UNIVERSIDAD
DE GRANADA

Facultad de Ciencias y Escuela Técnica Superior de Ingenierías
Informática y de Telecomunicación

Doble Grado en Ingeniería Informática y Matemáticas

TRABAJO DE FIN DE GRADO

Criptosistemas basados en el problema de la mochila

Presentado por:
Juan Manuel Mateos Pérez

Tutores:
Gabriel Navarro Garulo
Departamento de Ciencias de la Computación e Inteligencia Artificial

Francisco Javier Lobillo Borrero
Departamento de Álgebra

Curso académico 2022-2023

Criptosistemas basados en el problema de la mochila

Juan Manuel Mateos Pérez

Juan Manuel Mateos Pérez *Criptosistemas basados en el problema de la mochila*.

Trabajo de fin de Grado. Curso académico 2022-2023.

Responsables de tutorización

Gabriel Navarro Garulo
Departamento de Ciencias de la Computación e Inteligencia Artificial

Francisco Javier Lobillo Borrero
Departamento de Álgebra

Doble Grado en Ingeniería Informática y Matemáticas

Facultad de Ciencias y Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación

Universidad de Granada

Declaración de originalidad

D. Juan Manuel Mateos Pérez

Declara explícitamente que el trabajo presentado como Trabajo de Fin de Grado (TFG), correspondiente al curso académico 2022-2023, es original, en el sentido de que no ha utilizado para la elaboración del trabajo fuentes sin citarlas debidamente.

En Granada a 18 de julio de 2023

Fdo: Juan Manuel Mateos Pérez

Dedicatoria (opcional)
Tito Pepe
Ver archivo `preliminares/dedicatoria.tex`

Índice general

Agradecimientos

Agradecimientos del libro (opcional, ver archivo `preliminares/agradecimiento.tex`).

Summary

Summary en preliminares/summary.tex

Introducción

Introducción en preliminares/introduccion.tex

1 Criptografía Básica

1.1. Introducción

La criptografía es una disciplina que se ocupa de la seguridad de la información en la comunicación a través de canales inseguros. Desde la antigüedad, la criptografía ha sido utilizada para mantener la privacidad y la confidencialidad en la comunicación de mensajes importantes. Hoy en día, la criptografía se ha convertido en una herramienta crucial para proteger los datos sensibles en sistemas informáticos y en la comunicación en línea.

En este capítulo, se abordarán algunos conceptos fundamentales de la criptografía moderna, incluyendo los sistemas criptográficos simétricos y asimétricos, la criptografía en grupos, la criptográfica visual y los algoritmos de cifrado y descifrado tales como AES o RSA. [vzG15]

El objetivo de este capítulo es proporcionar al lector una comprensión básica de la criptografía moderna y cómo se aplica en la protección de la información en los sistemas informáticos, para que así pueda entender sin dificultades todo lo explicado en los siguientes capítulos.

La principal tarea que tiene la criptografía es la trasmisión segura de información. Siguiendo la tradición, se suele explicar que un usuario A, denominado Alice, quiere enviar un mensaje secreto a un destinatario B, llamado Bob. En este escenario, también se encuentra Eva, que quiere enterarse del mensaje secreto que envía Alice, y estará atenta al canal de comunicación que utilicen Alice y Bob, para interceptar todos sus mensajes.

Para conseguir esto, Alice tendrá que encriptar su mensaje x con una clave K y enviarle a Bob el resultado $y = enc_K(x)$. Por tanto, luego Bob deberá desencriptar el mensaje encriptado y con su propia clave S, para obtener el mensaje original $x = dec_S(y)$.

Obviamente surgen diversas dudas ante esta situación, tales como : ¿Cómo puede hacerle llegar Alice a Bob la clave necesaria para desencriptar el mensaje? ¿Qué métodos son "mejores" para encriptar el mensaje? O en el peor de los casos, ¿qué pasaría si Eva averigua la clave que están usando?

Volviendo al escenario planteado, está claro que, a priori, nos da igual que Eva consiga el mensaje encriptado, siempre y cuando no sea capaz de desencriptarlo. Por tanto, Alice debería utilizar una función que no sea fácil de desencriptar, ya que su mensaje sería vulnerable. Llamamos a esta función, función unidireccional.

Definición 1.1. [vzG15]
Una función unidireccional es una función f tal que $f(x) = y$ fácil de computar, pero que dado y, imagen de x, debe ser dificil encontrar x tal que $f(x) = y$. En caso de que no sea así, se denominará función trampilla.

Ejemplo 1.2. [vzG15]
Sea $x = (p, q)$ con p y q primos tal que $p < q$ y $f(x) = p \cdot q$.
Es fácil multiplicar ambos números primos para obtener un valor N, pero es muy dificil, a nivel computacional, obtener los primos p y q a partir del valor N. De hecho, no se conoce ninguna función trampilla para esta f. Ésta es la función unidireccional utilizada en el algoritmo RSA, que se explicará más adelante.

En realidad, que Eva "rompa el sistema", no tiene que significar necesariamente que sea capaz de descifrar el mensaje de manera completa. Podría simplemente encargarse de desencriptar una pequeña parte, o incluso palabras clave, como podrían ser "bomba" o "Mastercard".

Obviamente, debe ser inviable poder recuperar tanto el mensaje x, como la clave de Bob S, a partir del mensaje y

1.2. Advanced Encryption Standard (AES)

1.3. Problema de la mochila

2 Criptosistema de Merkle-Hellman

2.1. Introducción

En el vasto mundo de la criptografía, el criptosistema de Merkle-Hellman ha destacado como una de las joyas más brillantes del campo de la seguridad informática. Desarrollado en la década de 1970 por Ralph Merkle y Martin Hellman, este sistema de clave pública basado en el problema de la mochila, ha capturado la imaginación de investigadores y entusiastas de la seguridad durante décadas debido a su simplicidad y su robustez frente a diversos ataques.

En este capítulo, nos adentraremos en el fascinante universo del criptosistema de Merkle-Hellman, desentrañando sus principios fundamentales y descubriendo cómo su ingenioso diseño permite el cifrado y descifrado de mensajes de manera segura. Desde los conceptos básicos hasta las complejidades más sutiles, acompañaremos a nuestros lectores en un viaje enriquecedor para comprender la esencia y el potencial de este criptosistema.

Comenzaremos por sentar las bases con una explicación clara y concisa de los conceptos clave que sustentan el criptosistema Merkle-Hellman. Posteriormente, nos sumergiremos en el algoritmo de generación de claves, donde veremos cómo se forja el candado y la llave que garantizará la confidencialidad de nuestros mensajes. A continuación, exploraremos el proceso de cifrado paso a paso, descubriendo cómo una secuencia aparentemente aleatoria de números transforma nuestros mensajes en datos ilegibles para los ojos no autorizados.

Sin embargo, nuestro viaje no se detendrá allí. Con la misma dedicación, abordaremos las vulnerabilidades y limitaciones que el criptosistema Merkle-Hellman presenta, garantizando una visión completa y realista de sus capacidades. Al comprender las posibles debilidades, podremos apreciar los escenarios en los que este sistema brilla y aquellos en los que es necesario considerar otras alternativas, destacando y explicando por supuesto, algunos de los ataques más importantes a este criptosistema, como el ataque de Shamir o el de Brikell.

A medida que desentrañamos los misterios del criptosistema de Merkle-Hellman, su relevancia en el panorama actual de la ciberseguridad se volverá evidente. Este capítulo aspira a convertirse en una guía esclarecedora para todos aquellos que buscan comprender y aplicar esta poderosa herramienta criptográfica en la protección de información confidencial y en la preservación de la privacidad en un mundo cada vez más interconectado.

Así que, comencemos nuestro viaje hacia el corazón del criptosistema de Merkle-Hellman y descubramos juntos los secretos que hacen de esta creación un logro más que notable en el campo de la criptografía moderna.

3 Otros criptosistemas

Capítulo en capitulos/capitulo3.tex

4 Apéndice

Apendice en capitulos/apendice.tex Aquí irá el código de los programas realizados

Conclusiones

Conclusiones en capitulos/conclusiones.tex

Bibliografía

Las referencias se listan por orden alfabético. Aquellas referencias con más de un autor están ordenadas de acuerdo con el primer autor.

[vzG15] Joachim von zur Gathen. *CryptoSchool*. Springer, 2015. [Citado en págs. 17 and 18]