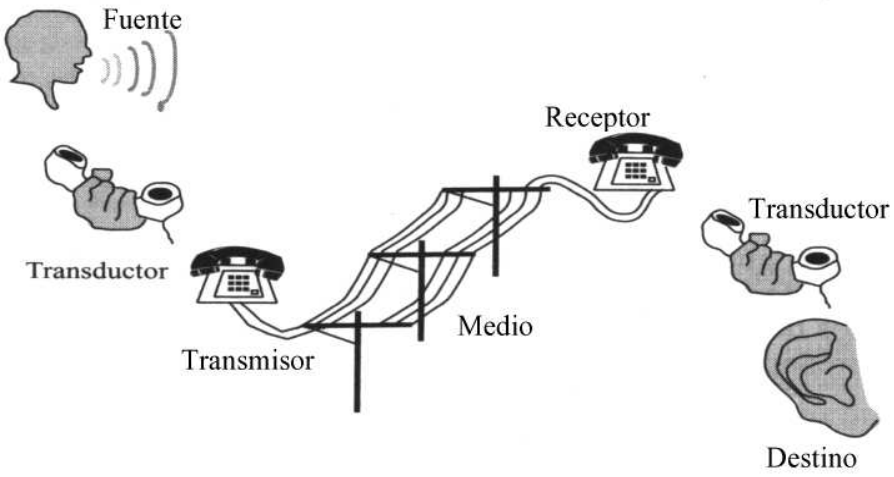
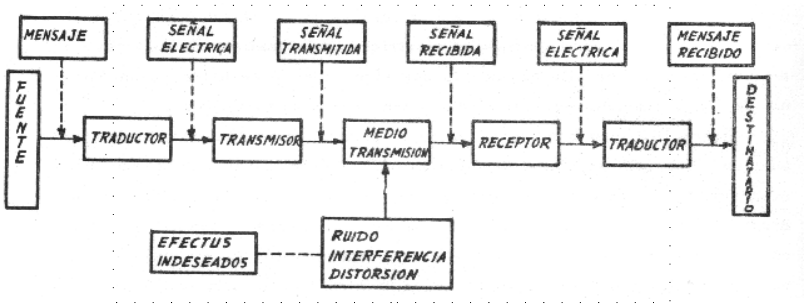
Ejemplo de comunicación



Concepto de comunicación



- **Comunicación** = transvase de <u>información</u> entre dos o más entes a través de un medio físico, mediante signos entendibles por todas las partes y siguiendo unos procedimientos establecidos por todas las partes
- Transductores -> conversión entre magnitudes físicas/electricas
- Transmisor -> adaptación de la señal al medio (modulación)
- Medio de transmisión -> transmisión de las señales eléctricas/ópticas
- Canal de comunicación = transmisor + medio + receptor
- Efectos indeseados -> pérdida de información

TELECOMUNICACIONES

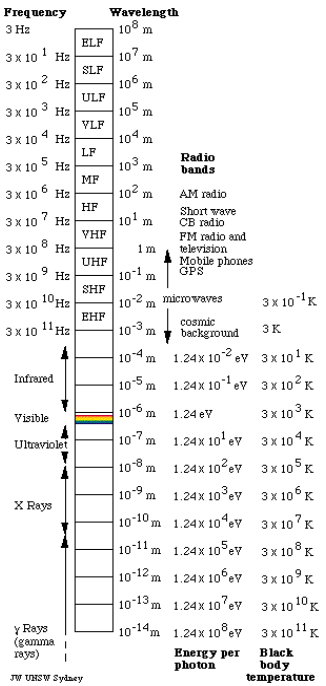
- 1835-1844 Samuel F. B. Morse: invención del telégrafo
- 1858 tendido del cable trasatlántico
- 1874 Emile Baudot: invención del telégrafo múltiple (varios mensajes simultáneos por la misma línea)
- 1876 Alexander Graham Bell: invención del teléfono.
- 1895 telégrafo sin hilos de Marconi (precursor) de las transmisiones por radio
- 1920 primera emisora de radio
- 1920 circuito superheterodino de Armstrong (precursor de la radio moderna)
- 1925 inicio de la televisión
- 1941 inicio de la radiodifusión comercial en FM
- 1946 inicio de la TV color
- 1950 primeros sistemas de telefonía por radio
- 1957 lanzamiento del Sputnik ruso
- 1971 aparición de la red ARPANET (Estados Unidos)
- 1972 aparición de la red IBERPAC (España)
- 1977 Primer sistema de fibra óptica para prestar servicios telefónicos
- 1982 inicio de la telefonía móvil en España
- 1995 inicio de la telefonía GSM en España
- 2001 inicio de la telefonía GPRS en España
- 2005 inicio de la telefonía UMTS

TELECOMUNICACIONES

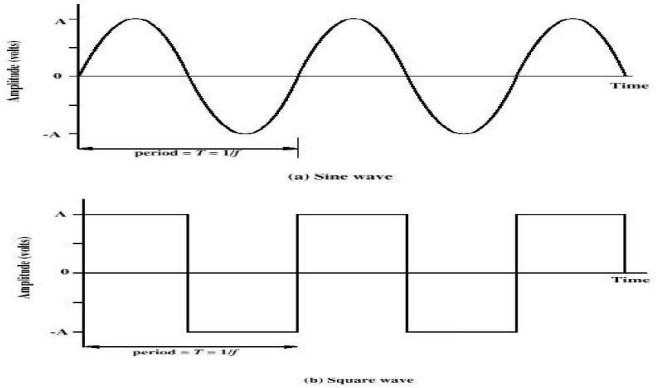
- Normalización
  - ITU (Unión internacional de Telecomunicaciones)
    - CCITT (Comité Consultivo Internacional de Teléfonos y Telégrafos)
    - CCIR (Comité Consultivo Internacional de Radiocomunicaciones)
  - ECMA (Asociación de Fabricantes Europeos de Ordenadores)
  - ANSI (American National Standards Institute)
  - EIA (Electronics Industries Asociation)
  - ISO (International Standards Organization)
  - IETF (Internet Engineering Task Force)
  - CEN (Comité Europeo para Estandarización)
  - IEEE (Instituto de Ingeniería Electrica y Electrónica)

Señales en la frecuencia

- **30 Hz – 300 Hz. Extremely Low Frecuency (ELF)** Radiaciones producidas por redes eléctricas.
- **300 Hz - 3 kHz. Ultra Low Frequency (ULF)**. Frecuencias de voz.
- **3 - 30 kHz. Very Low Frequency (VLF)**. Capacidad de transporte de información muy pequeña.
- **30 - 300 kHz. Low Frequency (LF)**. Ondas kilométricas. Propagación a lo largo del mundo mediante reflexión en la inonosfera y en la tierra.
- **300 kHz - 3 MHz. Medium Wave (MW)**. (Ondas hectométricas). Peor reflexión, pero aún así se propagan cientos de Km.
- **3 - 30 MHz. High Frequency (HF) o Short Wave (SW)**. Ondas decamétricas. Incluye Banda Ciudadana (CB) y radiocontrol. Mayor capacidad de transporte
- **30 - 300 MHz. Very High Frequency (VHF)**. Ondas métricas. Incluye FM y televisión. Antenas típicamente de ½ o ¼ de la longitud de onda. Transmisión sólo en línea recta. Gran atenuación por obstáculos
- **300 MHz - 3 GHz. Ultra High Frequency (UHF)**. Ondas decimétricas. Televisión y telefonía móvil. Gran capacidad de transporte de información.
- **3 - 30 GHz. Super High Frequency (SHF)**. Ondas centimétricas o microondas Comunicación por satélite. Muy alta capacidad de transporte. Altísima atenuación por obstáculos
- **30 - 300 GHz. Extra High Frequency (EHF)**. Ondas milimétricas. Poco usada por sus dificultades técnicas.



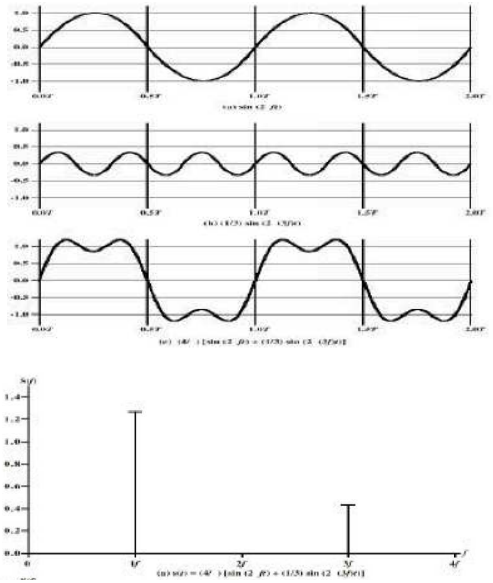
Características de las señales



- Señal -> variación de una magnitud física (tensión/corriente) en el tiempo
- Señales periódicas:
  - Periodo (T) = tiempo que tarda en completar un ciclo (segundos)
  - Frecuencia (f) = número de ciclos por segundo -> f = 1/T (Hz = Hertzios)
  - Fase -> posición relativa en el tiempo (grados o radianes)
  - Amplitud (A) -> valor máximo de la magnitud física (voltios, amperios)
  - Potencia (P) -> energía que transmite por unidad de tiempo (W = Watios)

Dualidad tiempo-frecuencia

- Señal sinusoidal = tono puro
- Señal compuesta -> formada por muchos tonos (Fourier)
- Espectro de la señal -> frecuencias contenidas en la señal y su amplitud
- Ancho de banda de la señal -> margen de frecuencias del espectro
- Señales con ancho de banda ilimitado -> ancho de banda efectivo = banda que contiene la mayor parte de la energía
- Componente continua (DC) = componente de frecuencia 0



- Ondas -> propagación de la señal en el espacio
  - Velocidad de propagación (v) -> depende del medio
  - Longitud de onda (λ) -> distancia entre dos dos puntos "en el mismo estado" $\lambda = T \bullet v$
- Señales continuas y discretas:
  - Continua -> puede tomar cualquier valor dentro de un rango (p.e.: números decimales: 1, 1,234, 1,566678, 2, 2,333333333)
  - Discretas -> sólo pueden tomar algunos valores fijados (p.e.: números enteros: 1, 2, 3, 4 .....)

tiempo\amplitud	Continua	Discreta
Continua	ANALÓGICA	Discreta
Discreta	Muestreada	DIGITAL

- Periodicidad
  - Señal periódica -> se repite en el tiempo
  - Señal aperiódica -> no se repite

Representación digital de la información

- Unidades de información
  - Información de un suceso a: $I(a)=\log_x \frac{1}{P(a)}$
    - X = 2 -> Shannon
    - X = e -> NAT
    - X = 10 -> Hartley
- Representación de dígitos binarios -> bits
  - Si '0' y '1' son equiprobables => 1 bit ≡ 1 Shannon

$$I('0')=\log_2 \frac{1}{0,5}=1\ Shannon$$

$$I('1')=\log_2 \frac{1}{0,5}=1\ Shannon$$

Parámetros de la comunicación

- Atenuación $A(dB)=10\log \frac{P_E}{P_S}$

  La atenuación es función de la frecuencia

  Función de trasferencia del canal -> modifica la señal

  Ancho de banda del canal -> atenuación menor del 50% en potencia (3dB)
- Distorsión = efecto por el cual el medio se comporta de forma no lineal
  - Amplitud -> se atenúa de distinta forma las distintas componentes
  - Retardo -> retardo distinto para las distintas componentes
- Perturbaciones = señales ajenas al sistema:
  - Ruido
    - Ruido térmico -> agitación de los electrones
    - Ruido de intermodulación -> no linealidad => aparición de armónicos que interfieren
    - Diafonía -> acoplamiento entre líneas que transportan señales
    - Ruido impulsivo (ráfagas)
  - Interferencias

Adaptación de impedancias

- Potencia transmitida

$$P_L=|E|^2\cdot\frac{R_L}{|Z_S+Z_L|^2}$$

Potencia máxima para adaptación de impedancias

- Reflexión de ondas -> coef. de reflexión de potencia

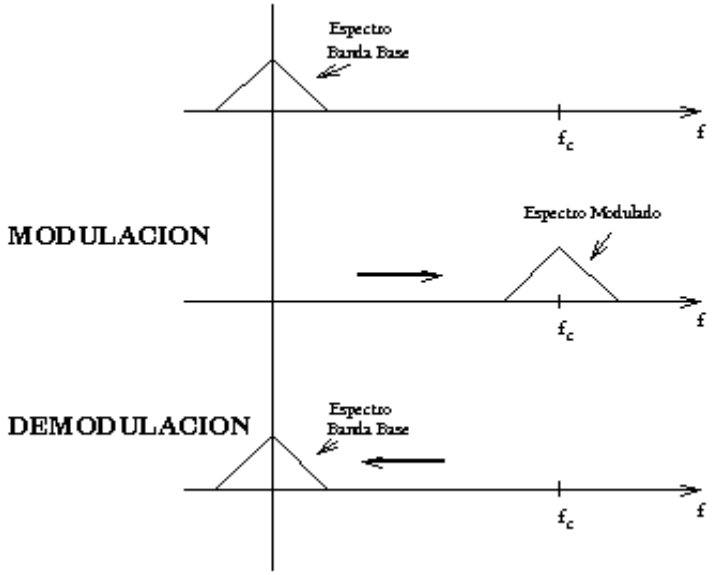
$$R_p=\frac{P_{incidente}}{P_{reflejada}}=\left[\frac{|Z_L-Z_S|}{|Z_L+Z_S|}\right]^2$$

Reflexión nula para adaptación de impedancias

Parámetros de la comunicación

- Calidad del canal -> se mide como:
  - tasa de error (errores/bit)
  - relación S/R = $(S/R)(dB)=10\log \frac{P_S}{P_R}$
- Capacidad del canal = velocidad máxima de transmisión
  - Teorema de Nyquist: máxima velocidad de modulación = 2W (baudios)
  - Teorema de Shanonn (señales multinivel):
    - Amplitud total (señal + ruido) = $\sqrt{S+R}$
    - Separación mínima entre niveles = $\sqrt{R}$
    - Máximo número de niveles posibles (según ruido) = $\log_2 \sqrt{1+S/R}$
    - Capacidad máxima del canal (bps): $C=W\log_2(1+S/R)$
- Protocolos de transmisión
  - Protocolo = conjunto de reglas que hacen posible la comunicación
  - El protocolo controla la comunicación transmitiendo información de control junto con los datos

Modulación



SE UTILIZA UNA PORTADORA SENOIDAL (SENAL MODULADA):

$$a_c = A_c \operatorname{sen}(2\pi f_c t + \theta_c)$$

MODULACION ANALOGICA: SENAL ANALOGICA COMO MODULADORA

MODULACION DIGITAL : SENAL DIGITAL COMO MODULADORA

A_c : MODULACION EN AMPLITUD (AM, ASK)

f_c : MODULACION EN FRECUENCIA (FM, FSK)

θ_c : MODULACION EN FASE (PM, PSK)

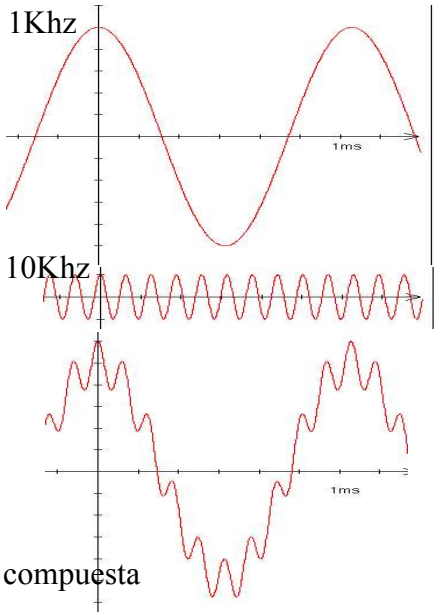
→ QAM

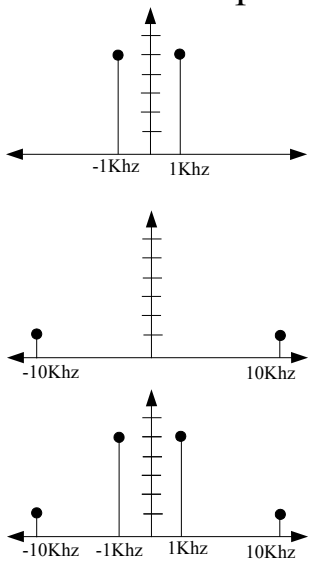
Modulación

- Modulación = variación de la frecuencia de la señal para permitir su transmisión por el medio
  - Facilidad de radiación => longitud antena ~ λ
  - Reducción del ruido e interferencias
  - Posibilidad de multiplexación
  - Superar limitaciones de los equipos -> funcionamiento óptimo a determinadas frecuencias (p.e. amplificadores)
- "Superposición" de dos señales
  - Moduladora (baja frecuencia) -> señal de información
  - Portadora (alta frecuencia) -> señal que se transmite (modificada)

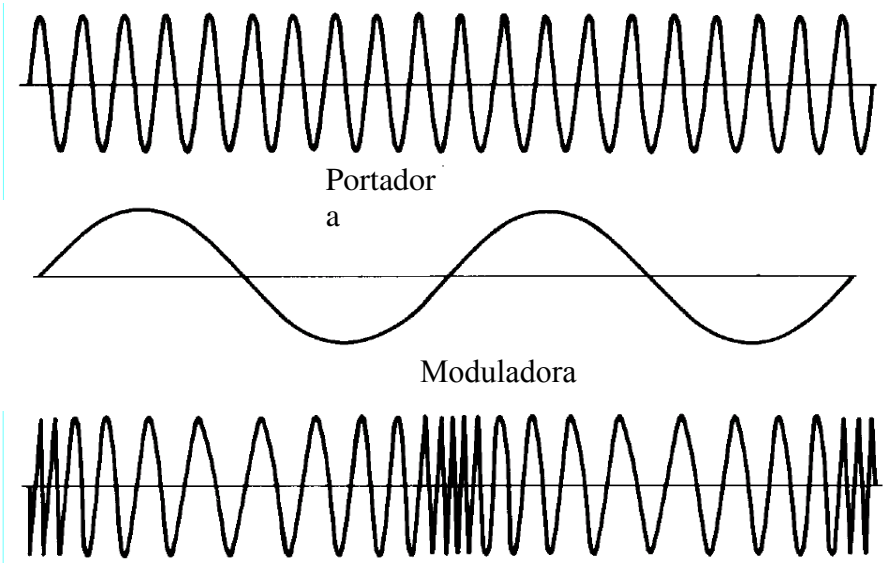
Port.\Mod.	Analógica	Digital
Analógica	Modulación analógica	Modulación Digital
Digital	Codificación o modulación por impulsos	Codificación

Representación tiempo-frecuencia. El espectro



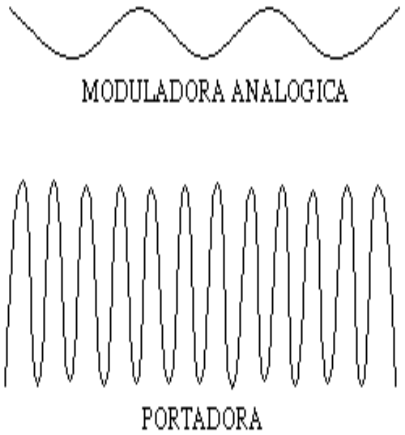


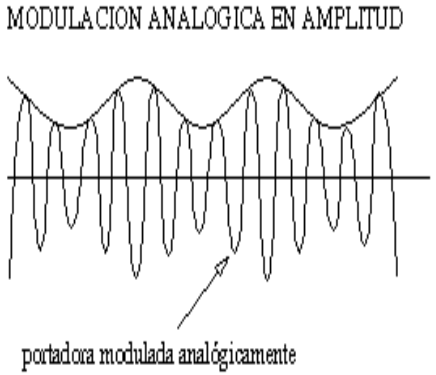
Modulación en fase (PM)

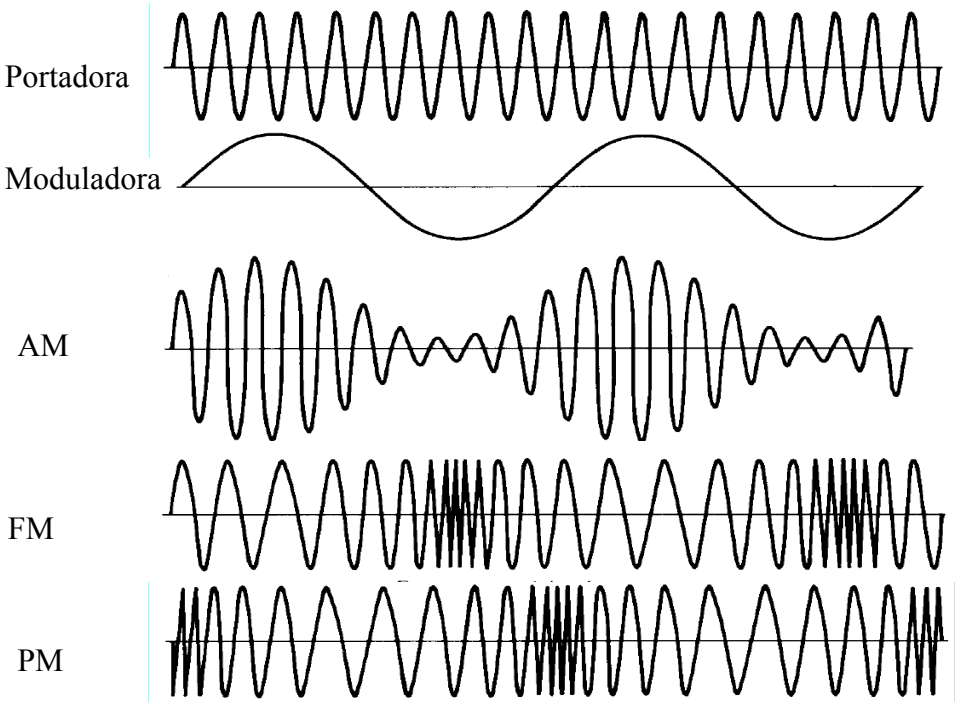


Portadora modulada

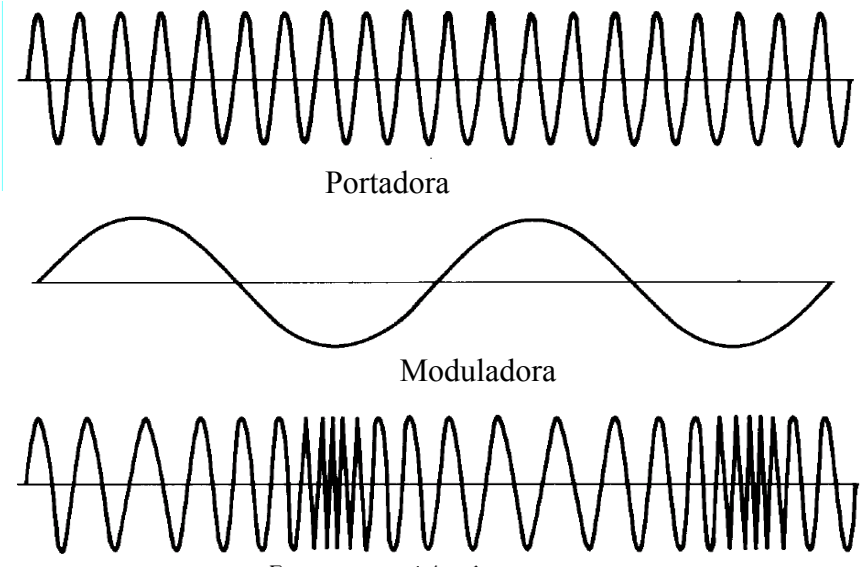
Modulación analógica





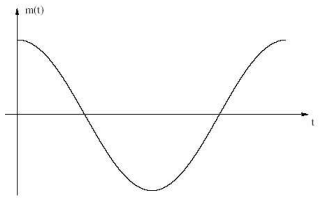


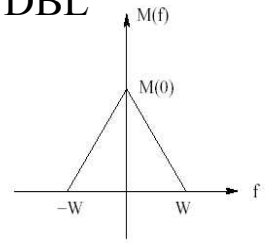
Modulación en frecuencia (FM)



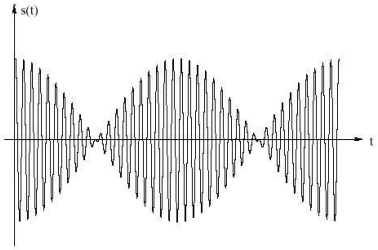
Portadora modulada

Modulación DBL

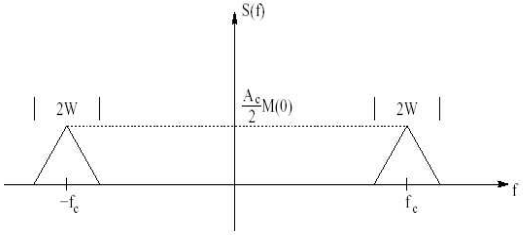




Espectro de la señal moduladora.



portadora modulada



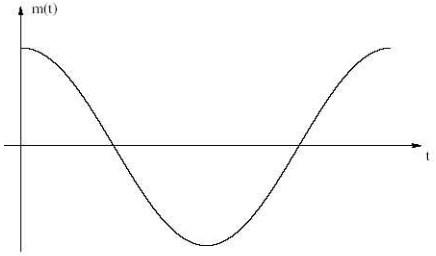
Espectro de la señal modulada DSB.

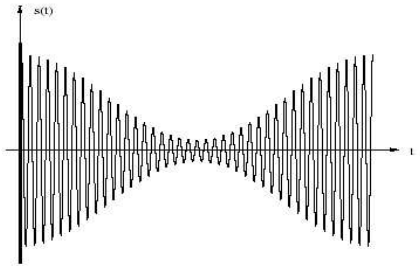
$S_{DBL}(t) = p(t)\cdot m(t) = Ap\cos(2\,pi\,f_p t)\cdot m(t)$

Rendimiento máximo = 50% B_T=2W

Receptores más complejos

Modulación de AM





Señal modulada sin sobremodulación.

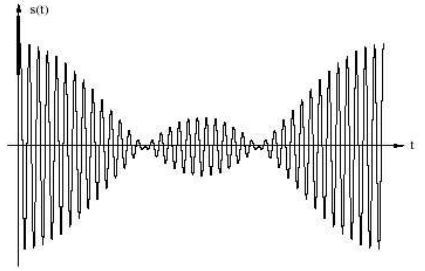
- moduladora $m(t) = A_m\cos(2\,pi\,f_m t)$
- portadora sin modular $S_{AM}(t) = Ap\cos(2\,pi\,f_p t)$
- portadora modulada

$S_{AM}(t) = Ap[1 + k_a\cdot m(t)]\cos(2\,pi\,f_p t)$

$|k_a\cdot m(t)| < 1$ sin sobremodulación

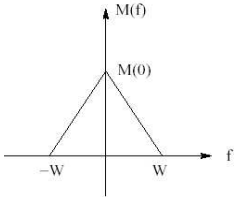
$|k_a\cdot m(t)| < 1$ con sobremodulación

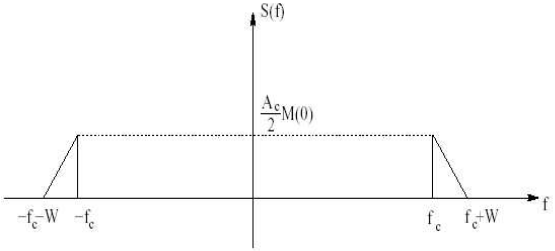
índice de modulación $u = k_a\cdot A_m$

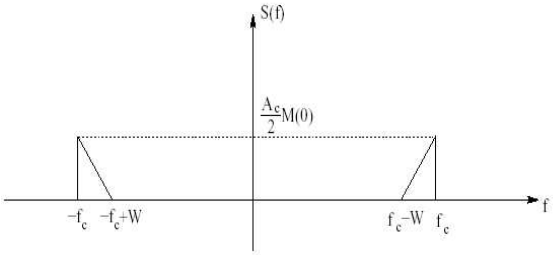


Señal modulada con sobremodulación.

Modulación BLU

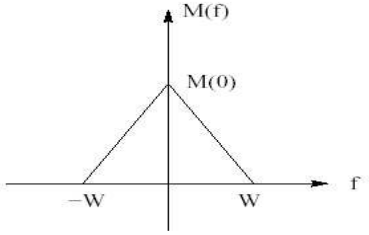




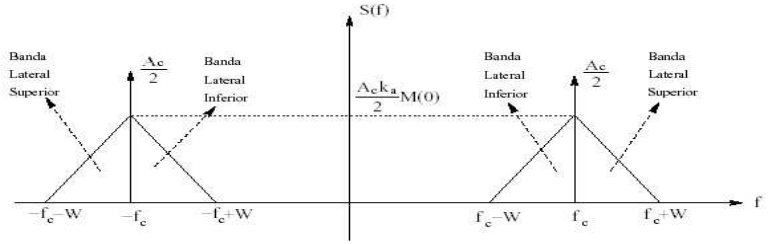


- Rendimiento máximo = 100
- B_T=W
- Circuitos muy complejos, con filtros muy difíciles de hacer.

Modulación de AM vista en frecuencia



Espectro de la señal moduladora.

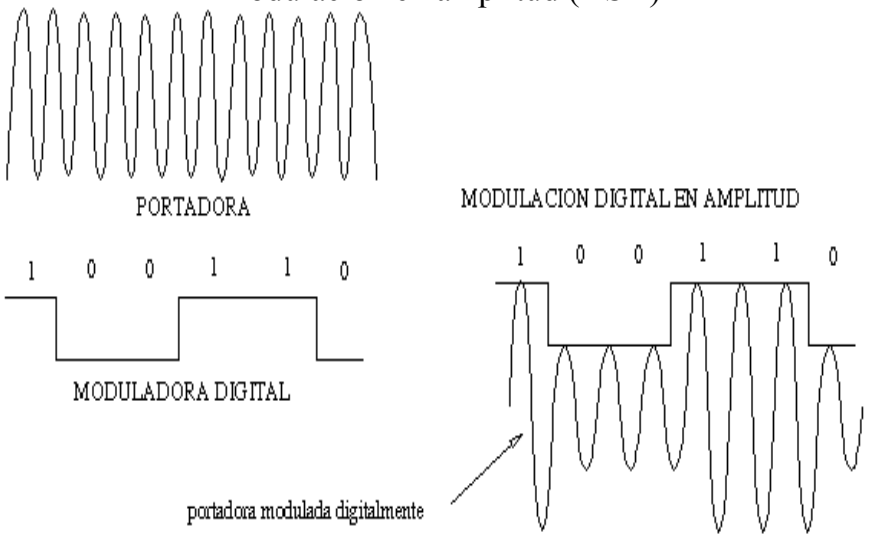


Espectro de la señal modulada.

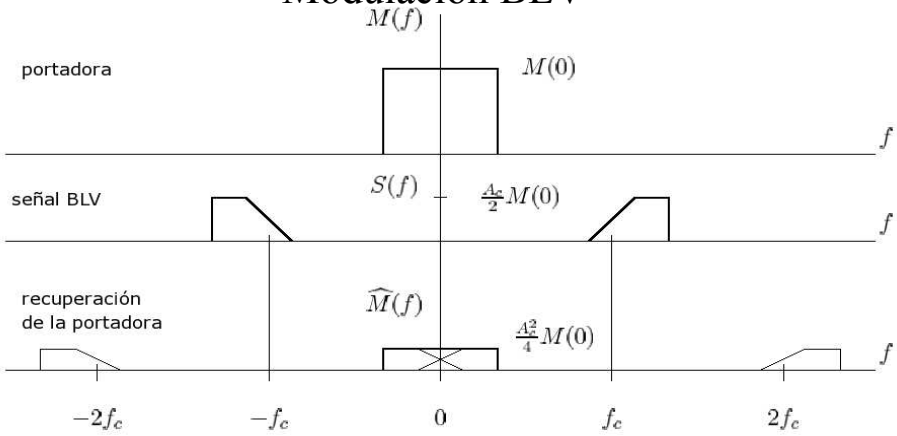
B_T=2W Rendimiento máximo potencia = 17%

Modulación digital con portadora analógica

Modulación en amplitud (ASK)

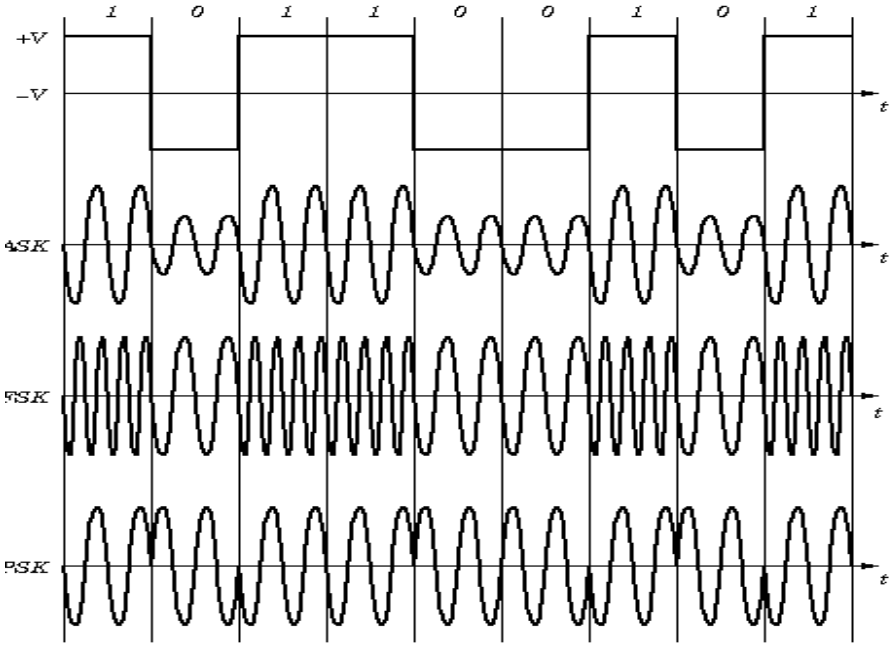


Modulación BLV

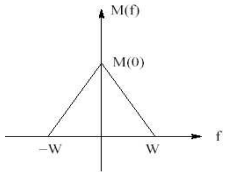


- A partir de DBL, por filtrado -> una banda y parte de la otra
- Rendimiento máximo cercano a 100%
- B_T cercano a W
- Circuitos más sencillos que en BLU -> filtro más sencillo
- La señal "que falta" en una banda se compensa con "la que sobra" en la otra. Aparece algo de distorsión

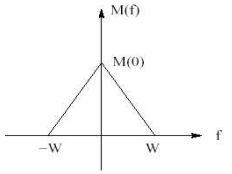
Modulación en frecuencia y fase (FSK y PSK)



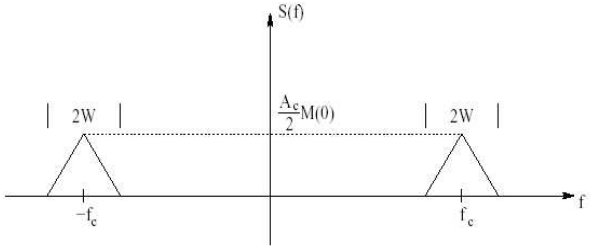
Modulación en cuadratura QAM



moduladora m_1

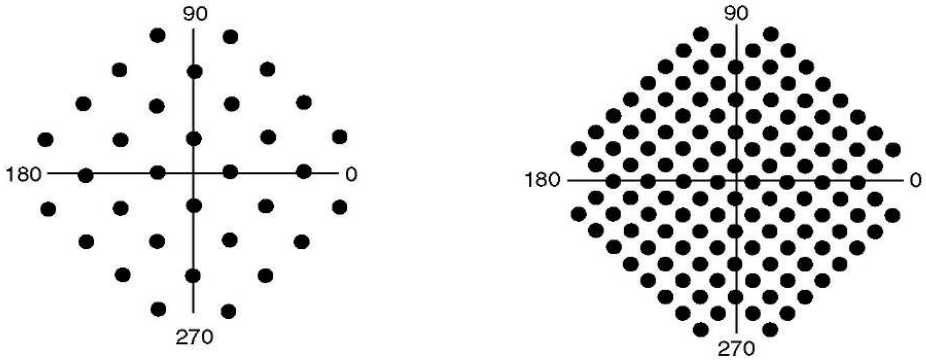


moduladora m_2



$$S_{QAM}(t) = A_p m_1(t)\cos(2\pi f_p t) + A_p m_2(t) sen(2\pi f_p t)$$

- Modulación de dos señales W
- Transmisión de las señales desfasadas 90º
- $B_T = 2W$

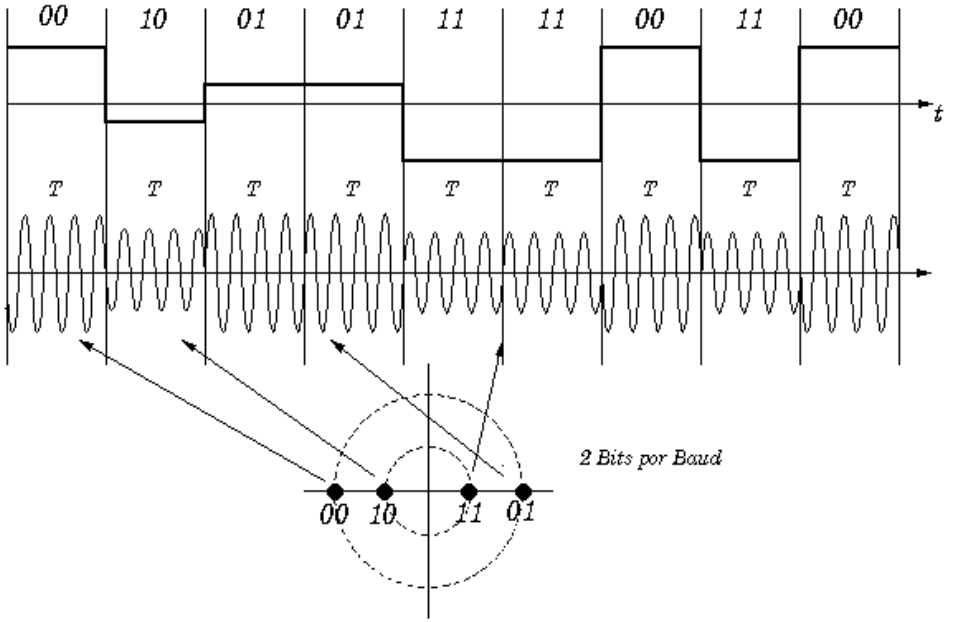


(a) (b)

(a) V.32 para 9600 bps

(b) V32 bis para 14.400 bps

MODULACIÓN HÍBRIDA FASE–AMPLITUD

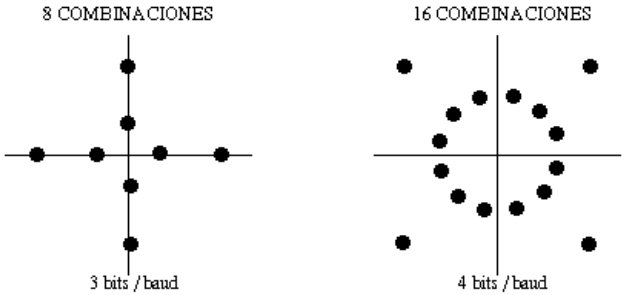


Codificación

- Moduladora analógica => modulación por impulsos
  - Objetivo: Transmisión digital de señales analógicas
  - Proceso (conversión Analógico-Digital):
    - Muestreo -> discretización en amplitud => señal discreta en el tiempo. No hay pérdida de información
    - Cuantificación -> discretización en amplitud => señal digital. Pérdida de información
    - Codificación => formato de representación binaria
  - Tipos: PAM, PWM, PPM, delta, MIC....
- Moduladora digital => codificación
  - Objetivos:
    - Reducir ancho de banda de la señal
    - Eliminar componente continua
    - Sincronización
    - Detección de errores
    - Mejorar la tasa de error
  - Tipos: bifásica, multinivel, manchester, NRZ, 5B6B, HDB3, etc.

MODULACION HIBRIDA QAM

(QUADRATURE AMPLITUD MODULATION)



9600 bps SOBRE LINEA DE 2400

BAUD: NUMERO DE VECES QUE LA SEÑAL CAMBIA SU VALOR (VOLTAJE, FRECUENCIA, FASE)

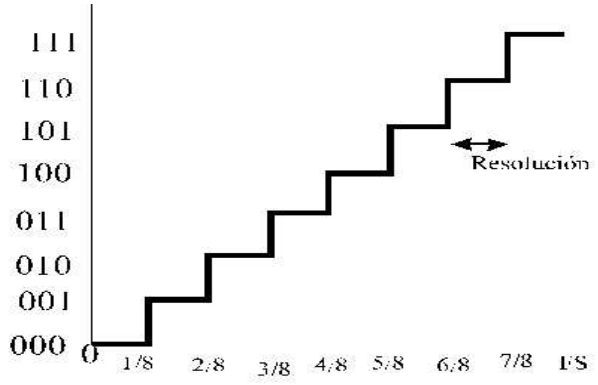
POR SEGUNDO: $\frac{1}{T}$

TASA BINARIA: $R = \frac{1}{T} \log_2 M \text{ bits / seg}$

T : INTERVALO DE LA SEÑAL

M : NUMERO DE VALORES POSIBLES DE LA SEÑAL EN EL INTERVALO (EJEMPLO: AMPLITUD & FASE)

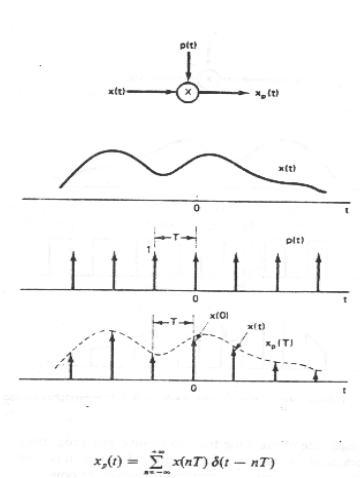
La cuantificación



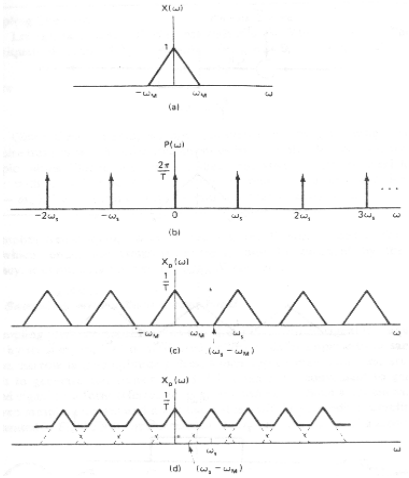
- Muestra -> cualquier amplitud
- N valores normalizados de aplitud => aproximación
  - Redondeo -> error = ±½Δ
  - Truncamiento -> error = Δ
- Codificación -> n bits, siendo $N = 2^n$

El muestreo

- Muestreo = discretizar en el tiempo señal analógica
- No se pierde información si fm ≥ 2W



Muestreo visto en el tiempo



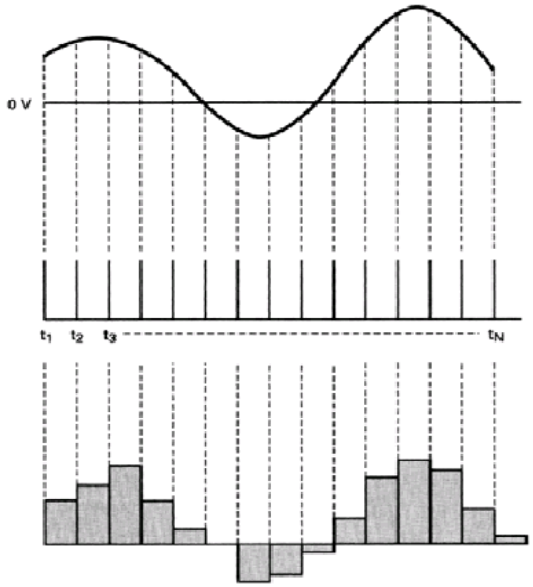
Muestreo visto en la frecuencia

Modulación por amplitud de pulsos (PAM)

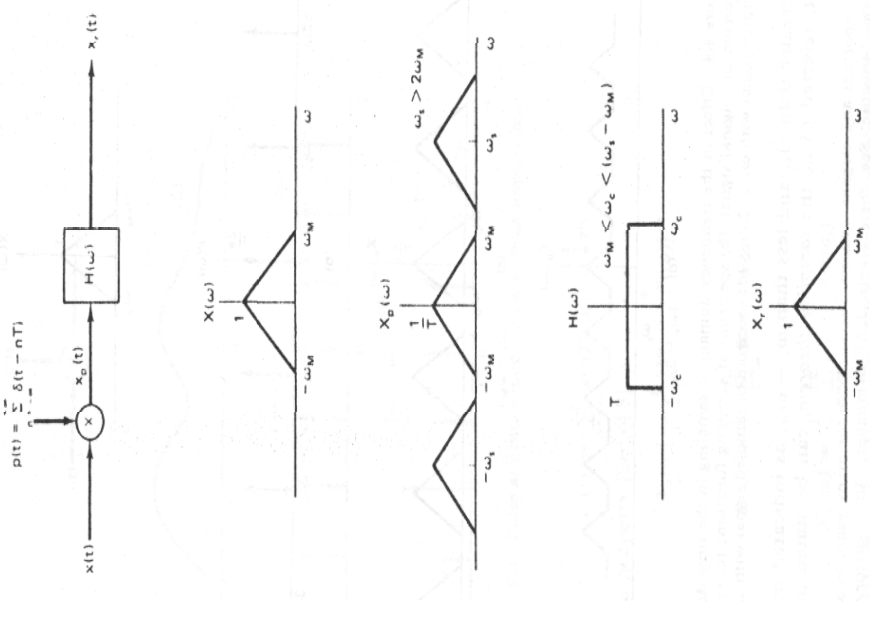
(a) input signal;

(b) Sampling signal

(c) PAM signal



recuperación de la señal original con un filtro ideal



Modulaciones PWM y PPM

(a) analog signal;

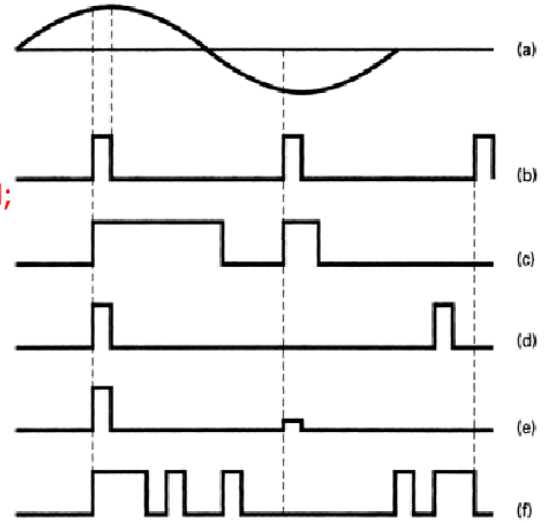
(b) sampling signal;

(c) PWM;

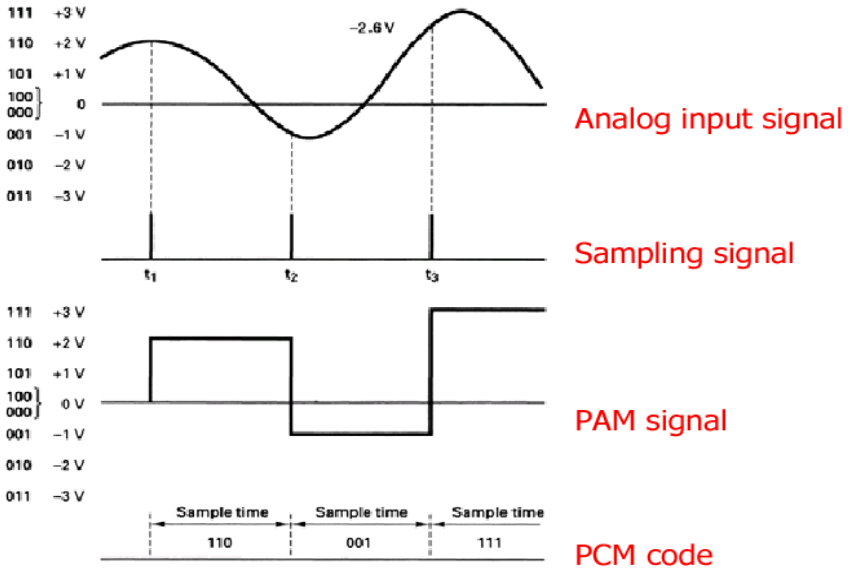
(d) PPM;

(e) PAM;

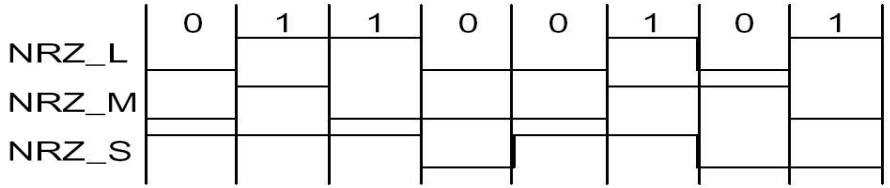
(f) PCM



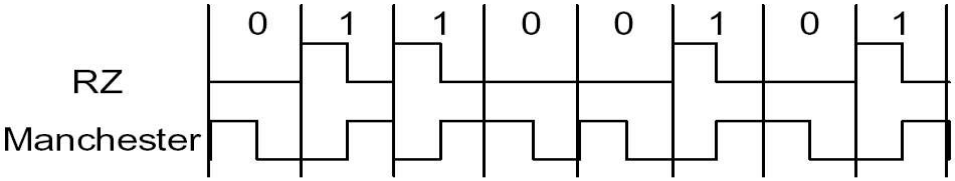
Modulación por pulsos codificados (MIC o PCM)



Datos digitales – señales digitales

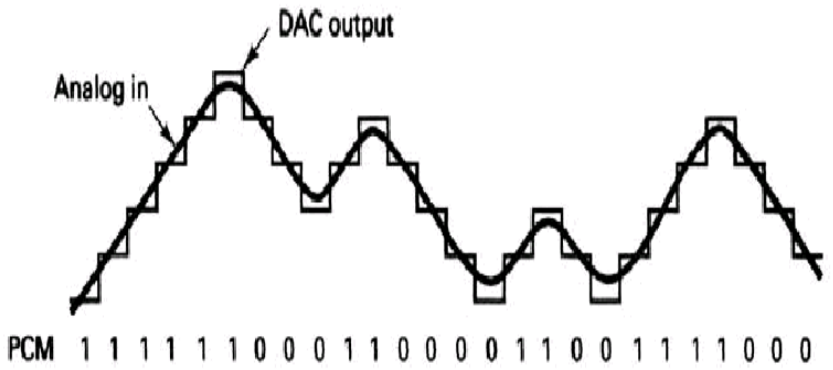


- NRZ_L = bipolar "normal"
- NRZ_M -> "1" = transición al principio del intervalo
- NRZ_S -> "0" = transición al principio del intervalo



- RZ -> valor del bit en ½ periodo + retorno a cero en el otro medio
- Manchester -> flancos en el centro del bit: "1" = flanco subida, "0"=flanco bajada. Garantiza reloj. Duplica ancho de banda.

Modulación delta (diferencial)



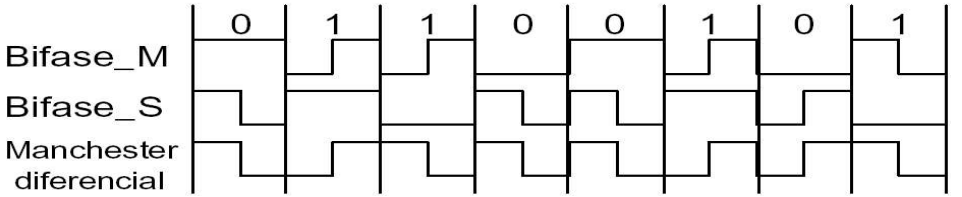
Codificación de la información

- Representación de un dígito binario (“0” o “1”) -> bit
- Representación de un rango mayor de símbolos => código:
  - Símbolos mensaje = cada uno de los símbolos representados
  - Palabras del código = cada una de las combinaciones de bits que representa a un símbolo.
  - N mensajes => como **mínimo** código n bits $N = 2^n$
  - ejemplo -> representación de los símbolos decimales (BCD)

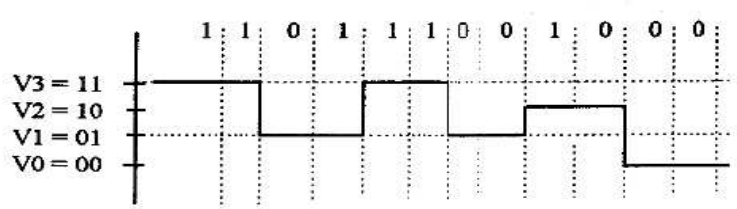
Símbolo	código
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001

- Fuentes de información
  - De memoria nula -> la probabilidad de cada símbolo depende sólo de ese símbolo
  - Con memoria -> la probabilidad de cada símbolo depende de los anteriores

Datos digitales – señales digitales



- Bifase_M -> “1” = flanco de subida
- Bifase_S -> “0” = flanco de bajada
- Manchester diferencial -> siempre flanco en medio. “1” sin flanco al principio, “0” flanco al principio.

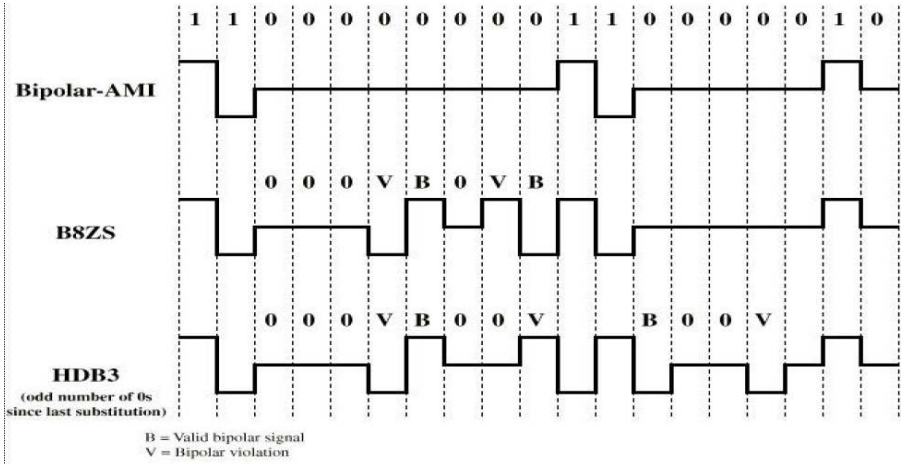


- Multivalente -> N niveles. Codificacion n bits por transición.

- Códigos históricos:
  - Morse (telégrafo)
  - Baudot (teletipo) -> 5 bits + bit inicio + bit paada
- Códigos modernos
  - EBCDIC (8 bits) -> entornos IBM
  - ASCII (7 bits) -> normalizado ANSI e ISO

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.asciitable.com



- AMI -> “0” = ausencia de señal. “1” = pulso positivo o negativo (alternados)
- B8ZS (EEUU)
  - no permite 8 “0” seguidos -> genera dos violaciones de AMI (invierte polaridad)
- HDB3 (UE y Japón)
  - No permite 4 “0” seguidos -> genera una violación de AMI

- Proceso
  - Generación
    - Se añaden al dato a transmitir tantos ceros a la derecha como el orden del polinomio generador
    - Se divide el polinomio resultante por el polinomio generador y se obtiene el resto
    - El resto se suma al dato a transmitir expandido con los ceros
  - Comprobación
    - El receptor divide el dato que le llega por el polinomio generador.
    - Si el resto es 0 no hay error
    - Si el resto no es 0 hay errores
- Polinomios cíclicos más usados
  - CRC-12 = $x^{12} + x^{11} + x^3 + x^2 + x + 1$
  - CRC-16 = $x^{16} + x^{15} + x^2 + 1$
  - CRC-CCITT = $x^{16} + x^{12} + x^5 + 1$
  - Características de los CRC16
    - Detecta 100% errores simples, y dobles
    - Detecta 100% errores en un número impar de bits
    - Detecta 100% de los paquetes con errores de longitud menor que 18 y 99'998% de los mayores

Códigos detectores y correctores de error

- Redundancia de un código
  - Redundancia = diferencia entre la información máxima que puede generar una fuente y la que realmente genera
  - Redundancia de un código -> uso de más bits de los "necesarios"
  - bits de código (cod. binario) > bits de información (Shannon)
  - Distancia de hamming
    - D. H. entre dos combinaciones binarias = nº de bits que hay que cambiar para pasar de una a otra.
    - D. H. de un código = D.H. mínima entre combinaciones
    - D.H. > 1 => redundancia
- Códigos detectores y correctores de error
  - Un error de n bits es detectable por un código con distancia n
  - Y corregible por un código de distancia 2n + 1

Compresión de datos

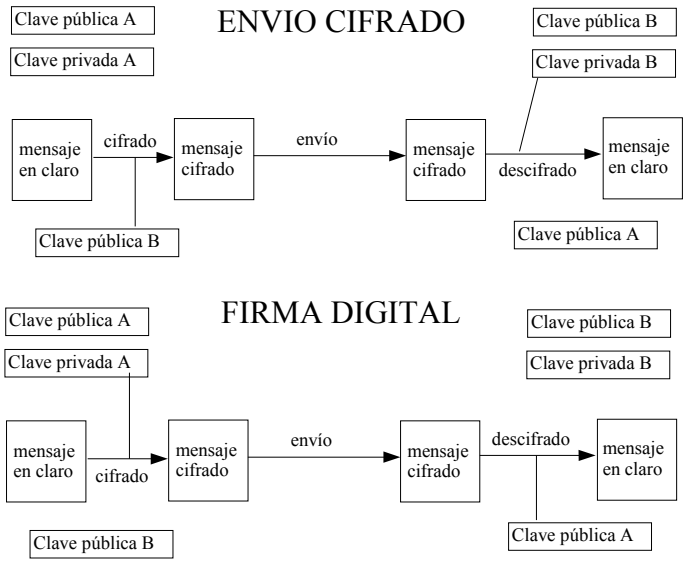
- Dos tipos de técnicas:
  - Sin pérdidas -> información almacenada = original
  - Con pérdidas -> información comprimida ≠ original
- Compresión sin pérdidas
  - Basada en eliminar la redundancia => 1bit = 1 Shannon
  - Códigos
    - Símbolos no equiprobables (p.e. letras).
    - Dependen de los anteriores.
    - Agrupaciones en bloques -> también dependen unas de otras
    - Ejemplo: "ME LLEVO EL PARAGUAS PORQUE ESTA LLOVIENDO"
  - Tipos:
    - Compresores estadísticos -> basados en la probabilidad de un símbolo: codificación con nº de bits menor según probabilidad
    - Compresores basados en diccionario -> estudian secuencias repetidas.

- Códigos m sobre n
  - Son códigos de m bits
  - Sólo son válidas las combinaciones que tienen n bits a 1
  - Distancia de Hamming = 2
- Control de paridad
  - Se añade un bit de paridad
  - Distancia de Hamming = 2
  - Paridad horizontal = para cada dato transmitido
  - Paridad vertical = para todos los bits de una secuancia de datos (columnas)
  - Paridad cruzada = combinación de las dos -> distancia de Hamming = 4
- Códigos cíclicos (CRC)
  - características
    - Detectan ráfagas de errores
    - Tratamiento de las series de bits como polinomios
    - Utilizan un polinomio generador para la comprobación de errores

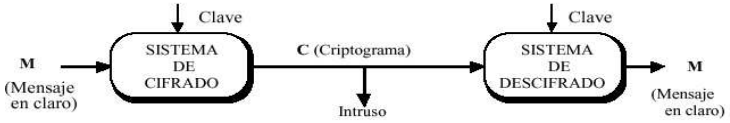
- Advanced Encryption Standard (AES)
  - Publicado el 2 de Octubre de 2000.
  - Se intuye que substituirá al actual D.E.S.
  - El tamaño de clave debe ser de, al menos, 128, 192 y 256 bits (debe admitir los tres), y el tamaño de bloque de cifrado debe ser de 128 bits.
  - Los productos que incorporen AES podrán ser exportados fuera de EE.UU.
- Algoritmos asimétricos
  - Cada usuario tiene un par de claves:
    - Clave privada -> debe ser secreta
    - Clave pública -> puede difundirse a todo el mundo.
  - Sirve para que:
    - Otros usuarios le envien documentación cifrada
    - El propietario de la clave envíe documentación "firmada"

- Compresión con pérdidas
  - En sistemas donde se pueden tolerar diferencias (p.e. audio)
  - Basadas en:
    - Medidas de la percepción -> puede no notarse diferencia
    - Filtrado -> selección del espectro donde está la mayor parte de la potencia.
    - Redundancia temporal -> "lentitud" de variación en la imagen/señal
    - Uso de compresión sin pérdidas
- Ejemplos (algoritmos):
  - Sin pérdidas
    - Estadísticos
      - Shannon-Fano (no óptimo): Se usa en ZIP
      - Huffman (óptimo): Se usa en LZH, BZIP2
    - Basados en diccionario
      - Familia LZ78 (Lempel-Ziv 78): LZW, LZC (compress), GIF, V42bis
      - Familia LZ77 (Lempel-Ziv 77): ZIP, LZH
  - Con pérdidas: MPEG (audio), JPEG (imagen), MPEG-1, MPEG-2, MPEG-4 (video)

Funcionamiento de un sistema de doble clave



Cifrado de datos



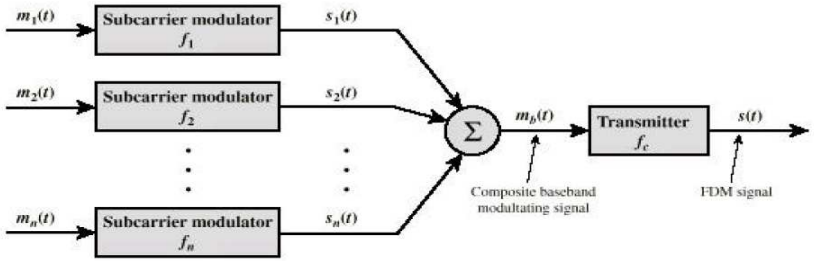
Esquema de transmisión segura de un mensaje

- Claves iguales -> Algoritmos simétricos (DES, IDEA, AES)
- Claves diferentes -> Algoritmos asimétricos (RSA, D-H, PKCS)
- Data Encryption Standard (DES)
  - Estándar americano de 1977
  - clave de 56 bits sobre bloques de datos de 64 bits-> con la tecnología de la época se tardaban 2200 años en romper la clave, hoy 3 días.
- International Data Encryption Algorithm (IDEA)
  - Tuvo su aparición en 1992.
  - Considerado por muchos el mejor y más seguro algoritmo simétrico disponible en la actualidad.
  - Trabaja con bloques de 64 bits de longitud, igual que el DES, pero emplea una clave de 128 bits.
  - Se usa el mismo algoritmo tanto para cifrar como para descifrar.

Multiplexación

- Objetivos -> compartir el medio
  - Un solo cable frente a muchos cables
  - Posibilidad de trasnmisión de varias señales donde de otro forma no se podría (p.e. por el aire)
  - Aprovechamiento del ancho de banda
- Tipos
  - Multiplexación por división en frecuencias (FDM).
  - Multiplexación por division en tiempo (TDM síncrona).
  - Multiplexación estadística por división en el tiempo (TDM estadística, asíncrona o inteligente).

Modulación por división en frecuencia (MDF)



- Modulación -> desplazamiento de la señal a frecuencias altas
- Multiplexación -> suma de varias señales moduladas a frecuencias distintas
- Señales limitadas en banda => no hay solapamiento
- Válido para trasnmisión analógica y digital
- Ancho de banda total = suman anchos de banda

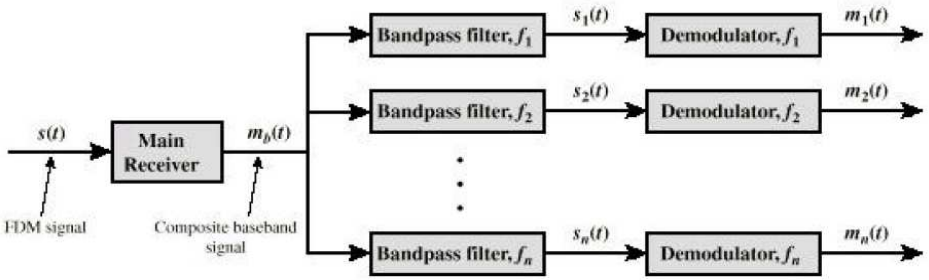
Sistemas de doble clave

- Propiedades
  - Algoritmos asimétricos
  - Válidos para encriptar y firmar
  - Tiempos de cálculo muy altos => sólo se firma un extracto.
  - Necesidad de autoridades certificadoras para las firmas:
    - Fábrica Nacional de Moneda y Timbre
    - Agencia de Certificación Electrónica
    - Verisign
    - .....
- Algoritmos de cifrado
  - RSA
    - Basado en la utilización de un número producto de dos números primos grandes => producto=clave públlica, factorización=clave privada.
    - Claves de tamaño variable, típicos 512 o 1024bits.Bloques variables, menores que la clave
    - Muy seguro. Se usa en ssh

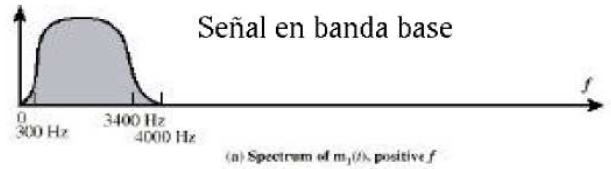
Sistemas de doble clave

- Diffie-Hellman
  - Algoritmo histórico (1976)
  - Precursor de RSA
  - Es vulnerable en algunos supuestos
- PKCS (Publick-key Cryptografy Standards)
  - 15 estándads basados en RSA.
- Funciones de hash
  - Son funciones unidereccionales de resumen -> generan una cadena de resumen de un documento (“no puede haber” dos cadenas de resumen iguales)
  - MD5 (128 bits), SHA-1(160 bits), RIPEMD(160 bits), etc.
- Protocolos de seguridad
  - Utilizan funciones de hash y sistemas de doble clave para trasnferir información de forma segura
  - PGP, SSL, SET, IPSEC, etc.

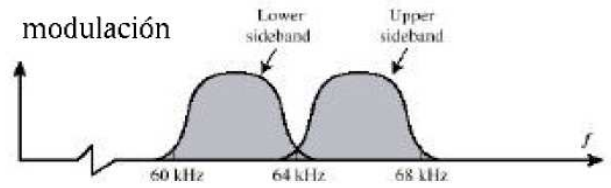
Recuperación de la señal



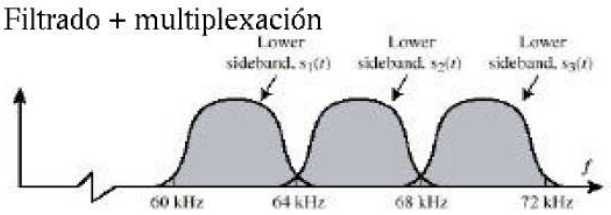
- Filto P.Banda-> elimina todo menos un canal
- Demodulador -> desplaza a frecuencia baja => banda de base
- Problemas
  - Diafonía si los espectros de señales adyacentes se solapan demasiado.
  - Intermodulación en enlaces largos. Los amplificadores de un canal podrían generar frecuencias en otro canal.



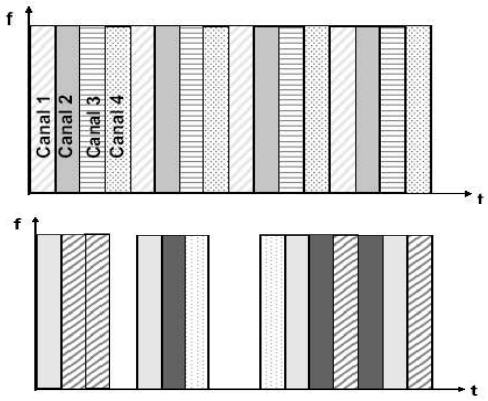
(a) Spectrum of $m_1(t)$, positive f



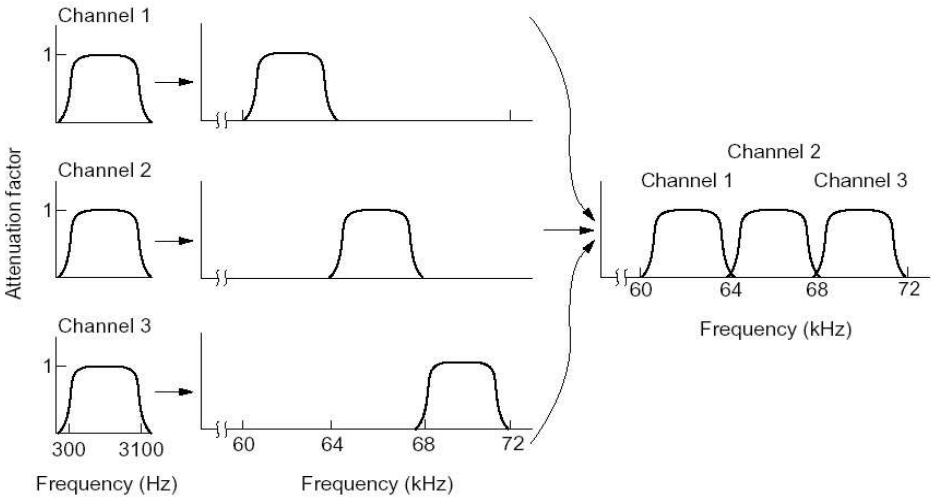
(b) Spectrum of $s_1(t)$ for $f_1 = 64$ kHz



Multiplexación por división en el tiempo (MDT)



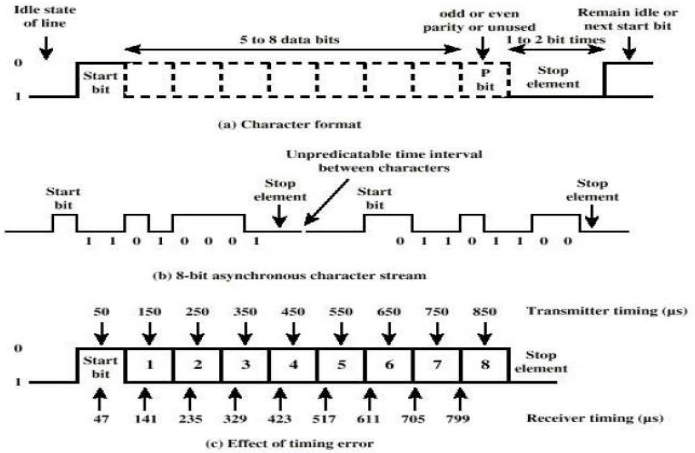
- Asignación de intervalos de canal (slots) a los distintos canales.
- MDT síncrona -> asignación fija de intervalos de canal => desperdicio de ancho de banda
- MDT asíncrona -> asignación variable según las necesidades => hay que identificar canales



Transmisión serie/paralelo

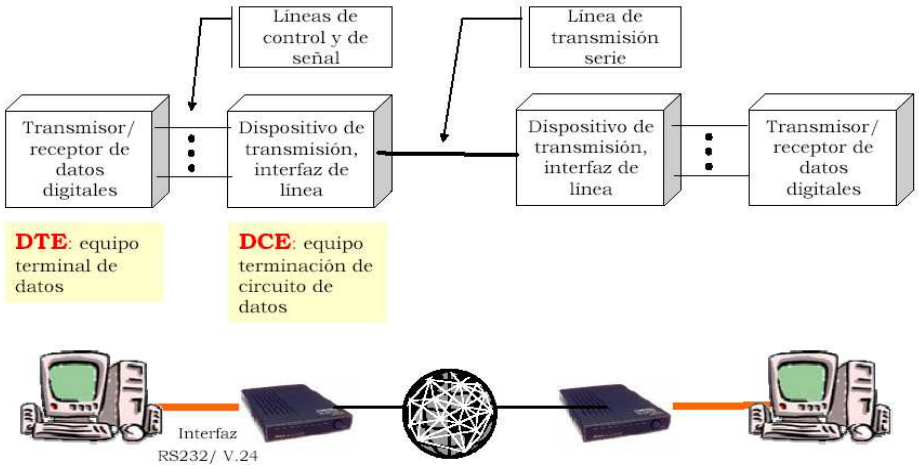
- Transmisión serie
  - Bit a bit
  - Menos hilos
  - Mayor complejidad: necesidad de una protocolo
  - Transmisión a larga distancia
- Transmisión paralelo
  - Varios bits a la vez
  - Mayor nmero de hilos
  - Más simple, sin protocolo o protocolo más sencillo
  - Transmisión a corta distancia

Transmisión asíncrona

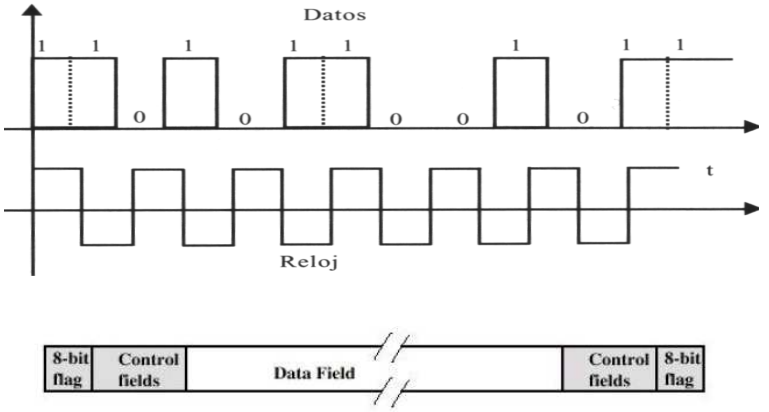


- Relojes distintos
- Errores de sincronización -> cadenas cortas.

Interfaces para las comunicaciones de datos



Transmisión síncrona

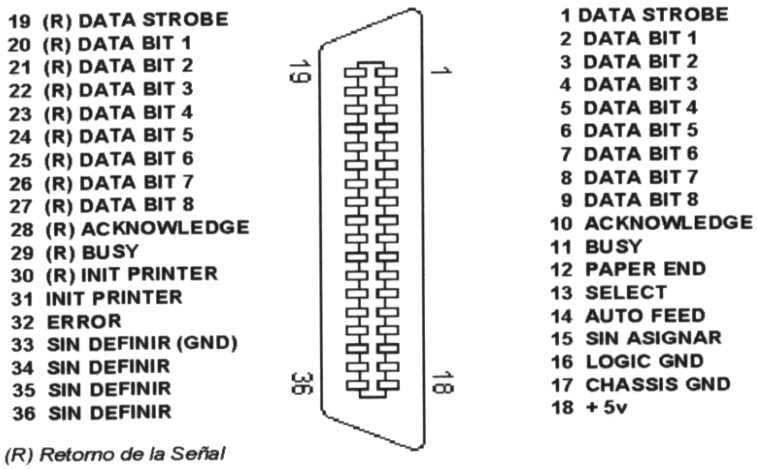


- Reloj
  - Por linea aparte
  - Incluido en la codificación (p.e. manchester)
- Menor sobrecarga de bits de control que en t. asíncrona.

Señales RS-232 en un conector PC de 9 pines

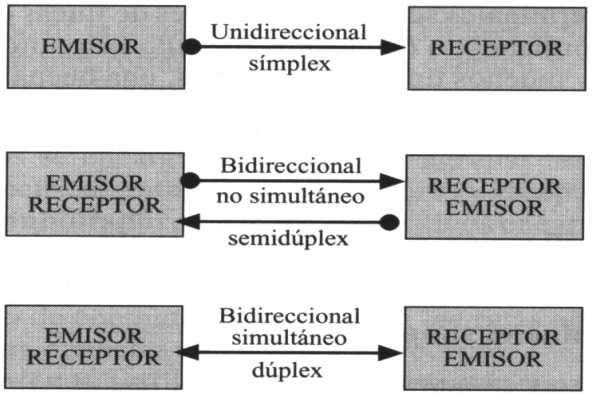
PIN	SEÑAL	NOMBRE	FUNCIÓN
1	DCD	Data Carrier Detect	Detección de portadora
2	RD	Received Data	Entrada de datos en el DTE
3	TD	Transmitted Data	Salida de datos del DTE
4	DTR	Data Terminal Ready	DTE preparado y listo. Pone en funcionamiento al módem
5	GND	Masa	Masa del circuito
6	DSR	Data Set Ready	ETCD está listo para comunicar con DTE
7	RTS	Request To Send	DTE desea cambiar a modo de transmisión
8	CTS	Clear To Send	ETCD está listo para transmitir
9	RI	Ring Indicator	Aviso de llamada detectada

Interfaz Centronics

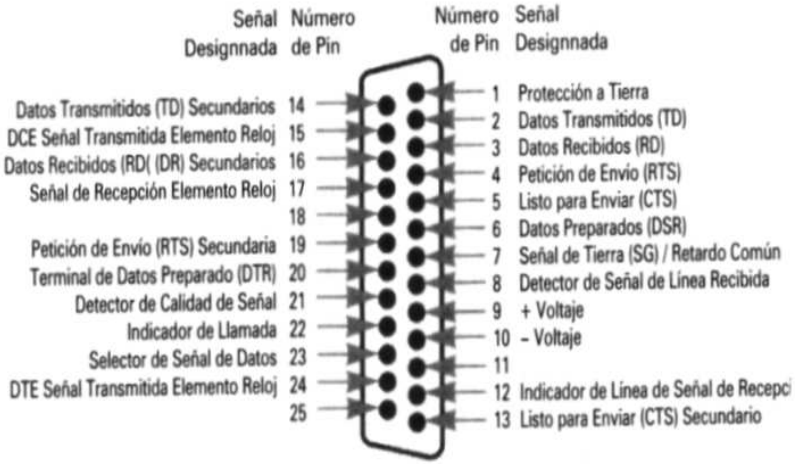


(R) Retorno de la Señal

Modos de diálogo



Interfaz RS-232



- Según utilicen o no sondeo
  - Protocolos de sondeo-selección
    - Sondeo = la estación primaria pide información a la secundaria
    - Selección = la estació primaria envía información a la estación secundaria
    - El proceso se controla con señales:
      - Sondeo = petición de información
      - Selección = aviso de envio de información
      - ACK = validación
      - NAK = no validación
      - EOT = fin de transmisión
  - Protocolos sin sondeo: no realizan sondeo
    - Control de flujo hardware: RTS/CTS
    - Control de flujo software: XON/XOFF
      -

Protocolos de comunicación

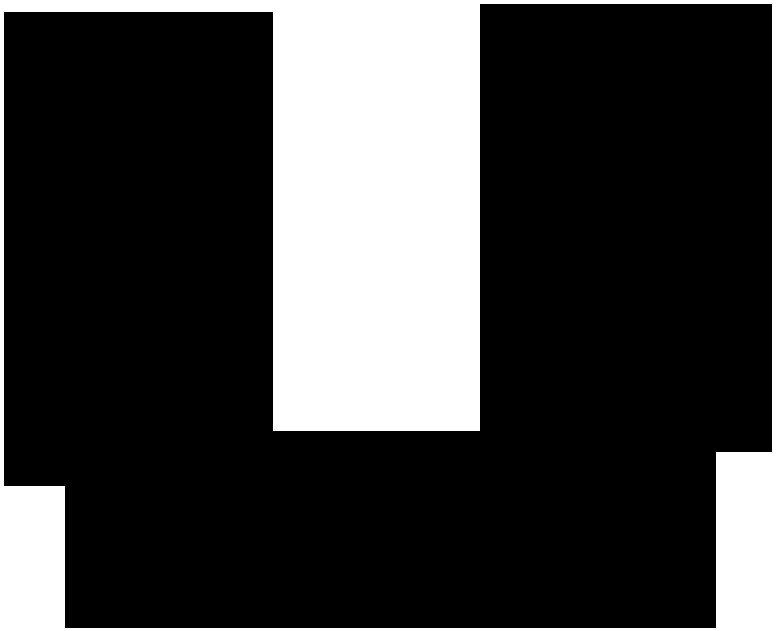
- Protocolo = conjunto de normas que hacen posible la comunicación entre dos o más nodos.
- Funciones más importantes de un protocolo:
  - Establecimiento y fin de la comunicación
  - Sincronización de la comunicación -> a nivel de bit, de palabra y de trama.
  - Direccionamiento -> identificación de los nodos
  - Control de flujo y de congestión -> permitir a la rede compartir sus recursos entre varios nodos dando servicio a todos.
  - Control de errores -> códigos y sistemas para la detección y recuperación de errores.
  - Estrategias de encaminamiento -> utilización de los recursos de la red de forma óptima, caminos alternativos, etc.
- Arquitectura de protocolos
  - Procesos independientes
  - Implementación por software o hardware
  - Estructura en capas.

- Según utilicen o no prioridades
  - Sistemas sin prioridad
    - MUX-MDT (Multiplex por división en el tiempo)
      - El canal se divide en intervalos de tiempo
      - Se asigna un intervalo a cada estación
    - CSMA/CD (acceso múltiple por detección de portadora y detección de colisiones)
      - Todas las estaciones pueden utilizar el canal cuando está libre
      - Una estación escucha a ver sie l canal está libre, y si está libre transmite
      - Si dos estaciones empiezan a emitir a la vez se produce una colisión. Cada estación corta el envío y espera un tiempo aleatorio antes de empezar a enviar de nuevo
      - El rendimiento se degrada en sistemas con mucho tráfico por el aumento de las colisiones
    - Paso de testigo
      - Se ransmite por la red un testigo
      - Sólo la estación que tiene el testigo puede transmitir

Clasificación de los protocolos

- Según las unidades de datos con las que trabajan
  - Protocolos orientados a carácter -> década de los 60
  - Protocolos orientados a bit -> modernos
- Según su forma de sincronización -> síncronos / asíncronos
- Según el control sobre el medio
  - Balanceados o simétricos:
    - los dos extremos trabajan igual.
    - Cada uno puede tomar la iniciativa de la comunicación
  - No balanceados a asimétricos
    - Una estación primaria (maestra) y las demás secundarias (esclavas)
    - La estación primaria emite y/o da turnos de palabra para emitir
    - La estación secundaria recibe o espera su turno para emitir
  - Híbridos

Protocolos con ventana deslizante



- Sistemas con prioridad
  - CSMA/CD con prioridad
    - El tiempo de espera después de una colisión no es aleatorio sino que se fija para cada estación, menor cuanto mayor sea la prioridad de la estación
  - Paso de testigo con prioridad
    - El paso del testigo no se hace por turnos, sino que se puede reservar por las estaciones según su prioridad
- Protocolos de ventana deslizante
  - En protocolos normales (parada y espera) el canal permanece sin utilizar mientras se espera la validación del receptor
  - Los protocolos de ventana deslizante permiten enviar varias tramas sin esperar validación y validarlas luego todas a la vez
  - Llevan un contador de tramas transmitidas

- Clasificación según el nivel (OSI):
  - Protocolos de nivel físico (1)
  - Protocolos de nivel de enlace (2)
  - Protocolos de nivel de red (3)
  - Protocolos de nivel de transporte (4)
  - Protocolos de nivel de sesión (5)
  - Protocolos de nivel de presentación (6)
  - Protocolos de nivel de aplicación (7)

Desperdicio de tiempo de canal en protocolos de parada y espera

Protocolo kermit

- Protocolo para transferencia de archivos entre ordenadores (no PCs) a través del módem
- Protocolo de parada y espera, serie, asíncrono
- Tramas de longitud variable:

Mark	Long	no	Tipo	DATOS	Check

  - mark (1 byte) = cabecera (secuencia irrepetible)
  - long (1 byte) = longitud de la trama
  - no (1byte)= número de secuencia de la trama
  - tipo = tipo de trama
  - DATOS (longitud variable)
  - Check (1,2,3 byte) = puede ser check o CRC

Protocolo XMODEM

- Protocolo para transferencia de archivos entre PC's a través del módem
- Protocolo de parada y espera, serie, asíncrono
- Tramas de longitud fija:

SOH	No	C1 no	DATOS	Checksum

  - SOH = cabecera (carácter 1 ASCII)
  - no (1byte)= número de secuencia del paquete
  - C1 no (1byte)= nº secuencia en complemento a 1
  - DATOS (128 bytes)
  - Checsum (1 byte) = suma de todos los bytes de datos

- Permite la transferencia de archivos entre diferentes sistemas
- Sólo presupone que los sistemas son capaces de enviar caracteres imprimibles (20h-7Fh ASCII)
- Lós "códigos de control" son tramas en vez de caracteres
- Tramas de longitud variable
- El protocolo incluye el nombre del fichero
- Permite negociar parámetros de la comunicación
- Permite versiones de ventana deslizante (nº de secuencia en tramas ACK y NACK)
- Permite transferir múltiples ficheros

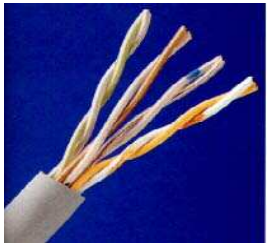
- Inicio de la transmisión -> receptor envía ACK indicando que está preparado para recibir
- Transmisión:
  - El emisor envía un dato
  - Si el receptor lo recibe bien envía ACK
  - Si hay error de secuencia en vía CAN -> corta la transmisión
  - Si hay otro error envía NACK -> el emisor reenvía la trama
- Fín de la transmisión -> el emisor envía EOT

Par trenzado

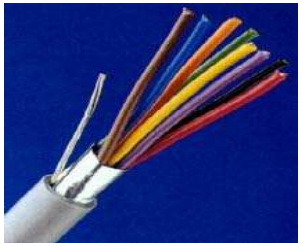
- Características
  - Inicialmente pensado para telefonía: común y económico.
  - Dos conductores aislados y trenzados.
    - Van trenzados para evitar que hagan de antenas.
    - Poca protección frente a interferencias.
    - Resistencia → Diámetro → Ancho de banda.
    - Blindaje.
    - Normalización: **A**merican **W**ire **G**auge.

Calibre (AWG)	19	22	24	26	28
Diámetro (mm)	0.912	0.644	0.511	0.405	0.320

- Composición
  - Dos o cua[redacted]
  - Cables multipares -> de 6 a 2200 pares.
- Tipos
  - No apantallados (UTP)
  - Apantallados (STP)



No apantallado UTP.



Apantallado STP.

Protocolo HDLC

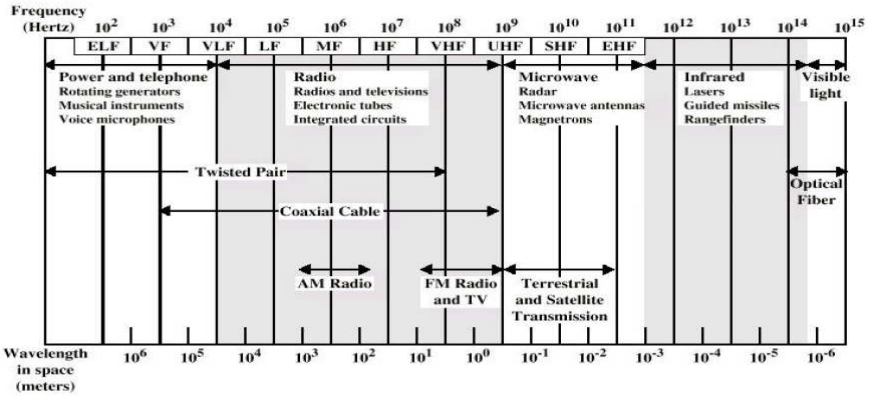
- Protocolo orientado a bit, sínrono, punto a punto o multipunto, de ventana deslizante.
- Estandar ISO.
- Permite explotación duplex del enlace.
- Permite la transmisión de cualquier tipo de datos.
- Permite enlaces equilibrados y no equilibrados.
- Trama:

Band	Dir	Cntrl	DATOS	FCS	Band

  - Bandera = 01111110
  - Dirección (8bits) = identifica estación (multipunto)
  - Control (8bits) = tipo de trama, etc
  - DATOS = cualquier número de bits
  - FCS (16 bits) = control de errores

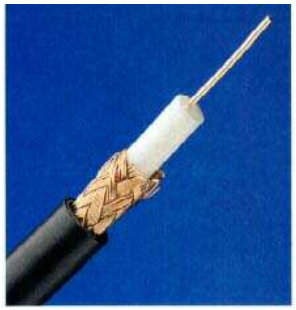
Medios de transmisión

- Tipos de medios:
  - Guiados -> par trenzado, cable coaxial y fibra óptica
  - No guiados -> atmósfera o espacio exterior (infrarrojos, radioenlaces, satelite, radio)
- Espectro electromagnético y uso de los distintos medios



Cable coaxial

- Dos conductores concéntricos.
- Señales TV, redes locales (Ethernet).
- Características
  - Menor atenuación -> repetidores cada Km o hasta decenas de Km, según frecuencia
  - Mejor respuesta en frecuencia.
  - Inmunidad al ruido.
  - Mayor ancho de banda que cable de pares
  - Más caro y pesado.
- Denominación: RG xx X/U (norma MIL C-17 E)



- Coaxial fino: RG 58 C/U
  - Impedancia: Z=50ohm.
  - Capacidad C=101 pF/m
  - Veloc. Propagación = 66% (5ns/m)
  - Tensión máxima U=1.9 KV
  - Atenuación (a 20ºC)

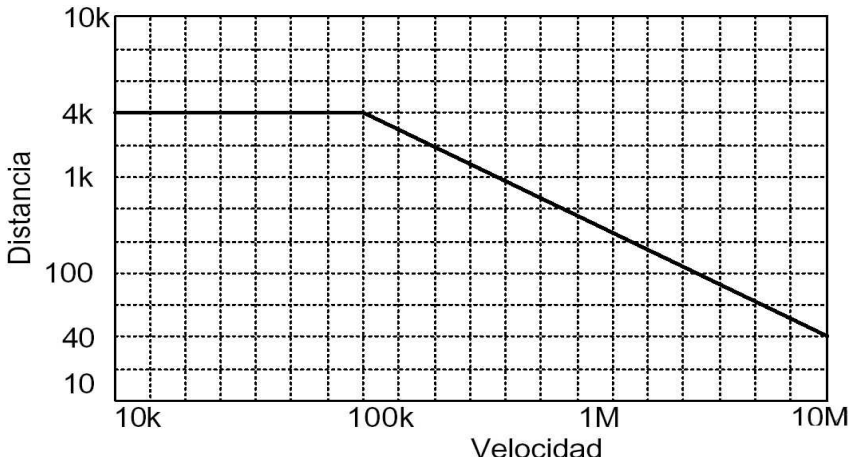
MHz	10	50	100	200	400	1000
dB/100m	4.9	12	17	26	38	65

Coaxial tipo	Capacidad (pF/m)	Velocidad propag.(%)	Vmáx (KV)	ATENUACIÓN (dB/100m) a Mhz.					
				10	50	100	200	400	1000
RG 174A/U		66	1'5	12'8	23	29'2	39'4	61	98'4
RG 122/U	101	66	1'9	5'9	14'2	23	36'1	56	95'2
RG 58 C/U	101	66	1'9	4'9	12	17	26	38	65
RFA 223/U	101	66	1'9	4'3	10	14	30	29	45
RG 223/U	101	66	1'9	3'9	9'5	15'8	23	33	54'2
RG 213 /U	101	66	5	2	4'9	7	10'5	15'5	26
RG 9 B/U	101	66	5	2'2	5'4	7'6	11'5	17'5	30
RG 21 4/U	101	66	5	2'2	5'4	7'6	10'9	17	28'9
RG 21 8/U	101	66	11	0'75	1'8	3	4'6	7	12
RG 177 /U	101	66	11	0'78	1'8	3'1	4'6	7'9	14'5

Diámetro	0.40	0.50	0.65	0.80	0.90
Ohms/Km	143	91.4	54.5	35.7	28.2

- Cables UTP
  - Categoría 1: Telefonía, transporte de voz (< 1Mbps)
  - Categoría 2: Datos hasta 4 Mbps. Token Ring a 4 Mbps.
  - Categoría 3: Datos hasta 10 Mbps. Ethernet 10base-T. 3-4 vueltas/pie.
  - Categoría 4: Token-Ring, Token-bus y 10base-T, 20MHz.
  - Categoría 5: Datos hasta 100 Mbps (Fast-Ethernet).
  - Redes 100baseT y 10baseT.
  - Hasta 100MHz
  - 3-4 vueltas/pulgada.

- Distancia máxima -> inversamente proporcional a la velocidad.



Dispersión en la fibra

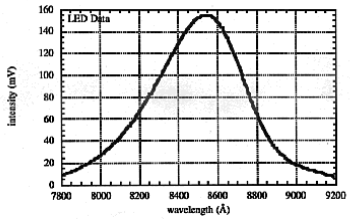
- Tipos de dispersión
  - Dispersión modal -> la luz viaja por distintos caminos (distintas longitudes) => depende de la fibra
  - Dispersión espectral -> las distintas longitudes de onda de la luz sufren distintos retardos => depende de la fuente de luz.
- Tipos de fuentes de luz
  - LED -> luz poco coherente => uso en fibras multimodo en la primera ventana
  - ILD (Injection Laser Diode) -> luz coherente => uso en fibras monomodo en la segunda y tercera ventanas.
- Detectores => fotodiodos polarizados en inverso

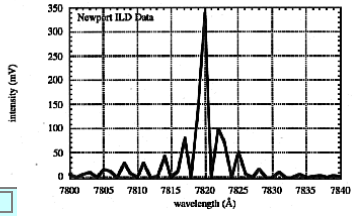
Fibra óptica

- Formado por una o varias hebras de cristal o plástico.
- Transmisión por luz infrarroja
  - Ventana de 850nm -> distancias cortas y medias
  - Ventana de 1300nm -> distancias largas, menor atenuación
  - Ventana de 1550 nm -> distancias largas, menor atenuación
- Reflexión de la luz
- Propiedades.
  - Gran ancho de banda (hasta 2Gbps)
  - Baja atenuación.
  - Inmunidad ruido electromagnético.
  - Baja potencia.
  - Poco peso y tamaño.
  - Transmisión al larga distancia (decenas de Km)
  - Necesidad de conversiones electricidad/luz

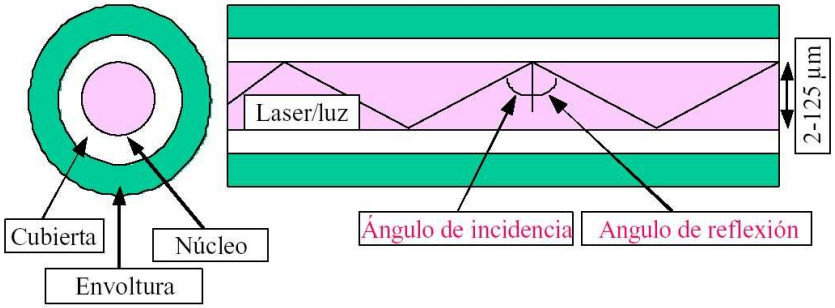
Fuentes de luz

- LED
  - Luz poco coherente => distintas velocidades de propagación.
  - Baja potencia => menor alcance
  - Bajo coste
- ILD
  - Luz mucho más coherente => menor dispersión espectral
  - Alta potencia => más alcance
  - Mayor coste





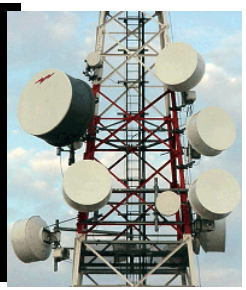
Características	LED	Laser
Ancho espectral	20-60 nm	0.5-6 nm
Corriente	50 mA	150 mA
Potencia de salida	5 mW	100 mW
Velocidad	100 MHz	2 GHz
Tiempo de vida	10,000 hrs.	50,000 hrs.
Costo	$1.00- $1500	$100 - $10000



- Angulo de incidencia menor que un cierto ángulo => reflexión
- Según la anchura del núcleo
  - Fibras multimodo (anchura del nucleo mucho mayor que la longitud de onda de la portadora) -> varios modos de propagación
  - Fibras monomodo (anchura del nucleo cercana a la longitud de onda de la portadora)-> un solo modo de propagación

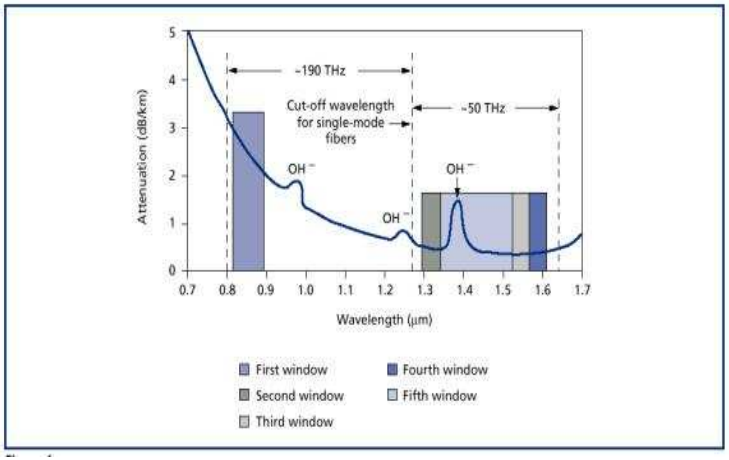
Fibra multimodo

Fibra monomodo



- Enlaces via radio -> microondas (1-40Ghz, λ=30cm-1mm)
- Propagación en línea recta hasta 30-50Km (punto a punto)
- Mucha atenuación por obstáculos => visión directa
- Antenas de tamaño varias veces λ
- Haz muy direccional: entre 1º y 5º -> parabólicas
- No son necesarios permisos para "utilizar el aire"
- Problemas con la difracción en el aire y el agua.
- Muy gran ancho de banda (mayor a mayor frecuencia)

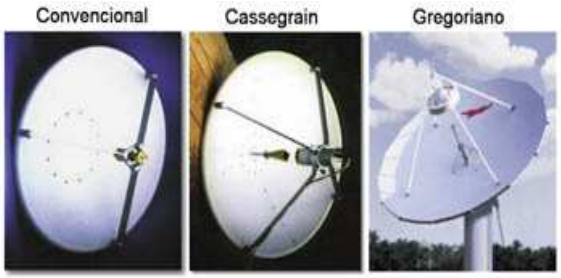
Pérdidas en la fibra



- Pérdidas -> dependen de la frecuencia de la portadora
- Segunda y tercera ventana -> menos pérdidas => transmisión a larga distancia.

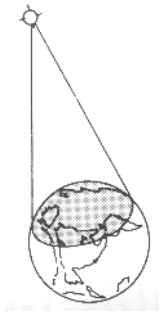
Antenas usadas en los radioenlaces

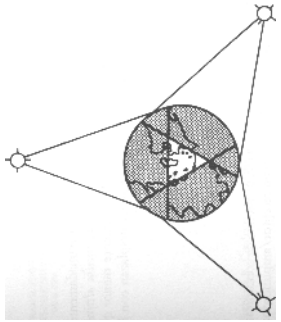
Pantalla para reducir lóbulos laterales



Transmisión por radio

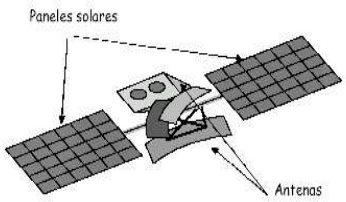
- Bandas de frecuencia VLF-UHF (aprox 50Khz – 3Ghz)
- Transmisión omnidireccional
- Antenas monopolares o dipolares ½λ – ¼λ
- Transmisión
  - Bajas frecuencias
    - Ondas terrestres -> poca atenuación por obstáculos (larga distancia)
    - Poco ancho de banda
  - Altas frecuencias
    - Ondas espaciales (propagación en línea recta) -> gran atenuación
    - Mucho mayor ancho de banda
- Usos:
  - Radiodifusión comercial (AM, FM..)
  - Televisión
  - Telefonía móvil
  - Radiocomunicación (Banda Ciudadana, 2metros,...)
  - Varios (telecontrol, telemando, telemedida, servicio móvil marítimo, radiobalizas, RLAN/WiFi, etc.)

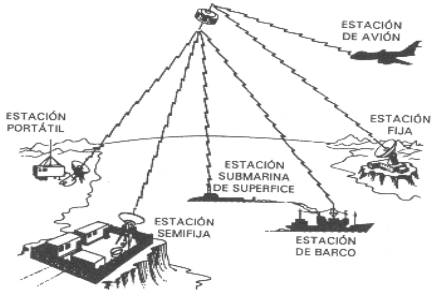




- Satélites geoestacionarios
  - Satélite mantiene altura si peso = fuerza centrífuga => velocidad
  - A 36.000Km de altura velocidad = 1 vuelta cada 24h => igual que la tierra => posición “fija”
  - Un satélite geoestacionario cubre casi la mitad de la tierra.

Transmisión por satélite





- Características
  - Eluden barreras naturales
  - Alcance todo el planeta (sin necesidad de otras infraestructuras)
  - Retardos de propagación (señal viaja 72.000km)
  - Atenuación por lluvia, nieve, etc.
  - Interferencias de radio, microoondas, etc.
  - Costes de lanzamiento muy altos, pero rentable para trasnsmisiones a muy larga distancia
  - Gran ancho de banda

- Tipos
  - Satélite pasivo
    - Refleja la señal de radio procedente de la tierra
    - Señal ascendente y descendente de la misma frecuencia
  - Satélite activo
    - Recibe la señal, la amplifica y la envía
    - Frecuencias ascendente y descendente distintas.
- Frecuencias
  - 30Mhz – 40Ghz
  - Distintas bandas para distintas aplicaciones
- Usos
  - Transmisión a larga distancia
  - GPS
  - Telefonía por satélite
  - Aplicaciones espaciales
  - Usos militares