

Tema 0: Introducción Asignatura

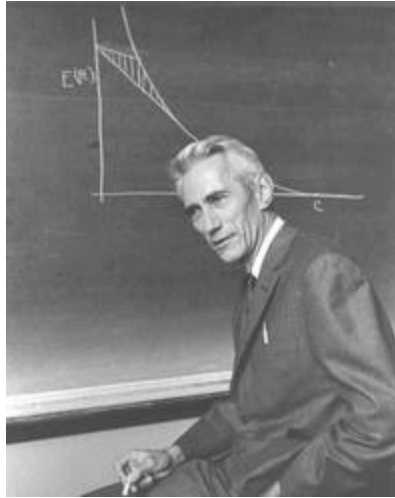
José A. Montenegro Montes

Dpcho 3.2.40 – 952 13 28 98

monte@lcc.uma.es

Teoría de la Información y Codificación
2013 / 2014

Comienzos



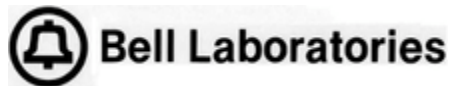
Claude Elwood Shannon

(30 de abril de 1916 - 24 de febrero de 2001)

Ingeniero Electrónico y Matemático

A mathematical theory of communication.

Bell System Technical Journal, vol. 27, pp.
379-423 and 623-656, July and October,
1948



Lucent Technologies
Bell Labs Innovations



- Transistor,
- Teoría de la Información,
- UNIX, C y C++.
- 7 Premios Nobel

•

•

•

Temario

1. Introducción.

2. Compresión Datos

3. Corrección Errores

4. Criptografía

Planning Semestre 13/14

- Septiembre / Octubre 18 Horas
- Noviembre 16 Horas
- Diciembre 10 Horas
- Enero 10 Horas

54 HORAS

Planning Semestre Detallado I

octubre 2013

Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14 Apertura oficial del curso 2013/14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

18 HORAS

1

Introducción

2

Compresión Datos

Planning Semestre Detallado I

noviembre 2013

Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

16 HORAS

3

Corrección Errores

Planning Semestre Detallado I

diciembre 2013

Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

10 HORAS

3

Corrección Errores

Planning Semestre Detallado I

enero 2014

Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

10 HORAS

3 **Criptografía**

¿Qué es Teoría Codificación?

- Un “mix” de matemáticas, informática, telecomunicaciones
 - **Algebra Lineal**
 - **Algebra Abstracta (grupos, anillos, cuerpos)**
 - **Probabilidad y Estadística**
 - Señales y Sistemas
 - **Cuestiones relativas a la Implementación**
 - *Cuestiones relativas a la Optimización*
 - *Cuestiones relativas al Rendimiento*

Compresión Datos

Compresión Datos

- **Compresión reduce el tamaño de un archivo:**
 - ahorra TIEMPO cuando transmite.
 - ahorra ESPACIO cuando almacena.
- **Ejemplos:**
 - **Compresión Archivos:** (sin pérdida)
 - Files: GZIP, PKZIP.....
 - Sistema Ficheros: NTFS.
 - **Multimedia.** (pérdida)
 - Imagen: GIF, JPEG....
 - Sonido: MP3.
 - Video: MPEG, DivX™, HDTV.
 - **Comunicación.**
 - ITU-T T4 Group 3 Fax.
 - V.42bis modem.
 - **Base de Datos**

Compresión Datos

- Básicamente se basa en que la mayoría de la información posee redundancia.
 - ¿Qué ocurriría con archivos con caracteres aleatorios?

Fclkkacifobjofmkgdcoiicnfmcpjfccabckjamolnihkbgobcjbngjiceeelpfgcjiihppenefllhglfemdengahlbpigggmlmnefnhjelmgjn
cjcidlhkgllhcninidmmgnobkeglpnadanfbecoonbiehglmpnhkkamdffpacjmgojmcaabpcjcecpfbgamlidceklhfkkmiojldnoaagih
eiapaimlcnljnjggpeanbmojgkccogpmkmoifioeikefjidbadgdcepnhdpfjaeeapdjeofklpdegghidbgcaiemajllhndigeihbeibifemacf
adknhlbgincpmimdogimgeomgeljfgklkdgnhafonpjbmlkapddhmepdnckeajebmeknmeejnmenbmnnfefdhhpmigbbjknjm
obimamjjaaaffhlhiggajlbaijnebidpaeigdgoghcihodnlhahllhhojdfacnhadhgkfahmeaebccacgeojgikcoapknlomfignanedmajnl
ompjoaifiaejbcjcdibpkofcbmjiobbpdhfilfajkhfmppcngdneeinpnfafaeadbhifechinknpdnplamackphekokigpddmmjnbngklhib
ohdfeaggmclllmdhafklmdimdbplggbbejckmhlkjocjjlcngckfpfakmnpiaanfddjdlleiniilaenbnikgfnjfcophbgkhdgmfpoeihfmkbpiai
gnphogbkelphobonmfghpdgmkfedkfkchceeldkcofaldinljcgafimaanelmfkokcjekefkbmegcgjifjcpjppnabldjoaafpbdafigcoibb
cmoffbbgigmngefpkmbhbghlbdjngenldhgnfbdldcmjdmoflhkogfjoldfjpaokepndejmnbiealkaofifejdkgedgdgbioacflfjafbaem
gpjlagbdgilhcfdcamhfmppfgojhplmhjegchgdppkkljpnphfcnganmbmnggpphncbieknjhilafkegboilajdppcodpeodddjfcpi
aloalfeomjbpkhmhnmdmcpkggeaohfmcnegmibjkajcdcpjcpjgminhhakihiachfepffnilcooiciepoapmdjniimfbolchikibkmhb
kgconimkdchahcnhapfdkiapikencegcjapjkfjlgdlmgncpbakhjidapblcdcgeekkjaohbnbigmhboengpmedliofoofdcphelapijce
gejgldcdfodikalehbccpbbscfakkblmoobmdgdkaafbbkjnidioikfakjclbchambcpaepfeinmenmpoodadoecbgbmfkkeabilaoeogggh
oekamaibhjibefmoppbhfbhffapjnodlofeihmjahmeipejlfhloefgmjhjnlomapjakhjhjpncomippeanbikkhekpcfgbgkmklipfbiiidkdc
bolofhelipbkbjmjfoemppcneaebklibmcaddlmjdcajpmhhaeedbbfpjafcnanlfcjmmbfncpdcodldhmnbdjmeajmboclkgojgh
lohlbhgjkhkmclohgjamfmcchkhmiadjghjehflcbklfifackbecgjoggbkhlcmfhipflhnmfipjmcoldbeghpcekhgmnahijpabnom
nokldjcpbbcpjgcfjofngmbdcpeeeiiclmmbmfjkhlanckidhmbanmlabncncpbbhoafajjicnfeenppoekmlddholnbdepfmmeoafedfl
mdcbaodgeahimcgpcammjljoebpfmgfhogfckgmomecdipmodbcempidfnlcggpgbfffoncajpncomalgoiieo.....

Corrección Errores

Corrección Errores

- Queremos enviar datos de un origen a otro...
 - Fuente: línea telefónica, cables de ethernet, canales de radio, canales de telefonía móvil, etc.
- O queremos escribir y después obtener la información...
 - Fuente: disco duros, CD-ROMs, DVDs, etc.
- ¡PERO! Los datos, o señales, pueden estar corruptos
 - Ruido en el canal, atenuación de la señal, interferencia, etc.

Corrección errores (Solución)

- Añadir redundancia controlada a los mensajes para comprobar si la emisión ha sido correcta y en caso negativo poder recuperar el mensaje original.
- Ejemplos.....

Número Identificación Fiscal



- $XY = x_1 x_2 \dots x_8 y_9$
- y_9 es un carácter de control de forma que
 $S = X \bmod 23$; $Y = \text{Tabla}[S]$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
T	R	W	A	G	M	Y	F	P	D	X	B	N	J	Z	S	Q	V	H	L	C	K	E

No se utilizan las letras: I, Ñ, O, U

La I y la O se evitan para evitar confusiones con los números 0 y 1

Utilizan **veintitrés letras** por ser éste un número primo.

Número Identificación Fiscal



- *Realizar en JAVA una clase NIF*
 - *Método verifique si NIF es válido*
 - *Método obtenga DNI y devuelva NIF*
 - *Método obtenga NIF incorrecto devuelva NIF válido*

```
public static final String NIF_Tabla = "TRWAGMYFPDXBNJZSQVHLCKE";

public static String nifFromDni(int dni) {
    return String.valueOf(dni) + NIF_Tabla.charAt(dni % 23);
}
```

Código ISBN



- $x_1 x_2 \dots x_{10}$
- x_{10} es un dígito de verificación

$$S = x_1 + 2x_2 + \dots + 9x_9 + 10x_{10} = 0 \pmod{11}$$

Ejemplo 0-13-088976-?

- Calcular $1(0) + 2(1) + 3(3) + 4(0) + 5(8) + 6(8) + 7(9) + 8(7) + 9(6) = 272$
- $272 + 10(?) = \text{múltiplo de } 11$
- Aritmética Modular nos muestra que el dígito es el 8!!

UPC

(Universal Product Code)



- $x_1 x_2 \dots x_{12}$
- x_{12} es un dígito de control tal que

$$S = 3x_1 + 1x_2 + \dots + 3x_{11} + 1x_{12} = 0 \pmod{10}$$

Criptografía

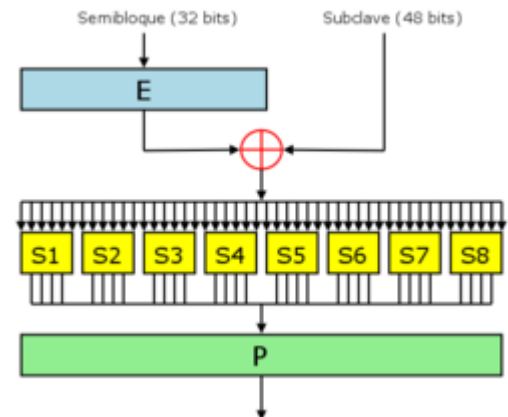
Criptografía

- Nace básicamente para asegurar la confidencialidad de la información.
- Primeros algoritmos tan antiguos como la humanidad:

Algoritmo Cesar:

- ABCDEFGHIJKLMNOPQRSTUVWXYZ y Clave = 3
- DEFGHIJKLMNOPQRSTUVWXYZABC

- Algoritmos Actuales basados en conceptos de Teoría de la Información



Sumario

- Desde Cesar a Clave Pública.... desde códigos repetición a Códigos to Reed-Solomon....
 - Aplicación matemáticas mas sofisticadas → mejor códigos
- Teoría de la Información hace uso de algebra, cuerpos finitos, anillos, grupos, probabilidad, algebra lineal, teoría de númerosy muchos campos de las matemáticas!

¿A quién afecta?

- ¡A todos!
 - Compras y comercio electrónico
 - Cajeros Automáticos y banca por internet
 - TV & Radio Satelite, TV Cable, lectores mpX, divx ...
- ¿A quien más?
 - RSA, Bell Labs, AT&T, NASA, Amazon, iTunes...

Metodología

Teorema

..... ENTROPIA

Prueba del Teorema

- $\sum \sum p(b_j | a_i) \log p'(a_i, b_j) =$
- $\sum \sum p(b_j | a_i) \log [p(a_i) p(b_j)] =$
- $\sum \sum p(b_j | a_i) \log p(a_i) + \sum \sum p(b_j | a_i) \log p(b_j) = - [H[A] + H[B]]$

Teorema

..... ENTROPIA

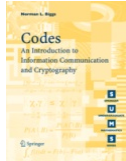
Aplicación programación (Clases, Métodos ... JAVA)



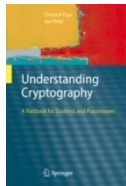
Método de Evaluación

- Evaluación
 - Práctica Obligatoria 40%
 - Tipo Test 10%.
 - Examen Final 60%
 - Realización Tareas Campus Virtual.
 - **Participación Clase**
 - **Asistencia Obligatoria**
- Evaluación Semestre:
17 Febrero 2014. 16:00 Horas – Aula 413
- Evaluación Septiembre:
15 Septiembre 2014. 16:00 Horas – Aula 302
- Laboratorios: Lunes 3.1.4 y Miércoles 3.1.7

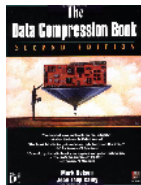
Bibliografía



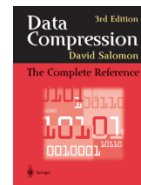
Codes: An Introduction to Information Communication and Cryptography
Biggs, Norman L.
Springer, 2008, X, 274 p.



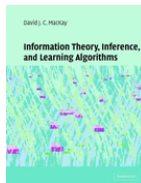
Understanding Cryptography. A Textbook for Students and Practitioners
Paar, Christof, Pelzl, Jan
Springer 2010



The Data Compression Book
Mark Nelson, Jean-Loup Gailly



Data compression.. The complete reference
Salomon D.
Springer, 3rd edition, 2004)



Information Theory, Inference, and Learning Algorithms
David J.C. MacKay
Cambridge University Press, 2003
<http://www.inference.phy.cam.ac.uk/mackay/itila/>

Bibliografía

- *J. Rifá, LL. Huguet. **Comunicación Digital**. Masson*
- *Teoría de la información y codificación*
Abramson, Norman
Madrid : Paraninfo, 1986
- *A first course in coding theory*
Hill, Raymond
Oxford : Clarendon Press, 2006
- *Error control coding : fundamentals and applications*
Shu Lin, Daniel J. Costello, Jr
Englewood Cliffs, N.J. ; London : Prentice-Hall, cop. 1983



José A. Montenegro Montes

Dpcho 3.2.40 – 952 13 28 98

monte@lcc.uma.es

Teoría de la Información y Codificación
2013 / 2014