de autenticación basada en dispositivos. Es decir, una tarjeta puede actuar con el mismo compromiso de seguridad que dichos elementos biológicos.

Al igual, en los sistemas criptográficos (criptosistemas), la implementación más segura suele ser la menos eficiente. En la actualidad, la competencia hace de la optimización un objetivo en el que se invierten millones de capital. En el campo de la automoción competitiva, un incremento de la velocidad punta de 3km/h puede implicar reducir el tiempo de un competidor en unas décimas vitales que podrían suponer la diferencia entre ser primero o ser segundo. Dentro de la criptología y la seguridad de comunicaciones también está afectado por este hecho y no está exento de la voracidad por optimizar el trinomio de recursos, tiempo y resultados. Dentro de este contexto la tecnología tan asequible co-

mo NFC (‘Near Field Comunication‘), - dispositivos para la comunicación de información empleando radiofrecuencia de corto alcance- que ha conquistado numerosos ámbitos, será el soporte de estudio de este ‘Trabajo de Fin de Grado‘ (TFG a partir de ahora) como dispositivo de autenticación.

Como suele ser habitual, un dispositivo ‘barato‘ tiene ciertas desventajas. Respecto a la seguridad criptográfica con NFC el mayor inconveniente suele ser el tamaño de almacenamiento - inferior a 500 bits generalmente-. Este problema implica utilizar criptosistemas que puedan trabajar con tamaños reducidos de información sin comprometer la seguridad. La evolución en la criptografía es considerable desde que en la Segunda Guerra Mundial el proyecto ULTRA tratara de descifrar los mensajes del ejército alemán; quienes se encontraban a la vanguardia de la criptografía.

Bibliografía

[1] Manuel José Lucena. Criptografía y seguridad en computadores. *versión 0.7*, 5, 1999.

[2] Mohamad Ramli, Nurul Akmar, Muhammad Saufi Kamarudin, and Ariffuddin Joret. Iris recognition for personal identification. 2008.