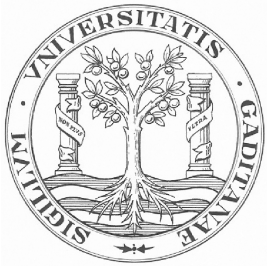

UNIVERSIDAD DE CÁDIZ

FACULTAD DE CIENCIAS

GRADO EN MATEMÁTICAS

CRIPTOGRAFÍA POSCUÁNTICA

Trabajo de fin de grado presentado por

Juan Antonio Guitarte Fernández

Tutor: Dr. Nombre apellidos del tutor

Firma del alumno Firma del tutor

Puerto Real, Cádiz, Julio de 2.020

Abstract

Five years ago, a first volume of open problems in Mathematical Systems and Control Theory appeared.

Some of the 53 problems that were published in this volume attracted considerable attention in the research community. The book in front of you contains a new collection of 63 open problems. The contents of both volumes show the evolution of the field in the half decade since the publication of the first volume. One noticeable feature is the shift toward a wider class of questions and more emphasis on issues driven by physical modeling.

Early versions of some of the problems in this book have been presented at the Open Problem sessions of the Oberwolfach Tagung on Regelungstheorie, on February 27, 2002, and of the Conference on Mathematical Theory of Networks and Systems (MTNS) in Notre Dame, Indiana, on August 12, 2002. The editors thank the organizers of these meetings for their willingness to provide the problems this welcome exposure. Since the appearance of the first volume, open problems have continued to meet with large interest in the mathematical community. Undoubtedly, the most spectacular event in this arena was the announcement by the Clay Mathematics Institute of the Millennium Prize Problems whose solution will be rewarded by one million U.S. dollars each. Modesty and modesty of means have prevented the editors of the present volume from offering similar rewards toward the solution of the problems in this book. However, we trust that, notwithstanding this absence of a financial incentive, the intellectual challenge will stimulate many readers to attack the problems. The editors thank in the first place the researchers who have submitted the problems. We are also very thankful to the Princeton University Press, and in particular Vickie Kearn, for their willingness to publish this vol- ume. The full text of the problems, together with comments, additions,

and solutions, will be posted on the book website at Princeton Univer- sity Press (link available from `http://pup.princeton.edu/math/`) and on `http://www.inma.ucl.ac.be/?blondel/op/`.

Readers are encouraged to submit contributions by following the instructions given on these websites.

The editors, Louvain-la-Neuve, March 15, 2003.

A mis padres.

Resumen

Se ha creado e investigado un modelo de interacción entre un fabricante y el estado donde el fabricante produce un solo producto y el estado controla el nivel de contaminación. Se considera una economía local con un problema de contaminación almacenada, que debe escoger entre inversiones en producción y medio ambiente (funciones de control). El modelo es descrito por un sistema de dos ecuaciones diferenciales con dos controles acotados. La mejor estrategia de control se encuentra analíticamente usando el Principio del Máximo de Pontryagin y el Teorema de Green.

En este trabajo analizamos algunos aspectos de la Teoría de Control que incluyen consideraciones sobre sus orígenes, sus motivaciones y su evolución. Describimos algunos elementos matemáticos fundamentales y diversos avances que se caracterizan a la vez por su interés científico y su transcendencia desde un punto de vista social, tecnológico e industrial. También, mencionamos algunos de los retos que se plantean en esta disciplina para un futuro inmediato.

Hay dos divisiones principales de la teoría de control, es decir, clásicos y modernos, que tienen implicaciones directas sobre las aplicaciones de ingeniería de control. La teoría desarrollada para el control de procesos, desde el punto clásico y moderno tiene su base esencial en el conocimiento de la dinámica del proceso que se desea controlar.Desde la teoría clásica de control, considerando el caso más sencillo de un sistema lineal de una entrada y una salida (SISO) del diseño del sistema. Estadinámica normalmente se expresa asiendo uso de ecuaciones diferenciales ordinarias, y en el caso de sistemas lineales, usando de igual manera la transformada de Laplace para obtener así de una representación matemática que relaciona la señal que se quiere controlar y la señal de

entrada al sistemas.Un controlador diseñado por la teoría clásica por lo general requiere en ellugar de sintonía debido a las aproximaciones de diseño. Los controladores diseñado con la teoría de control clásica comunes son los CONTROLADORESPID.En contraste, la teoría de control moderna se lleva acabo estrictamente enel complejo-s o el dominio de la frecuencia y puede lidiar con múltiples entradas y múltiples salidas (MIMO) de sistemas. Esto para diseño sofisticado, como el control de aviones de combate etc.,. En el diseño moderno, un sistema representa como un conjunto de primer orden ecuaciones diferenciales. El área de control moderno tiene muchas áreas que explorar. Lo cual se detallara en este trabajo.

Agradecimientos

Por mi excelencia y formación profesional, gracias a su cariño, guía y apoyo. Este presente simboliza mi gratitud por toda la responsabilidad e inestimable ayuda que siempre me han proporcionado. Porque gracias a su apoyo y consejos, he llegado a realizar una de mis grandes metas lo cual constituye la herencia más valiosa que piduera recibir.

Con un testimonio de eterno agradecimiento por el apoyo moral que desde siempre me brindaron y con el cual he logrado terminar mi carrera profesional, que es para mi la mejor de las herencias. Gracias por ayudarme cada día a cruzar con firmeza el camino de la superación, por que con su apoyo y aliento hoy he logrado uno de mis más grandes anhelos.

Por el cariño y apoyo moral que siempre he recibido de ustedes y con el cual he logrado culminar mi esfuerzo, terminando así mi carrera profesional, que es para mi la mejor de las herencias.

Al término de esta etapa de mi vida, quiero expresar un profundo agradecimiento a quienes con su ayuda, apoyo y compresión me alentaron a lograr esta hermosa realidad. Como un testimonio de eterno agradecimiento por el gran amor y la confianza que siempre me brindaron, gracias por darme la fuerza para irme superando. Sabiendo que jamás encontraré la forma de agradecer su constante apoyo y confianza, sólo espero que comprendan que mis ideales, esfuerzos y logros han sido también suyos e inspirados en ustedes. Por que gracias a su cariño, apoyo y confianza he llegado a realizar dos de mis más grandes metas en la vida. La culminación de mi carrera profesional y el hacerlos sentirse orgullosos de esta persona que tanto los ama.

A quien jamás encontraré la forma de agradecer el que me haya brindado su mano en las derrotas y logros de mi vida, haciendo de este triunfo más suyo que mío por la forma en la que guió mi vida con amor y energía.

Agradezco de todo corazón a dios y a mis padres por que a través de ellos me concedió la vida en este mundo, así como a mis abuelos, tíos, hermanos, suegros, esposa e hijos y a todas las personas que directa o indirectamente han tenido a bien ayudarme en forma moral y económica para mi formación como ser humano y profesional, en respuesta a esto, cuenten con un gran amigo.

A quien jamás encontraré la forma de agradecer su apoyo, comprensión y confianza esperando que comprendas que mis logros son también tuyos e inspirados en tí, hago de este un triunfo y quiero compartirlo por siempre contigo.

A quienes jamás encontraré la forma de agradecer el cariño, comprensión y apoyo brindado en los momentos buenos y malos de mi vida, hago este triunfo compartido, sólo esperando que comprendan que mis ideales y esfuerzos son inspirados en cada uno de ustedes.

Sabiendo que no existirá forma alguna de agradecer una vida de sacrificios, esfuerzos y amor, quiero que sientan que el objetivo alcanzado también es de ustedes y que la fuerza que me ayudo a conseguirlos fue su gran apoyo.

A dios que me ha heredado el tesoro más valioso que puede dársele a un hijo ”sus padres”. A mis padres quienes sin escatimar esfuerzo alguno sacrificaron gran parte de su vida para educarme. A mis hermanos quienes la ilusión de su vida ha sido verme convertido en un hombre de provecho. Y a todas aquellas personas que comparten conmigo este triunfo.

Con la mayor gratitud por los esfuezos realizados para que yo lograra terminar mi carrera profesional siendo para mi la mejor herencia. A mi madre que es el ser más maravilloso de todo el mundo. Gracias por el apoyo moral, tu cariño y comprensión que desde niño me has brindado, por guiar mi camino y estar junto a mi en los momentos más difíciles. A mi padre porque desde pequeño ha sido para mi un gran hombre maravilloso al que siempre he admirado. Gracias por guiar mi vida con energía, esto ha hecho que sea lo que soy.

Con amor, admiración y respeto.

Pepito Pérez

febrero 2020

Índice general

Hay a quien le gusta comenzar cada capítulo con una cita...

Mulachenski

CAPITULO

1

Introduction

CAPITULO

2

Planteamiento y motivación

2.1 El problema de los ordenadores cuánticos

Hoy día, la criptografía está más presente que nunca en nuestro día a día: hacer compras por Internet, navegar por casi cualquier página web, chatear a través del teléfono móvil... Gracias a la criptografía, podemos mantener nuestras comunicaciones privadas y asegurarnos de que cualquier pago que realicemos o documento que publiquemos sólo podemos hacerlo nosotros, es decir, que nadie pueda falsificarlo.

El continuo desarrollo de los ordenadores cuánticos, que romperán los principales algoritmos de firma digital y criptosistemas de clave pública usados hoy en día (por ejemplo, *RSA*, *DSA* y *ECDSA*), puede hacer pensar que cuando la computación cuántica sea una realidad, la criptografía quedará obsoleta, que será imposible modificar información para que sea incomprensible o infalsificable por atacantes y personas no autorizadas; y que por tanto, la única forma de proteger nuestras comunicaciones y nuestros datos será aislarlos físicamente de ellos, por ejemplo, con dispositivos USB cerrados bajo llave en un maletín. Pero, ¿hasta qué punto es esto cierto?

Un estudio más detallado de los algoritmos criptográficos existentes muestra, sin embargo, que existen muchos otros criptosistemas más allá del *RSA*, *DSA* y *ECDSA*:

- **Criptografía basada en funciones hash**. El ejemplo más destacado dentro de este grupo es el sistema de firma con clave pública basado en árboles hash de Merkle

(en inglés, *Merkle's hash-tree public-key signature system*) de 1979, basado en un sistema de firma digital de un solo uso de Lamport y Diffie.

- **Criptografía basada en códigos**. El ejemplo clásico es el sistema de encriptación de clave pública con códigos Goppa ocultos de McEliece (1978).

- **Criptografía basada en retículos**. El ejemplo que más interés ha conseguido atraer, aunque no es el primero propuesto históricamente, esl el sistema de encriptación de clave pública "NTRU" de Hoffstein-Pipher-Silverman (1998).

- **Criptografía de ecuaciones cuadráticas de varias variables**. Uno de los ejemplos más interesantes es el sistema de firma con clave pública "HFE^{v-}" de Patarin (1996), que generaliza una propuesta de Matsumoto e Imai.

- **Criptografía de clave secreta**. El ejemplo más conocido (y usado actualmente) es el cifrado "Rijndael" de Daemen-Rijmen (1998), renombrado como "AES", siglas que significan Estándar de Encriptación Avanzada (Advanced Encryption Standard).

Se cree que todos estos sistemas son resistentes a los ordenadores clásicos y cuánticos, es decir, que no existe un algoritmo eficiente que pueda ser implementado en un ordenador clásico o cuántico que rompa estos sistemas. El algoritmo de Shor (el cual analizaremos más adelante en este trabajo), que permite resolver de manera eficiente el problema de la factorización de números enteros en ordenadores cuánticos (y por tanto rompe los sistemas de criptografía clásica como el *RSA*), no ha podido ser aplicado a ninguno de estos sistemas. Aunque existen otros algoritmos cuánticos, como el algoritmo de Grover, que pueden ser aplicados a algunos de estos sistemas, no son tan eficientes como el algoritmo de Shor y los criptógrafos pueden compensarlo eligiendo claves un poco más grandes.

Hay que notar que esto no implica que estos sistemas sean totalmente seguros. Este es un problema muy común en criptografía: algunas veces se encuentran ataques a sistemas que son devastadores, demostrando que un sistema es inútil para la criptografía; otras veces, se encuentran ataques que no son tan devastadores pero que obligan a elegir claves más grandes para que sigan siendo seguros; y otras, se estudian criptosistemas durante años sin encontrar ningún ataque efectivo. En este punto, la comunidad puede ganar confianza en el sistema creyendo que el mejor ataque posible ya ha sido encontrado, o que existe muy poco margen de mejora.

2.2 Criptosistemas y sistemas de firma

El objetivo principal de la criptografía es permitir que dos personas, normalmente referidas como Alice y Bob, puedan comunicarse entre ellas a través de un canal inseguro de tal manera que una tercera persona, Oscar, no pueda entender qué están diciendo entre ellos, aun teniendo acceso a toda la conversación. La información que Alice quiere enviar a Bob la denominamos "texto plano", aunque no tiene que ser necesariamente texto; puede tener la estructura que deseemos: datos numéricos, cadenas de bits, sonido... Alice encripta el texto plano usando una "clave" que solo conocen Alice y Bob, obteniendo así un "texto encriptado". Oscar, al ver la información a través del canal inseguro, no puede determinar cuál era el texto plano original; pero Bob, que sí conoce la clave, puede desencriptar el texto cifrado y recuperar el texto plano.

Formalmente, un criptosistema se define de la siguiente manera:

Definición 2.1. Un *criptosistema* es una 5-tupla $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ que satisface las siguientes condiciones:

1. $\mathcal{P}$ es un conjunto finito de *textos planos* posibles,
2. $\mathcal{C}$ es un conjunto finito de *textos cifrados* posibles,
3. $\mathcal{K}$ es el conjunto finito de todas las claves posibles,
4. Para cada $K \in \mathcal{K}$, existen dos aplicaciones $e_K : \mathcal{P} \to \mathcal{C}$ y $d_K : \mathcal{C} \to \mathcal{P}$, denominadas *regla de encriptación* y *regla de desencriptación* respectivamente, que verifican que $d_K(e_K(x)) = x$ para todo $x \in \mathcal{P}$.

La propiedad 4, que es la más importante, asegura que conociendo la clave $K \in \mathcal{K}$, se puede recuperar el texto sin cifrar original usando la función d_K. El proceso por el cual Alice y Bob utilizarían un criptosistema es el siguiente:

1. Alice y Bob seleccionan una misma clave $K \in \mathcal{K}$ de forma aleatoria.
2. Supongamos que Alice quiere enviar un mensaje $x = x_1 x_2 \cdots x_n$, con $x_i \in \mathcal{P}$ para todo $1 \leq i \leq n$. Alice calcula, para cada $1 \leq i \leq n$, $y_i = e_K(x_i)$, resultando en el mensaje cifrado

   $$y = y_1 y_2 \cdots y_n$$

   que Alice envía a través del canal inseguro a Bob.

3. Bob, al recibir y, calcula usando la clave K que conoce $d_K(y_i)$, que coincidirán con los x_i originales por la propiedad 4 de la Definición 2.1, obteniendo así el texto original x.

Hay que notar que para que este método funcione, Alice y Bob deben escoger la misma clave K para encriptar y desencriptar los mensajes. En algunos criptosistemas (como el AES mencionado anteriormente), sabiendo e_K o d_K, es sencillo obtener la otra función porque se conoce la clave secreta K. Un criptosistema de este tipo se denomina *criptosistema de clave simétrica*, ya que si un atacante obtuviese la función e_K o d_K, podría romper el sistema desencriptando los mensajes cifrados, bien usando d_K directamente en el segundo caso o bien calculando d_K a partir de e_K a través de la clave en el primero.

Por tanto, es fundamental que Alice y Bob, antes de iniciar cualquier comunicación a través del canal inseguro, se pongan de acuerdo a través de un canal seguro en la clave que van a utilizar. En la práctica, esto es muy difícil de conseguir (por ejemplo, en el caso de Internet). Para resolver este problema, existen los *criptosistemas de clave pública*.

La idea tras estos criptosistemas es que dada una función de encriptación e_K, sea computacionalmente infactible calcular d_K. En este caso, el receptor del mensaje, Bob, publicaría una *clave pública* que permitiría a cualquier persona determinar una función de encriptación e_K. Así, Alice encriptaría el mensaje que quiere enviar usando esta función. El mensaje cifrado llegaría entonces a Bob, que es el único que conoce su *clave privada* con la cual puede calcular la función de desencriptación d_K correspondiente a e_K, desencriptando así el mensaje.

Estos criptosistemas son los que se ven principalmente afectados por la aparición de los ordenadores cuánticos: mientras que en un ordenador clásico puede ser muy difícil calcular la clave privada a partir de la clave pública, pueden existir algoritmos cuánticos que resuelvan el problema en un tiempo razonable. Es por ello que se necesitan nuevos sistemas en los que no existan algoritmos conocidos, ni clásicos ni cuánticos, que permitan calcular eficientemente d_K a partir de e_K.

Definición 2.2. Un *sistema de firma* es una 5-tupla $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ que verifica:

1. $\mathcal{P}$ es un conjunto finito de posibles *mensajes*,
2. $\mathcal{A}$ es un conjunto finito de *firmas* posibles,
3. $\mathcal{K}$ es el conjunto de las claves posibles,

4. Para cada $K \in \mathcal{K}$, hay dos aplicaciones $sig_K \in S$ y $ver_K \in V$, denominadas algoritmos de *firma* y *verificación* respectivamente, siendo $sig_K : \mathcal{P} \to \mathcal{A}$ y $ver_K : \mathcal{P} \times \mathcal{A} \to \{0, 1\}$, que verifican para cada mensaje $x \in \mathcal{P}$ y cada firma $y \in \mathcal{A}$:

$$ver_K(x, y) = \begin{cases} 1 & \text{si } y = sig_K(x) \\ 0 & \text{si } y \neq sig_K(x) \end{cases}$$

A un par ordenado de la forma $(x, y) \in \mathcal{P} \times \mathcal{A}$ se le denomina *mensaje firmado*.

CAPITULO

3

Preliminares

3.1 Lo que vimos

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut ultrices egestas nunc, venenatis rhoncus elit fermentum non. Pellentesque gravida nulla vitae ipsum lobortis ullamcorper. Ut adipiscing, tellus in egestas mattis, enim metus pretium erat, ac tempor dolor neque placerat nulla. Nullam nec ligula eu ipsum pharetra semper a in magna. Integer ut tortor quis nisi fringilla euismod eu ac ipsum. Pellentesque sodales consectetur erat eget rutrum. Proin ornare dolor ut arcu aliquet vestibulum. Pellentesque laoreet tincidunt sem eget semper.

Integer interdum mattis magna ullamcorper tristique. Nullam commodo nulla eget ipsum vulputate tincidunt auctor leo aliquet. Fusce euismod sagittis ante, eu vulputate eros dictum at. Cras non euismod nunc. Nullam velit diam, consectetur sed eleifend vitae, blandit at arcu. Maecenas ut urna nec turpis lobortis commodo. Aliquam aliquet turpis id massa viverra id sollicitudin est cursus. Sed a tortor non mauris cursus imperdiet.

Integer fermentum rutrum urna at vestibulum. Vivamus ullamcorper erat in sapien dignissim pellentesque. Integer convallis fringilla dictum. In bibendum lectus eu nulla pretium volutpat. Morbi hendrerit fringilla tortor, sed gravida neque lacinia a. In risus magna, hendrerit vitae cursus ac, vehicula at eros. Aenean quis ipsum sit amet leo vestibulum cursus.

3.2 Otra que no vimos

Cras placerat mattis dui quis vehicula. Nulla sit amet metus nibh, at auctor enim. Quisque congue ultricies sapien in suscipit. Fusce vitae placerat ante. Praesent aliquet urna ac elit consequat nec mattis augue faucibus. Nunc et sapien vel felis mollis sodales. Aenean molestie nulla vestibulum nisi fringilla vel euismod dolor tristique. Aenean fermentum, dolor eget tincidunt faucibus, risus lorem feugiat elit, sagittis malesuada eros ligula in odio. Pellentesque ac libero lobortis justo bibendum laoreet. Cras egestas lorem eget ligula dignissim sollicitudin. Vestibulum sit amet augue ultrices erat faucibus vestibulum. Aenean tincidunt faucibus leo, nec auctor diam bibendum a. Sed varius, mauris in pellentesque scelerisque, nisl ligula viverra erat, in eleifend tellus enim ac magna. Pellentesque quis est risus. Cras mollis feugiat auctor. Proin ac eros vitae nulla gravida varius.

3.2.1 Otra cosita

Morbi at augue sapien. Duis tempus quam vitae velit interdum ultricies. Vivamus laoreet lacinia elit sit amet vehicula. Ut congue diam ac magna hendrerit sed fermentum justo lacinia. Curabitur vel odio neque, quis consequat mi. Proin lobortis justo quis enim fermentum accumsan sagittis ipsum imperdiet. Proin sem felis, laoreet placerat egestas id, fringilla id mauris. Pellentesque a nisi sit amet leo consectetur gravida nec et dui. Curabitur quis hendrerit augue. Etiam sed dui nec tortor convallis fringilla. Proin tempor mattis diam nec egestas. Quisque condimentum elementum lacus ac porta. Vivamus congue, odio eu ullamcorper elementum, leo turpis tempus sem, at condimentum dolor quam eu nunc. Pellentesque eget risus ac velit aliquam sollicitudin sed et ipsum.

CAPITULO

4

Primera cosa

4.1 Lo primero

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut ultrices egestas nunc, venenatis rhoncus elit fermentum non. Pellentesque gravida nulla vitae ipsum lobortis ullamcorper. Ut adipiscing, tellus in egestas mattis, enim metus pretium erat, ac tempor dolor neque placerat nulla. Nullam nec ligula eu ipsum pharetra semper a in magna. Integer ut tortor quis nisi fringilla euismod eu ac ipsum. Pellentesque sodales consectetur erat eget rutrum. Proin ornare dolor ut arcu aliquet vestibulum. Pellentesque laoreet tincidunt sem eget semper.

Integer interdum mattis magna ullamcorper tristique. Nullam commodo nulla eget ipsum vulputate tincidunt auctor leo aliquet. Fusce euismod sagittis ante, eu vulputate eros dictum at. Cras non euismod nunc. Nullam velit diam, consectetur sed eleifend vitae, blandit at arcu. Maecenas ut urna nec turpis lobortis commodo. Aliquam aliquet turpis id massa viverra id sollicitudin est cursus. Sed a tortor non mauris cursus imperdiet.

Integer fermentum rutrum urna at vestibulum. Vivamus ullamcorper erat in sapien dignissim pellentesque. Integer convallis fringilla dictum. In bibendum lectus eu nulla pretium volutpat. Morbi hendrerit fringilla tortor, sed gravida neque lacinia a. In risus magna, hendrerit vitae cursus ac, vehicula at eros. Aenean quis ipsum sit amet leo vestibulum cursus.

4.2 Lo segundo

Cras placerat mattis dui quis vehicula. Nulla sit amet metus nibh, at auctor enim. Quisque congue ultricies sapien in suscipit. Fusce vitae placerat ante. Praesent aliquet urna ac elit consequat nec mattis augue faucibus. Nunc et sapien vel felis mollis sodales. Aenean molestie nulla vestibulum nisi fringilla vel euismod dolor tristique. Aenean fermentum, dolor eget tincidunt faucibus, risus lorem feugiat elit, sagittis malesuada eros ligula in odio. Pellentesque ac libero lobortis justo bibendum laoreet. Cras egestas lorem eget ligula dignissim sollicitudin. Vestibulum sit amet augue ultrices erat faucibus vestibulum. Aenean tincidunt faucibus leo, nec auctor diam bibendum a. Sed varius, mauris in pellentesque scelerisque, nisl ligula viverra erat, in eleifend tellus enim ac magna. Pellentesque quis est risus. Cras mollis feugiat auctor. Proin ac eros vitae nulla gravida varius.

4.2.1 Lo que va con lo segundo

Morbi at augue sapien. Duis tempus quam vitae velit interdum ultricies. Vivamus laoreet lacinia elit sit amet vehicula. Ut congue diam ac magna hendrerit sed fermentum justo lacinia. Curabitur vel odio neque, quis consequat mi. Proin lobortis justo quis enim fermentum accumsan sagittis ipsum imperdiet. Proin sem felis, laoreet placerat egestas id, fringilla id mauris. Pellentesque a nisi sit amet leo consectetur gravida nec et dui. Curabitur quis hendrerit augue. Etiam sed dui nec tortor convallis fringilla. Proin tempor mattis diam nec egestas. Quisque condimentum elementum lacus ac porta. Vivamus congue, odio eu ullamcorper elementum, leo turpis tempus sem, at condimentum dolor quam eu nunc. Pellentesque eget risus ac velit aliquam sollicitudin sed et ipsum.

CAPITULO

5

Segunda cosa

5.1 Lo siguiente

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut ultrices egestas nunc, venenatis rhoncus elit fermentum non. Pellentesque gravida nulla vitae ipsum lobortis ullamcorper. Ut adipiscing, tellus in egestas mattis, enim metus pretium erat, ac tempor dolor neque placerat nulla. Nullam nec ligula eu ipsum pharetra semper a in magna. Integer ut tortor quis nisi fringilla euismod eu ac ipsum. Pellentesque sodales consectetur erat eget rutrum. Proin ornare dolor ut arcu aliquet vestibulum. Pellentesque laoreet tincidunt sem eget semper.

Integer interdum mattis magna ullamcorper tristique. Nullam commodo nulla eget ipsum vulputate tincidunt auctor leo aliquet. Fusce euismod sagittis ante, eu vulputate eros dictum at. Cras non euismod nunc. Nullam velit diam, consectetur sed eleifend vitae, blandit at arcu. Maecenas ut urna nec turpis lobortis commodo. Aliquam aliquet turpis id massa viverra id sollicitudin est cursus. Sed a tortor non mauris cursus imperdiet.

Integer fermentum rutrum urna at vestibulum. Vivamus ullamcorper erat in sapien dignissim pellentesque. Integer convallis fringilla dictum. In bibendum lectus eu nulla pretium volutpat. Morbi hendrerit fringilla tortor, sed gravida neque lacinia a. In risus magna, hendrerit vitae cursus ac, vehicula at eros. Aenean quis ipsum sit amet leo vestibulum cursus.

5.2 Otra cosa más

Cras placerat mattis dui quis vehicula. Nulla sit amet metus nibh, at auctor enim. Quisque congue ultricies sapien in suscipit. Fusce vitae placerat ante. Praesent aliquet urna ac elit consequat nec mattis augue faucibus. Nunc et sapien vel felis mollis sodales. Aenean molestie nulla vestibulum nisi fringilla vel euismod dolor tristique. Aenean fermentum, dolor eget tincidunt faucibus, risus lorem feugiat elit, sagittis malesuada eros ligula in odio. Pellentesque ac libero lobortis justo bibendum laoreet. Cras egestas lorem eget ligula dignissim sollicitudin. Vestibulum sit amet augue ultrices erat faucibus vestibulum. Aenean tincidunt faucibus leo, nec auctor diam bibendum a. Sed varius, mauris in pellentesque scelerisque, nisl ligula viverra erat, in eleifend tellus enim ac magna. Pellentesque quis est risus. Cras mollis feugiat auctor. Proin ac eros vitae nulla gravida varius.

5.2.1 Una subcosa

Morbi at augue sapien. Duis tempus quam vitae velit interdum ultricies. Vivamus laoreet lacinia elit sit amet vehicula. Ut congue diam ac magna hendrerit sed fermentum justo lacinia. Curabitur vel odio neque, quis consequat mi. Proin lobortis justo quis enim fermentum accumsan sagittis ipsum imperdiet. Proin sem felis, laoreet placerat egestas id, fringilla id mauris. Pellentesque a nisi sit amet leo consectetur gravida nec et dui. Curabitur quis hendrerit augue. Etiam sed dui nec tortor convallis fringilla. Proin tempor mattis diam nec egestas. Quisque condimentum elementum lacus ac porta. Vivamus congue, odio eu ullamcorper elementum, leo turpis tempus sem, at condimentum dolor quam eu nunc. Pellentesque eget risus ac velit aliquam sollicitudin sed et ipsum.

Bibliografía

[1] A.M. Turing. Computing machinery and intelligence. *Mind*, 59(236):433–460, 1950.

[2] Stuart Bennett. *A history of control engineering, 1800-1930*. IET, 1986.

[3] Benjamin Graham and David Dodd. *Security Analysis*. McGraw-Hill, 1934.