
COMPILANDO CONOCIMIENTO

Criptografía y Seguridad

MATEMÁTICAS &
CIENCIAS DE LA COMPUTACIÓN

Oscar Andrés Rosas Hernandez

Agosto 2019

Índice general

I	Introducción	3
1.	Introducción	4
1.1.	Llaves	5
II	Clásica	6
2.	Ideas generales	7
3.	Historia	8
3.1.	Porque es importante cifrar la información	9
3.2.	Cifrado y Mary	10
3.3.	La piedra Rosetta	11
3.4.	Enigma Sueco	12
3.5.	Maquina Purpura	13
3.6.	Grandes personajes	14
3.6.1.	Alan Turing	14
3.6.2.	Claude Shannon	16
4.	Sustitución	18
4.1.	Cifrado Cesar y de corrimiento	19
4.2.	Cifrado Affine	20
4.3.	Cifrado Vigenère	21
5.	Transposicion	22

6. Cripto analisis	23
6.1. Analisis de Frecuencias	24
 III Moderna	 25
7. De llave privada o simétrica	26
7.1. Flujos	27
7.2. Bloques	28
 8. De llave pública o asimétrica	 29

Parte I

Introducción

Capítulo 1

Introducción

“ Es el estudio de técnicas matemáticas, algoritmos, protocolos y sistemas relacionadas con aspectos de la seguridad de la información como confidencialidad, autenticación, integridad, disponibilidad de los datos.

Trata tanto los recursos como técnicas y herramientas que ayudan a proveer seguridad de la información. ” - Menezes & Vanstone

El nombre criptografía viene de una palabra griega, donde criptos era ocultar y grafos que era escribir.

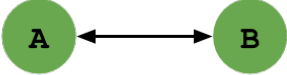
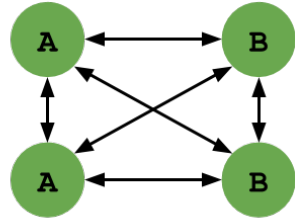
Lo mas importante que tenemos que saber es tenemos 4 servicios que vamos a ofrecer:

- Disponibilidad: Que nos permitirá impedir que se interrumpan las comunicaciones.
- Confidencialidad: Que nos permitirá asegurarnos que nuestro mensaje no pueda ser entendido por un tercero.
- Integridad: Que nos permitirá asegurarnos que nuestro mensaje no ha sido modificado.
- Autenticación: Que nos permitirá asegurarnos que nuestro mensaje fue creado por la persona que esperamos y no fue fabricado.

Es importante también definir a la criptología, que es el estudio de los criptosistemas, es decir sistemas que ofrecen medios seguros de comunicación, en los que el emisor oculta o cifra el mensaje antes de transmitirlo para que solo un receptor autorizado pueda recuperarlo.

1.1. Llaves

Supongamos que tenemos llaves simétricas, es decir, la llave para cifrar y para descifrar son la misma entonces podemos ver la siguiente tabla que nos muestra como crece la cantidad de llaves con respecto a los conexiones que tenemos:

Conexiones	Llaves
	1
	6

Ahora si queremos ser mas general es que:

$$llaves_para_n_conexiones(n) = \frac{n(n-1)}{2}$$

Por ejemplo para $n = 30$, osea si hay 30 nodos tenemos que:

$$llaves_para_n_conexiones(30) = \frac{30(29)}{2} = 435$$

Parte II

Clásica

Capítulo 2

Ideas generales

- En general, el alfabeto cifrado esta en minusculas y el alfabeto cifrado esta en mayuscula

Capítulo 3

Historia

3.1. Porque es importante cifrar la información

En general ciframos mensajes porque queremos que estos no caigan en las manos del enemigo, además para proteger el mensaje de tal manera que solo ciertos sectores de la población tuvieran acceso a estos.

En la mañana del sábado 15 de octubre de 1586, la reina María entró en la concurrida sala del tribunal en el castillo de Fotheringhay.

3.2. Cifrado y Mary

Mary Queen of Scots fue juzgada por traición. Había sido acusada de conspirar para asesinar a la reina Isabel con el fin de llevarse la corona inglesa. Sir Francis Walsingham, secretario principal de Elizabeth, ya había arrestado a los otros conspiradores, extrajo confesiones y las ejecutó. Ahora planeaba probar que Mary estaba en el corazón de la trama y, por lo tanto, era igualmente culpable e igualmente merecedora de muerte.

3.3. La piedra Rosetta

Encontrada en la época de Napoleon, durante sus campañas por Egipto, cuando la descubrieron se dieron cuenta que tenia un mensaje escrito en 3 lenguas diferentes, usando el griego, que era conocido para poder descifrar los jeroglíficos.

Esto se realizo en 1820 por Jean Francois.

3.4. Enigma Sueco

El creador fue Boris Hagelin en Suecia, Estocolmo, era una alternativa a la maquina enigma, era considera mas segura, aunque en el fondo no lo era.

Tambien se creo una version (C-35) que podia caber en un bolsillo.

3.5. Maquina Purpura

Fue creada por Japon, y fue apodada por los descrifradores como la maquina purpura. Fue descrifra por los estadounidenses en un par de meses, de hecho lograron hacer una maquina que automatica descifrara mensaje.

3.6. Grandes personajes

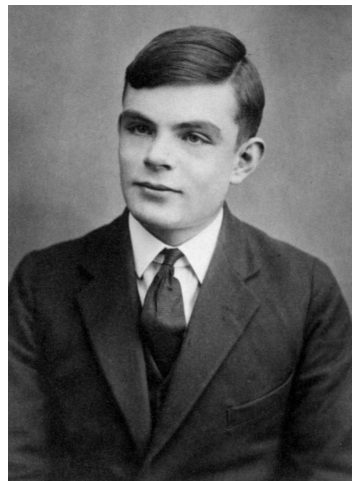
3.6.1. Alan Turing

Alan Turing fue concebido en Chatrapur, India, y nació el 23 de junio de 1912 en Londres, mientras sus padres pasaban una temporada de descanso en su tierra natal.

Cuando tenía solo un año de edad, sus padres regresaron a la India por unos años más, y a él y a su hermano mayor los dejaron al cuidado de un coronel del ejército retirado y su esposa para que los criaran en una ciudad costera del sur de Inglaterra.

En su último año en Sherborne, Turing obtuvo una beca para asistir al King's College de Cambridge, en el que ingresó en 1931 para cursar estudios de matemáticas.

...En un congreso celebrado en 1928, Hilbert planteó tres preguntas fundamentales válidas para cualquier sistema formal de matemáticas:



- ¿Era su conjunto de reglas completo, de modo que cualquier enunciado pudiera demostrarse (o refutarse) utilizando solo las reglas del propio sistema?
- ¿Era coherente, de modo que ningún enunciado pudiera demostrarse verdadero y a la vez falso?
- ¿Existía algún procedimiento que pudiera determinar si un enunciado concreto era demostrable, en lugar de permitir la posibilidad de que algunos enunciados (como les ocurría a problemas muy famosos, como el teorema de Fermat, la conjetura de Goldbach o de Collatz)?

Hilbert pensaba que la respuesta a las dos primeras preguntas era que sí, por lo que no tenía mucho sentido hacerse la tercera.

Cuando el gran profesor de matemáticas de Cambridge Max Newman le enseñó a Turing las preguntas de Hilbert, el expresó el Entscheidungsproblem del siguiente modo: ¿Existe algún proceso mecánico que se pueda utilizar para determinar si un enunciado lógico concreto es demostrable?

A Turing le gustó el concepto de proceso mecánico. En 1937 Alan Turing publicaba “Sobre los números computables”, en el que describe un computador universal, resolviendo la tercera pregunta de Hilbert.

En su intento de identificar preguntas indecidibles, el artículo de Turing describió una máquina imaginaria que fue diseñada para realizar una operación matemática o algoritmo particular.

En otras palabras, la máquina sería capaz de ejecutar una serie de pasos fijos y prescritos que, por ejemplo, multiplicarían dos números.

Turing preveía que los números que se multiplicarían podrían introducirse en la máquina a través de una cinta de papel, como la cinta perforada que se utiliza para alimentar una melodía en un piano antiguo. La respuesta a la multiplicación se emitirá a través de otra cinta. Turing imaginó una serie completa de estas llamadas máquinas de Turing, cada una especialmente diseñada para abordar una tarea en particular, como dividir, cuadrar o factorizar.

Luego dio el siguiente paso. Se imaginó una máquina cuyo funcionamiento interno podría ser alterado para que pudiera realizar todas las funciones de todas las máquinas de Turing concebibles. Las modificaciones se realizarían insertando cintas cuidadosamente seleccionadas, que transformaron la máquina flexible individual en una máquina divisoria, una máquina multiplicadora o cualquier otro tipo de máquina. Turing llamó a este dispositivo hipotético una máquina universal de Turing porque sería capaz de responder cualquier pregunta que pudiera ser respondida lógicamente.

En otras palabras Turing pensó: “No necesitamos una infinita variedad de máquinas distintas que realicen tareas diferentes. Bastará con una sola.

Del problema técnico de crear máquinas distintas para diversas tareas se pasa a la labor administrativa de “programar” la máquina universal para llevar a cabo esas tareas”

La carrera académica de Turing se detuvo abruptamente unos años más tarde cuando gracias al “Government Code and Cypher School” fue invitado a convertirse en criptoanalista en Bletchley, justo el 4 de septiembre de 1939, el día después de que Neville Chamberlain declarara la guerra a Alemania.

Turing comenzó a trabajar en la decodificación de la máquina The Enigma, un dispositivo de cifrado desarrollado y utilizado a principios y mediados del siglo XX utilizado por la Alemania nazi para proteger la comunicación comercial, diplomática y militar.

Turing se centró en lo que sucedería si el ejército alemán cambiara su sistema de intercambio de claves de mensajes.

Los primeros éxitos de Bletchley se basaron en el trabajo de Rejewski, que explotó el hecho de que los operadores de Enigma cifraron cada clave de mensaje dos veces (por ejemplo, si la clave de mensaje era YGB, el operador cifraría YGBYGB). Se suponía que esta repetición aseguraría que el receptor no cometiera un error, pero creó una brecha en la seguridad de Enigma.

Los criptoanalistas británicos adivinaron que no pasaría mucho tiempo antes de que los alemanes se dieran cuenta de que la clave repetida estaba comprometiendo a Enigma,

en cuyo punto se les pediría a los operadores de Enigma que abandonaran la repetición, confundiendo así las técnicas actuales de descifrado de códigos de Bletchley. (Simon Singh, *The Code Book Book*, Chapter 4: Enigma)

Era el trabajo de Turing encontrar una forma alternativa de atacar a Enigma, una que no dependiera de una clave repetida.

Esta sería la semilla de una máquina electromecánica llamada bombe (que le tomo un par de semanas), que podría romper Enigma de manera más efectiva que la bomba kryptologiczna polaca.

Se ha argumentado, aunque de forma controvertida, que los logros de Bletchley Park fueron el factor decisivo en la victoria de los aliados.

Lo que es seguro es gracias a los trabajos de Bletchley se acortó significativamente la guerra.

Esto se hace evidente al pensar en la situación en la Batalla del Atlántico y especular sobre lo que podría haber sucedido sin el beneficio de Ultra.

Para empezar, se habrían perdido más barcos y suministros para la flota dominante de submarinos, lo que habría comprometido el vínculo vital con Estados Unidos y forzado a los Aliados a desviar mano de obra y recursos en la construcción de nuevos barcos.

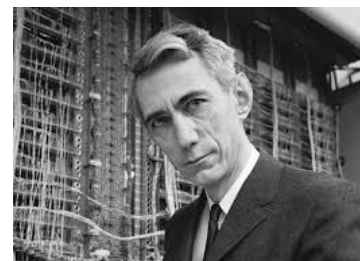
Los historiadores han estimado que esto habría retrasado los planes aliados en varios meses, lo que habría significado posponer la invasión del Día D hasta al menos el año siguiente.

Según Sir Harry Hinsley, “la guerra, en lugar de terminar en 1945, habría terminado en 1948 si el Reino Unido no hubieran podido leer los cifrados Enigma y producir Ultra”

(Walter Isaacson. *Innovadores (Innovators-SP)*).

3.6.2. Claude Shannon

En 1937 se produjo otro avance teórico trascendental, similar al de Turing en cuanto que se trataba puramente de un experimento mental. Era el trabajo de un estudiante de posgrado del MIT llamado Claude Shannon, que aquel año se convirtió en la tesis de máster más influyente de todos los tiempos, un artículo que *Scientific American* calificaría más tarde como: la Carta Magna de la era de la información.



Shannon creció en una pequeña población de Michigan, donde construyó maquetas de aviones y aparatos de radioaficionado; luego cursó estudios especializados de ingeniería eléctrica y matemáticas en la Universidad de Michigan.

Si la teoría de la información y la comunicación fueran tan emocionantes como la computación y la inteligencia artificial, tal vez Claude Shannon sería tan famoso como Alan Turing.

De hecho, al considerar la totalidad del trabajo de Shannon, puede que no sea una exageración decir que fue el padre de la era de la información en la que nos encontramos hoy.

Shannon es mejor conocido por introducir el concepto de entropía como una medida de información.

Esta idea fue introducida por primera vez por Shannon en un informe clasificado escrito para Bell Laboratories en 1945 titulado Una teoría matemática de la criptografía. El informe fue desclasificado y publicado en el Bell System Technical Journal en 1949 bajo el título de Communication Theory of Secrecy Systems, un año después de que Shannon publicara su artículo A Mathematical Theory of Communication.

Había una dualidad entre Shannon y Turing y su trabajo de criptografía en los tiempos de guerra.

Mientras Turing estaba en Bletchley Park decodificando mensajes interceptados de los alemanes, proporcionando a Churchill información invaluable, Shannon estaba en Bell Laboratories trabajando en el Sistema X, un teléfono utilizado por Churchill y Roosevelt para conducir conferencias transoceánicas.

Shannon estaba trabajando en ocultar información por un lado mientras intentaba transmitirla por otro lado, y tuvo la idea de su teoría de la comunicación mientras trabajaba en el esquema de cifrado para el Sistema X.

“Se dio cuenta de que, así como los códigos digitales podían proteger la información de miradas indiscretas, también podían protegerla de los estragos de la interferencia estática u otras formas de interferencia”. (Horgan, 1992, p. 74).

Al trabajar en su documento de criptografía de 1945, Shannon se dio cuenta de que los códigos digitales podrían diseñarse para empaquetar información no solo de manera más eficiente (de modo que se pudiera transmitir más información a través de un canal dado), sino que también podrían diseñarse para hacerlos irrompibles. (Shannon, 1949)

Mientras que en la criptografía desea proteger un mensaje de espías, en la información desea proteger un mensaje de errores de transmisión. En ambos campos se necesita una medida de información y se trabaja con métodos de codificación y decodificación

Resultó que ambos implicaban lo mismo, la entropía, que se convertiría en la pieza clave de la teoría de la información de Shannon.

Cuando Von Neumann murió, dejando su volumen “The Computer and the Brain” sin terminar solo había dos nombres mencionados en todo el libro: Alan Turing y Claude Shannon.

Capítulo 4

Sustitución

Es tomar cada caracter del alfabeto y transformarlo en otro diferente, cada caracter siempre va a parar al mismo caracter.

4.1. Cifrado Cesar y de corrimiento

Creado por el famoso general griego Cesar, el método es hacer un corrimiento del alfabeto, por ejemplo con un $k = 3$, entonces $A \rightarrow D$ ó $B \rightarrow E$.

Otra versión del cifrado tomaba el alfabeto griego y lo transformaba por el romano.

La fórmula general es:

$$e(x) = x + k \mod 26$$

4.2. Cifrado Affine

Es parecido al de corrimiento, se puede escribir como:

$$\begin{aligned}e(p) &= \alpha p + \beta \\d(c) &= \alpha^{-1}(p - \beta)\end{aligned}$$

4.3. Cifrado Vigenène

Es un cifrado de sustitución polialfabetico, porque una misma letra en el mensaje en texto plano sera mandado a diferentes letras dependiendo de su posicion en el mensaje original.

Su fórmula general:

$$E_k(M_i) = (M_i + K_i) \mod L$$

$$D_k(C_i) = (C_i - K_i) \mod L$$

- Primero que nada, escribe el mensaje en texto plano
- Se usa una llave que se escribe tantas veces como sea necesario
- Se busca en la tabla

Capítulo 5

Transposicion

Capítulo 6

Cripto análisis

6.1. Analisis de Frecuencias

No es loco pensar que la letra que mas aparece en un mensaje cifrado sera la letra mas comun del alfabeto original.

Parte III

Moderna

Capítulo 7

De llave privada o simétrica

7.1. Flujos

7.2. Bloques

Capítulo 8

De llave pública o asimétrica

Bibliografía

- [1] Nidia A. Cortez-Duarte, *Cryptography 2019*.
- [2] Walter Isaacson. “Innovadores (Innovators-SP).”