Télécom T1

Vue d'ensemble
Introduction au cryptage,
aux codes correcteurs et à l'étalement de spectre

R. Flamary, D. Mary

9 décembre 2015

Télécommunications : Quelques dates marquantes

Technologies câblées

Télégraphe

- 1837 : Invention
- 1874 : Multiplexage

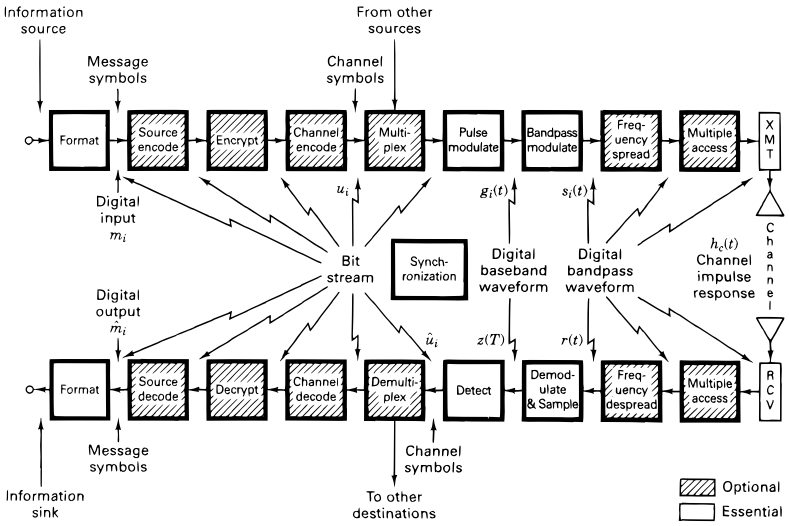
Téléphone

- 1876 : Brevet (G. Bell)
- 1880 : Premières lignes
- 1920 : Multiplexage
- 1920 : Commutation automatique
- 1966 : Techniques numériques
- 2000 : Téléphonie sur IP
- 2003 : Skype

Communications Hertziennes

- 1895 : Liaison radio (Marconi)
- 1897 : Radio en morse
- 1920 : Radiodiffusion
- 1935 : Télévision
- 1950 : Radio large bande (FM)
- 1955 : Radiotéléphone
- 1960 : Télévision couleur
- 1992 : Télévision par satellite
  Radiotéléphone numérique 2G
- 1994 : Bluetooth
- 1999 : Wifi
- 2005 : Radiotéléphone 3G
- 2011 : Radiotéléphone 4G

Modèle de la chaine de transmission



©*Digital Communications*, B Sklar, Prentice Hall

Plan du cours

Introduction, vision d'ensemble

Formatage, Codage de source

Cryptage
- Historique
- Cryptage symétrique (César, DES, AES)
- Cryptage asymétrique à clé publique (RSA, PGP)

Codage canal, codes correcteurs
- Détection et correction d'erreurs
- Codage par bloc et codage convolutif

Multiplexage

Mise en forme des impulsions

Modulation passe-bande

Étalement de spectre
- Robustesse au bruit localisé en fréquence (DS, FH)
- Applications (ADSL, Wifi)

Accés Multiples

Numérique VS Analogique

Communication numérique

- Données à transmettre décomposées en un ensemble de messages (composés de symboles) VS continuum en analogique.
- But du récepteur : déterminer quels symboles on été émis VS retrouver une forme d'onde en analogique.

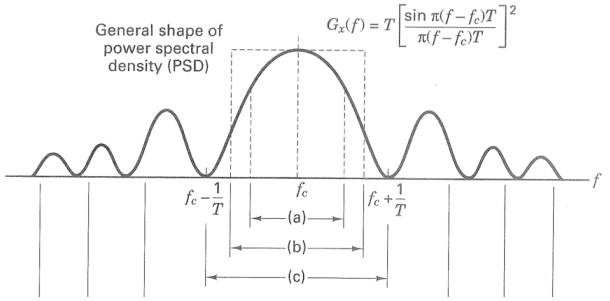
Avantages

- Signaux associés à des formes connues (résistance au bruit).
- Simplicité (format binaire pour tout type de données)
- Compatibilité entre systèmes informatiques.

Inconvénients

- Synchronisation nécessaire.
- Chute abrupte de SNR (Bit Error Rate).

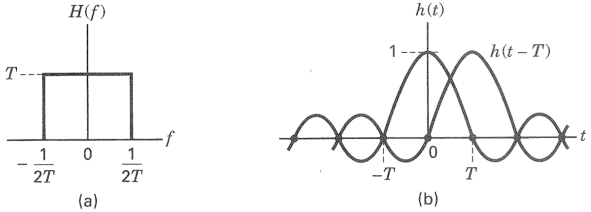
Rappels (1)



Largeur de bande W d'un signal

- $G_x(f)$ est la DSP du signal, f_c la fréquence de la porteuse.
- On prendra dans ce cours W = largeur entre le max et le premier zéro.
- Plusieurs définitions possibles pour la largeur de bande.
- Pour les pulses non rectangulaires, on a $W > \frac{1}{T}$.

Rappels (2)



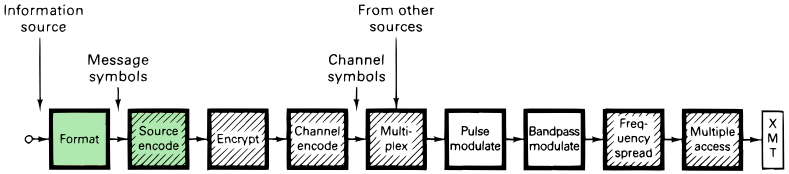
Contrainte de Nyquist

- Si les pulses sont des **sinc** de longueur infinie et espacés de T, il n'y a pas d'interférence inter-symboles (ISI).
- La largeur de bande est $W = \frac{1}{2T}$ et le débit $R_s = \frac{1}{T}$ en symb/sec .
- Contrainte de Nyquist pour qu'il n'y ai pas d'ISI :

$$\text{Bande disponible} > \frac{R_s}{2}$$

- En pratique on n'utilise pas de pulses infinis et on a $W > \frac{1}{2T}$.

Formatage et codage de source



- Le **formatage** permet de passer d'une représentation analogique à une représentation numérique.
- Le **codage de source** vise à réduire la redondance du signal pour économiser la mémoire, le débit et la largeur de bande lors de la transmission.
- La compression effectuée lors du codage de source aboutit à une liste de symboles qui représentent le signal de manière indirecte.

Formatage

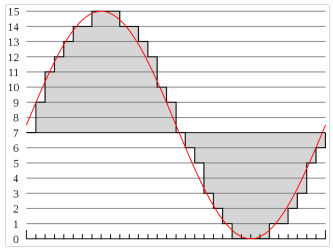
Sources discrètes

- Transformation des données en symboles binaires via un code.
- Exemple : ASCII

Code	...0	...1	...2	...3	...4	...5	...6	...7	...8	...9	...A	...B	...C	...D	...E	...F
0...	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
1...	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2...	SP	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
3...	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4...	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5...	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6...	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7...	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	DEL

Sources analogiques

- Échantillonnage spatial/temporel.
- Quantification en amplitude
- Exemple : PCM



Codage de source (1)

Principe

- Éliminer les redondances apparaissant naturellement dans des données *naturelles*.
- Économiser le débit.
- Deux types de compressions : sans perte (**lossless**) ou avec perte (**lossy**).

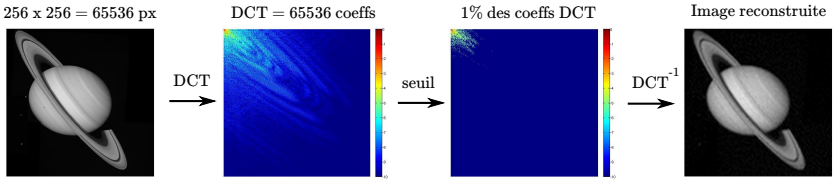
Codage sans perte

- Huffman.
- Lempel-Ziv (gzip,gif).
- Deflate (zip,png)

Codage avec perte

- Quantification non-uniforme (log,..).
- Differential pulse-code modulation, linear prediction.
- Quantification vectorielle (par bloc).
- Codage par transformée (DCT, ondelettes).

Codage de source (2)



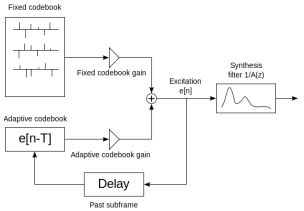
Codage avec perte : JPEG

- Transformation de l'image par DCT (Tranf. cosinus discrete).
- Seuillage des petits coefficients.
- Stockage des valeurs et des positions des coefficients restants.
- La reconstruction se fait en appliquant une DCT inverse sur les coefficients parcimonieux.

Codage de source (3)

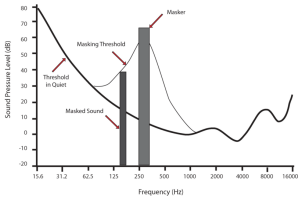
Codeur pour la téléphonie mobile

- Utilisent souvent des prédicteurs linéaires.
- Codeur CELP (Code-excited linear prediction).
- Utilisé également dans la norme MPEG-4.

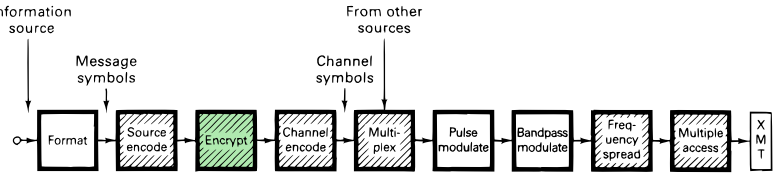


Codeur audio mp3

- Utilisation de transformées (DCT).
- Seuillage utilisant des critères psychoaccoustique.
- Principe : pas besoin d'encoder ce qui n'est pas perçu par un être humain.



Cryptage (1)



Le cryptage (ou chiffrement) est mis en oeuvre dans deux cadres d'utilisation :

- **Confidentialité** contre les attaques passives.
- **Authentification** contre les attaques actives.

On distingue deux types de cryptage

- **Symétrique** une clé unique (et partagée) permet de crypter est de décrypter le message.
- **Asymétrique ou à clé publique** le cryptage et décryptage se font avec des clés différentes.

Cryptage (2)

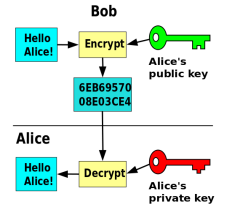
Historique

Période artisanale

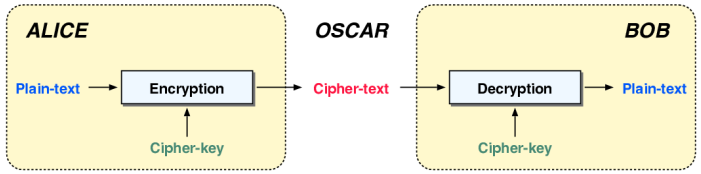
- Stéganographie (pas du cryptage).
- Scytale (Grecs anciens).
- Chiffre de César.
- 1553 : Chiffre de Vigenère.
- 1920 : Enigma.

Cryptographie Moderne

- 1977 : Data encryption Standard (DES).
- 1998 : Advanced Encryption Standard (AES).
- 1976 : Cryptage par clés publiques (W. Diffie and M. Hellman).
- 1978 : RSA Algorithm.
- 1991 : Pretty Good Privacy (PGP).



Cryptage (3)



Définitions

- Ci-dessus exemple de cryptage symétrique.
- Cryptage sûr sans condition ou opérationellement (difficile à décrypter).
- Cryptage par bloc ou par flot. Possibilité de transformer un cryptage par bloc en cryptage par flot.

Attaques

- **Cypher text only** accès uniquement au texte crypté.
- **Known plain text** accès à des exemples de textes connus cryptés.
- **Chosen text attack** provoque le cryptage d'un texte choisi.

Cryptage (4)

Exemples de cryptage par flot

Méthodes de substitution :

- **César** Décalage de l'alphabet d'un nombre définit par la clé K.
- **Trithemius** On commence avec un décalage de 1 vers la droite et on incrémente le décalage à chaque lettre (K=BCDEFG...).
- **Vigenère** Le décalage est décidé par une clé définie à priori. Plus la clé est longue, plus de code est sûr.
  Variantes : utilisation du texte brut ou du texte crypté dans la clé.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Cryptage (5)

Mise en oeuvre des cryptages

César (K=B)

```
Texte :  N O W I S T H E T I M E
Clé :    B B B B B B B B B B B B
Chiffre:
```

Trythemius

```
Texte :  N O W I S T H E T I M E
Clé :    B C D E F G H I J K L M
Chiffre:
```

Vigenère 1 (K=TYPE)

```
Texte :  N O W I S T H E T I M E
Clé :    T Y P E T Y P E T Y P E
Chiffre:
```

Vigenère 2 auto-plain key (K=F...)

```
Texte :  N O W I S T H E T I M E
Clé :    F N O W I S T H E T I M
Chiffre:
```

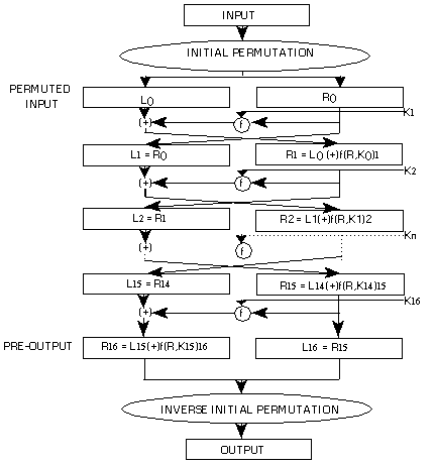
Vigenère 3 auto-cipher key (K=F...)

```
Texte :  N O W I S T H E T I M E
Clé :    F
Chiffre:
```


Cryptage (6)

Data Encryption System (DES)

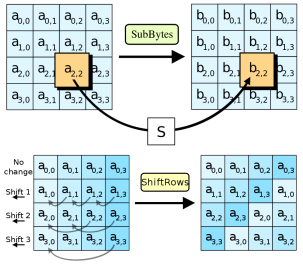
- Utilise une clé de 56 bits pour crypter des blocs de 64 bits.
- Commence par une permutation initiale et se termine par la permutation inverse.
- la transformation suivante est effectuée 16 fois :
  - Une sous-clé de 48 bits est générée.
  - Les données sous découpées en deux blocs.
  - Les blocs sont échangés en suivant un schéma de Feistel.
  - Le bloc de poid fort subit une tranfo. f.
- Cryptage considéré comme non-sûr car peut être craqué en quelques jours.



Cryptage (7)

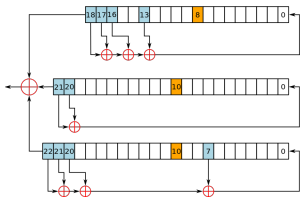
Advanced Encryption Standard (AES)

- Standard depuis 2001.
- basé sur le Rijndael (J. Daemen and V. Rijmen).
- basé sur des substitutions/permutations.
- Blocs de 128 bits et une clé de 128, 192 ou 256 bits.
- Plus rapide que le DES.

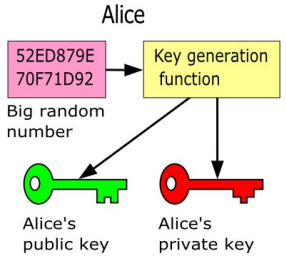


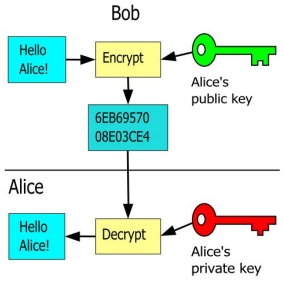
Autres algorithmes

- **A5** Communications GSM.
- **RC4** Protocole WEP du Wifi.
- **Py** Bluetooth



Cryptage (8)





Principe du cryptage à clé publique

- Chaque utilisateur a deux clés, une privée et une publique.
- Pour transmettre un message à Alice, Bob utilise la clé publique d'Alice.
- Alice peut décrypter le message en utilisant sa clé privée.
- Retrouver le message M à partir de la clé publique doit être une opération complexe.
- Exemple : RSA dont l'article a également introduit Alice et Bob.

Cryptage (9)

RSA

- Introduit en 1977 par R. Rivest, A. Shamir, and L. Adleman.
- Basé sur le fait que la factorisation du produit de deux grands nombres premiers est un problème difficile.
- Nécessite 2 clés :
  - (n, e) clé de cryptage publique.
  - (n, d) clé de décryptage privée.
- Cryptage :

$$c \equiv m^e \mod n$$

- Décryptage :

$$m \equiv c^d \mod n$$

Remarques

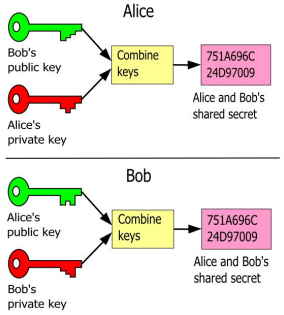
- Nécessite la génération de deux grands nombres premiers pour obtenir e, d et n.
- Nombres premiers obtenus à l'aide de tests de primalité probabilistes.
- Test de primalité de Fermat : Si p est premier et a est premier avec p alors

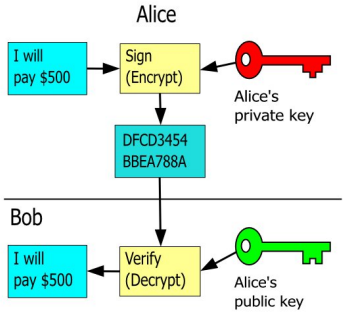
$$a^{p-1} \equiv 1 \mod p$$

- Le nombre p est donc probablement premier si il vérifie cette condition pour un certain nombre de a.
- PGP considère qu'on nombre x est premier si

$$1 \equiv 2^{x-1} \equiv 3^{x-1} \equiv 5^{x-1} \equiv 7^{x-1} \mod x$$

Cryptage (10)

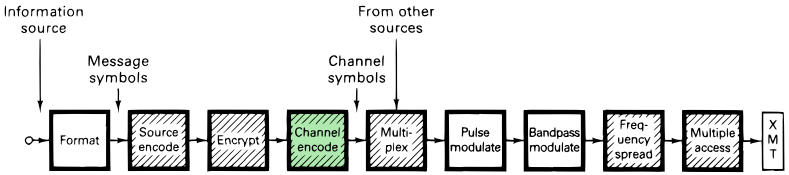




Pretty Good Privacy (PGP)

- RSA trop complexe pour crypter de long messages.
- Astuce de PGP : utiliser une cryptage symétrique pour le message et transférer la clé en utilisant RSA.
- OpenPGP est un standard décrivant le transfert et le cryptage de mail en utilisant ce format.
- Possibilité d'avoir un secret partagé en combinant les clés publiques/privée.
- Signature d'E-mail assurant l'authentification.

Codes correcteurs (1)



- Le but du codage canal est d'introduire de la redondance pour que le signal soit plus résistant aux *défauts* du canal.
- Défauts : bruit, interférences, atténuations.
- La redondance augmente le nombre de bits transmis (coût).
- Détection et correction d'erreurs de transmission.
- Deux type d'approches : **codeur d'onde** et **codeur structuré** (codeur de symboles).

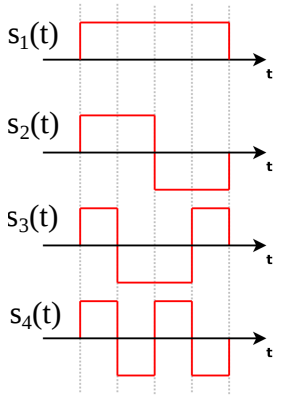
Codes correcteurs (2)

Codeur d'onde (waveform coder)

- Choisir des formes d'onde plus robustes pour minimiser les erreurs de détection.
- Exemples : codes orthogonaux, codes bi-orthogonaux ou transorthogonaux.

Exemple

- Alphabet $M = 4$ symboles. Nb e bits par unité de temps $k = 2$.
- Chaque symbole est codé par un signal $s_i(t)$.
- Le décodage se fait en corrélant le signal reçu avec chacun des $s_i(t)$.
- Corrélation nulle en $s_i(t)$ et $s_j(t)$ si $i \neq j$.
- Codes augmentant la bande passante.
- Synchronisation nécessaire.



Codes correcteurs (3)

Codeur structuré

On ne travaille plus sur les ondes mais sur les symboles. On introduit des dépendances (de la **redondance**).

Objectifs

- **Détection d'erreurs** pour pouvoir redemander un envoi des données.
- **Détection et correction d'erreurs** pour réparer les erreurs et éviter un renvoi des données (Forward Error Correction, FEC).
- Il faut trouver le compromis redondance/efficacité (bande-passante/SNR).

Exemple de transmission (numéro de téléphone)

$$06\,01\,80\,30\,12 \quad \longrightarrow \quad 06\,01\,82\,30\,15$$

zéro six zéro un quatre-vingt trente douze → zaro six zéro un wuatze vings trents doize

Le second code est clairement plus robuste aux erreurs de transmission.
Alphabet Phonétique de l'OTAN (alpha,bravo,charlie,delta,echo,...,zulu).

Codes correcteurs (4)

Types de codes structurés

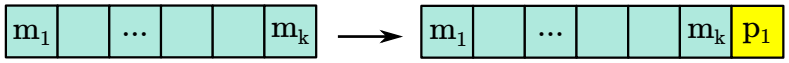
- Codes par bloc.
- Codes convolutifs.
- Turbo-codes.

Codes par bloc

- Les données sont traitées par bloc.
- Le code est caractérisé par (n, k) où
  - k est la taille d'un bloc en entrée du codeur.
  - n est la taille d'un bloc après codage.
- $(n - k)$ bits de redondance ou de parité sont ajoutés.
- Le taux du code (code rate) est définit comme :

$$r = \frac{k}{n}$$

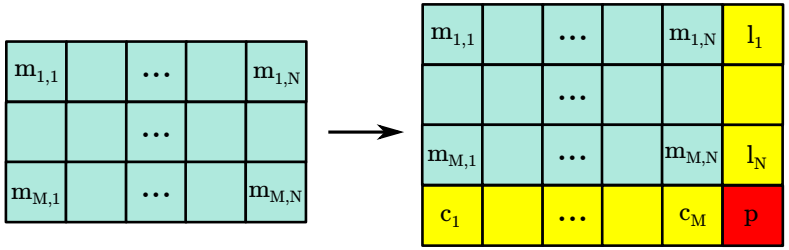
Codes correcteurs (5)



Single Parity Check code

- Ajout d'un bit de parité à la droite du message.
- Code $(k + 1, k)$ avec $p_1 = m_1 \oplus \cdots \oplus m_k$ ($\oplus$ ou exclusif).
- Détection d'erreur :
- Correction d'erreurs :

Codes correcteurs (6)



Double Parity Check code

- On groupe les bits dans une matrice de taille $M \times N$.
- On ajoute un bit de parité c_i par colonne, un bit de parité l_i par ligne et un bit de parité pour la somme des c_i ou l_i.
- Code $((N + 1)(M + 1), MN)$ avec $c_k = m_{1,k} \oplus \cdots \oplus m_{M,k}$.
- Détection d'erreur :
- Correction d'erreurs :

Codes correcteurs (7)

Exemple Single parity check

- $k = 5$, signal : 01010 00111
- On transmet : 01010 0 00111 1

Exemple Double parity check

- $M = 5, N = 5$, signal : 10011 00011 11000 00001 10101
- Signal en matrice :

$$\begin{matrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{matrix} \longrightarrow$$

- Taux du code $r =$

Codes correcteurs (8)

Linear block code

- Soit $\mathbf{m}$ le message à coder (vecteur colonne de dimension k) et $\mathbf{u}$ le message codé (dimension n).
- Le codage se fait par la multiplication matricielle binaire

$$\mathbf{u} = \mathbf{G}\mathbf{m}$$

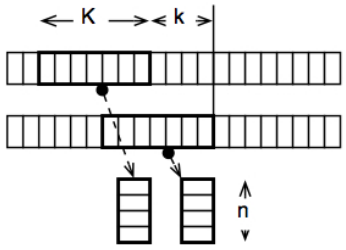
  où $\mathbf{G}$ est une matrice de transformation.
- Si les colonnes de $\mathbf{G}$ sont orthogonales, alors on a un code orthogonal.
- Les codes linéaires sont une généralisation des single et double parity check codes.
- Exemple le code de SPCC(5,4)

$$\mathbf{G} :=$$

Codes correcteurs (9)

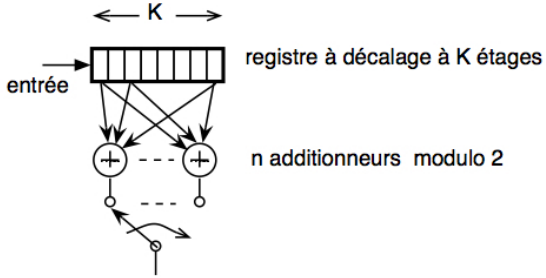
Codage convolutif

- Le signal codé est la sortie de n filtres linéaires (modulo 2).
- Basé sur une fenêtre glissante de taille K (filtre FIR).
- La fenêtre avance de k à chaque itération.



- Chaque itération peut être vue comme un codage linéaire par bloc sur la fenêtre glissante.
- Possibilité d'avoir des filtres récursifs (turbocodes).
- Code rate $r =$

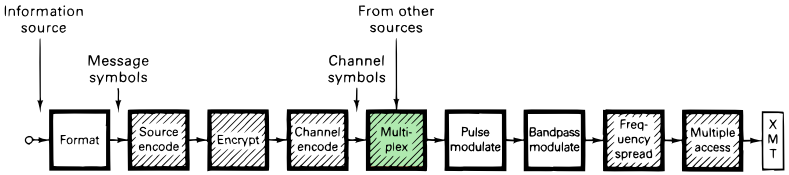
Codes correcteurs (10)



Codage convolutif avec $k = 1$

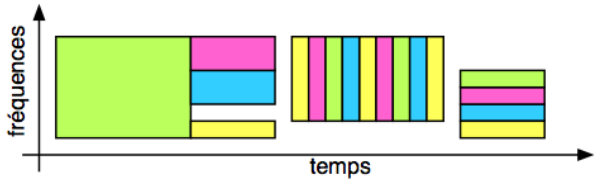
- On prend souvent $k = 1$.
- Décodage effectué en utilisant l'algorithme de Viterbi.
- Codes convolutifs plus utilisés ces dernières années car supérieurs aux codes par block pour une complexité équivalente.
- Communications satellite, Reed-Solomon, turbocodes.

Multiplexage (1)



- Un système de transmission utilise un certain nombre de ressources : l'espace, le temps, les fréquences la polarisation du champ électrique, et les codes.
- Le multiplexage permet de répartir des signaux de sources différentes sur les même ressources.
- Plusieurs facettes de ce problème :
  - Duplexage et multiplexage (statique).
  - Accès multiples (dynamiques).

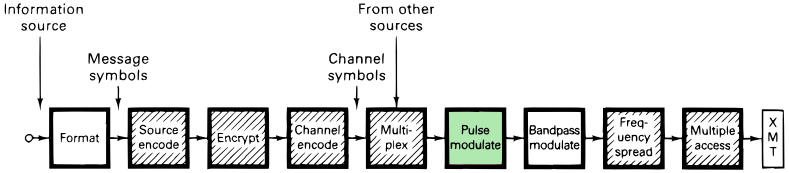
Multiplexage (2)



- Partage des ressources entre plusieurs utilisateurs (couleurs différentes)
- Il existe trois types principaux de multiplexage
  - Multiplexage fréquentiel (**FDM**).
  - Multiplexage temporel (**TDM**).
  - Multiplexage par codes orthogonaux (**CDM**).

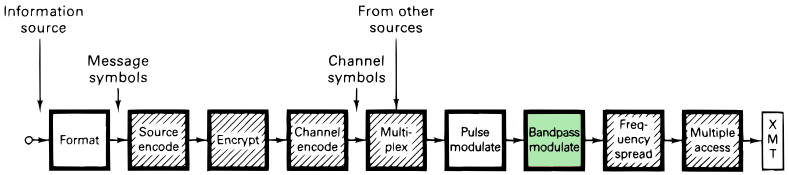
  Chacunes de ces approches est utilisé dans le cadre des accés multiples (FDMA,TDMA,CDMA).
- Il est également possible d'utiliser :
  - La directivité spatialle des antennes (SD).
  - Polarisation verticale ou horizontale des ondes (Ciné 3D).

Mise en forme des impulsions



- Codage du signal en bande de base.
- Permet de véhiculer des signaux physiques sur des canaux filaires courants (coax.,paire cuivre,...).
- Le codage doit minimiser les interférences inter-symboles (ISI) après réception.
- Le signal après codage occupe toujours une largeur de bande similaire à la bande de base.

Modulation passe-bande (1)

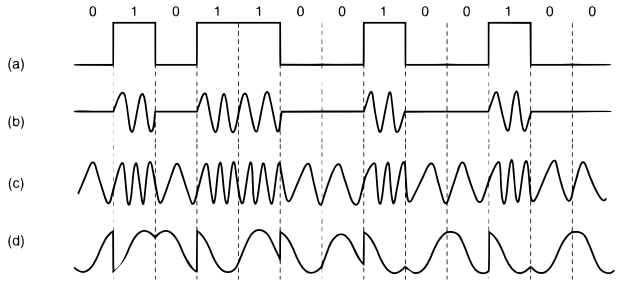


- Selon les caractéristiques physique et légales du canal, on transmet le signal dans une bande de fréquence déterminée.
- Le but de la modulation passe-bande est de décaler le signal de la bande de base à la bande passante autorisée (centrée en f_0).
- f_0 est la fréquence de la porteuse.
- La modulation passe-bande revient toujours à transmettre un signal sinusoidal du type :

$$s(t) = A(t)\cos(\Phi(t))$$

- Les symboles à transmettre peuvent être binaires ou M-aires (M symboles possibles).

Modulation passe-bande (2)

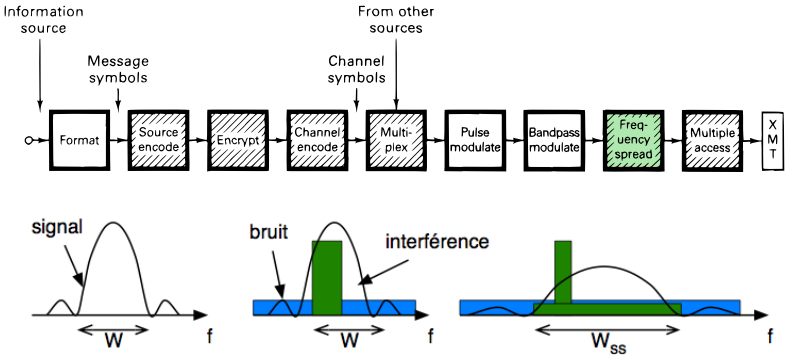


Exemples de modulation binaire

- **(a)** Signal binaire : $b(t)$
- **(b)** Amplitude Shift Keying (ASK) : $s(t) = b(t)\cos(2\pi f_0 t + \phi)$
- **(c)** Frequency Shift Keying (FSK) : $s(t) = \cos(2\pi f_0(t + \int_{-\infty}^{t} b(u)du) + \phi)$
- **(d)** Phase Shift Keying (PSK) : $s(t) = \cos(2\pi f_0 t + \phi_0 b(t))$

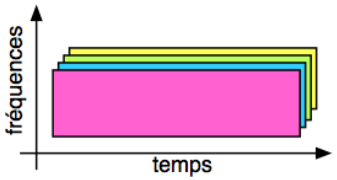
Pour les modulations M-aires, on peut combiner plusieurs approches (MPSK,APK, QAM).

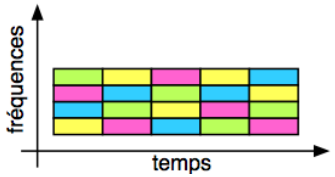
Étalement de spectre (1)



- Méthode visant à rendre la transmission plus robuste aux bruits localisés en fréquence (résistance au **jamming**).
- On élargit le spectre du signal transmis de W autour de f_0 à $W_{ss} \gg W$.
- Utilisé également pour les accès multiples avec une séquence pseudo-aléatoire.

Étalement de spectre (2)





Direct Sequence SS (DSSS)

- Étalement du spectre par séquence directe.
- Tous les utilisateurs utilisent toutes les fréquences.

Frequency Hoping SS (FHSS)

- Inventé par Hedy Lamarr en 1942.
- Chaque utilisateurs change de fréquence rapidement (hop) au cours du temps.

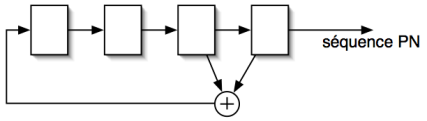
Les deux techniques reposent sur l'utilisation de **séquences pseudoaléatoires**.

Étalement de spectre (3)

Séquence pseudo-aléatoire

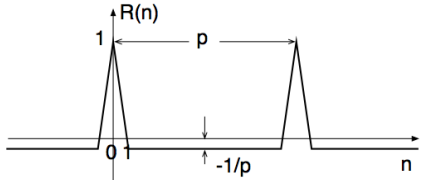
- Les séquences PN (Pseudo-Noise) ou SBPA (séquences binaires pseudoaléatoires) sont obtenues en rebouclant un registre à décalage à n étages incluant un (ou des) additionneur(s) modulo 2.
- La sortie ressemble à une suite aléatoire mais elle est périodique (séquences pseudo-aléatoires).
- Séquences de longueur maximale de période $p = 2^n - 1$ pour n étages

Exemple pour $n = 4$



- Calculer la séquence pour l'état initial 1000 (utiliser un tableau).
- Séquence : 0001
- Longueur de la séquence :

Étalement de spectre (4)



Propriétés des séquences pseudo-aléatoire

- On cherche une séquence la plus aléatoire (« blanche ») possible : son autocorrélation doit être proche d'un Dirac.
- En binaire l'autocorrélation d'une séquence PN $s(n)$ est définie comme

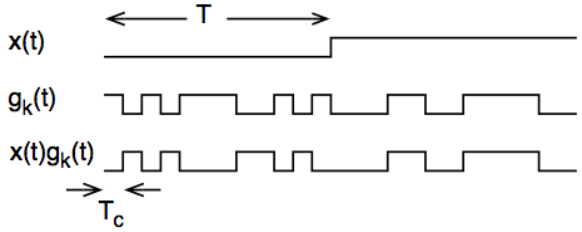
$$R(n) = \frac{\text{nb d'accords} - \text{nb de désaccords}}{p}$$

  sur une période p et un décalage de n.
- Il existe de nombreux type de générateurs aléatoires (Gold codes, Barker).

Exemple pour $n = 4$

- Calculer $R(0)$ et $R(1)$ pour l'exemple précédent.

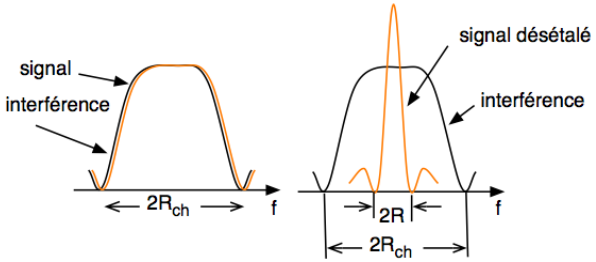
Étalement de spectre (5)



Étalement de spectre par séquence directe (DS)

- Un utilisateur k a une séquence aléatoire $g_k(t)$.
- La séquence est utilisées pour modifier le signal $x(t)$ à transmettre.
- T_c est la période d'un *chip*, c'est à dire un bit du signal aléatoire ($T_c \ll T$).
- Le décodage se fait en modifiant le signal reçu à l'aide de $g_k(t)$.
- Si les codes $g_k(t)$ sont orthogonaux alors les contribution des autres utilisateurs tendent à s'annuler.

Étalement de spectre (6)



Interprétation fréquentielle et gain du DS

- Les autres utilisateurs apparaissent comme du bruit (des interférences).
- Gain d'un étalement de spectre

$$G = \frac{\text{Rapport signal/interférences avec DS}}{\text{Rapport signal/interférences sans DS}} = \frac{R_{ch}}{R} = \frac{T}{T_c}$$

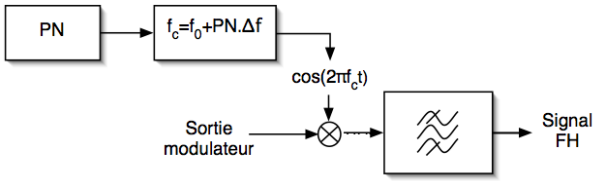
- $R = \frac{1}{T}$ est le *data rate* et $R_{ch} = \frac{1}{T_c}$ est le *chip rate*.

Étalement de spectre (7)

Exemple de séquençage direct DS/BPSK

$x(t)$	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	Données à transmettre
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
$g(t)$	0	1	0	1	0	0	0	1	1	0	1	0	1	1	1	0	Séquence aléatoire
	0	1	1	0	0	0	1	1									
$x(t)g(t)$	1	0	1	0	1	1	1	0	0	1	0	1	1	1	1	0	Séquence à transmettre
	0	1	1	0	0	0	1	1									
$\theta_x + \theta_g$	π	0	π	0	π	π	π	0	0	π	0	π	π	π	π	0	Phase du BPSK
	0	π	π	π	π	0	0	π									
$\hat{\theta}_g$	0	π	0	π	0	0	0	π	π	0	π	0	π	π	π	0	Saut de phase au receveur
	0	π	π	π	π	0	0	π									
$\hat{\theta}_x$	π	π	π	π	π	π	π	π	π	π	π	π	0	0	0	0	Phase après déséquençage
	0	0	0	0	0	0	0	0									
$\hat{x}(t)$	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	Signal reconstruit
	0	0	0	0	0	0	0	0									

Étalement de spectre (8)



Étalement par saut de fréquence (FH)

- Consiste à changer la fréquence de la porteuse f_0 (hopping).
- Souvent associé à une modulation MFSK. la fréquence du signal dépendra donc à la fois du symbole et de la valeur du générateur aléatoire.
- La bande résultante W_{ss} prend en compte la fréquence du modulateur MFSK, Δf (distance min entre les sauts) et le nombre de bit en sortie du générateur aléatoire.
- Par analogie avec le DS, on appelle T_c en FH la durée de la plus petite forme d'onde ininterrompue.

Étalement de spectre (9)

Propriétés de l'étalement par saut de fréquence (FH)

- Gain du Frequency Hopping

$$G = \frac{\text{Rapport signal/interférences avec FH}}{\text{Rapport signal/interférences sans FH}} = \frac{W_{ss}}{R}$$

- On distingue deux types de FH :
  - **Fast Frequency Hopping (FFH)** La fréquence de la porteuse saute plusieurs fois pendant la durée de transmission d'un symbole (symbole codé sur plusieurs fréquences). On a donc $T_c < T$.
  - **Slow Frequency Hopping (SFH)** Il n'a a pas de saut en fréquence (hop) pendant la durée de transmission d'un symbole. On a donc $T_c \geq T$.
- En pratique le FH permet un étalement sur une bande de plusieurs Ghz, soit environ 10 fois plus que le DS (meilleur gain).

Étalement de spectre (10)

Exemple pour une modulation MFSK

- $M = 8$ avec 8 fréquences séparées de 50Hz,
- Data rate $R = 150$bits/s, Symbole Rate $R_s =$

MFSK Classique

Sym.	Fréquence
000	$f_1 = f_0 - 175$ Hz
001	$f_2 = f_0 - 125$ Hz
010	$f_3 = f_0 - 75$ Hz
011	$f_4 = f_0 - 25$ Hz
100	$f_5 = f_0 + 25$ Hz
101	$f_6 = f_0 + 75$ Hz
110	$f_7 = f_0 + 125$ Hz
111	$f_8 = f_0 + 175$ Hz

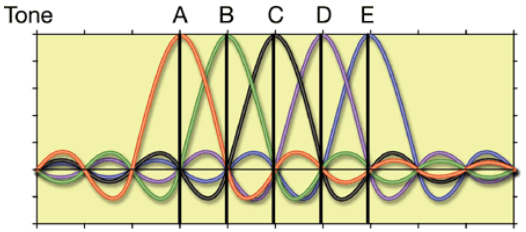
Exemple

- $f_0 = 3$KHz, Sym.=111
- $f =$

SFH/MFSK

- f_0 saute à chaque symbole.
- $W_{ss} = 400$MHz, $\Delta f = 100$Hz.
- Nombre de fréquences : $4 * 10^6$, Codées sur :
- À chaque symbole le PN génère un mot aléatoire par exemple :
  - $f_0 = f_s + PN\Delta f = 832.212\,000$MHz.
  - La fréquence finale est attribuée commme en MFSK.
  - Pour le symbole 111 :
  - $f =$ MHz

Étalement de spectre (11)



Modulation multiporteuse

- Sur une large bande W_{ss} les caractéristiques du canal peuvent varier selon la fréquence (dispersion temporelle, atténuation).
- La modulation multi-porteuse consiste à diviser la bande totale W_{ss} en N sous-bandes. Les données sont découpées en N paquets chacun transmis parmi une des sous-bandes.
- Cas particulier : les fréquences des canaux sont choisies de manière à avoir un impact nul sur les autres canaux (Orthogonal frequency-division multiplexing OFDM).
- Applications : ADSL, Wifi.

Exemples d'étalement de spectre (1)

Communication Sans-fil Wifi

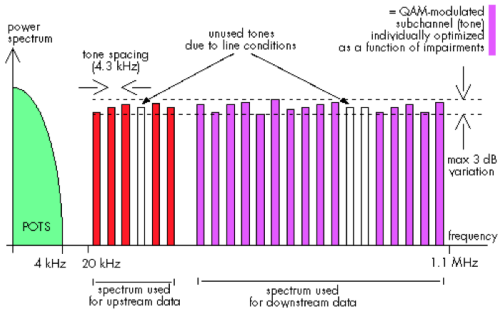
802.11 DSSS

- Débits de 1 et 2 Mbps, modulations BPSK et QPSK.
- Étalement de spectre (par code Barker).
- 14 canaux se recouvrant, de 22 Mhz chacun, de 2,401 à 2,483 Ghz
- Limites de puissance : 1000 mW aux USA, 100 mW en Europe, 20 mW au Japon

802.11 FHSS

- Débits de 1 et 2 Mbps.
- Modulation GFSK (Gaussian Frequency Shift Keying) : FSK avec préfiltrage des pulses pour limiter la bande sur chaque canal
- 79 canaux de 2,402 à 2,480 GHz, 78 séquences de sauts de 6 MHz.
- Taux de saut minimum : 2,5 sauts/seconde
- Tolérance aux interférences (et propagations multiples), faible portée (limité à 10 mW).

Exemples d'étalement de spectre (2)



Asymetric Digital Subscriber Line (ADSL)

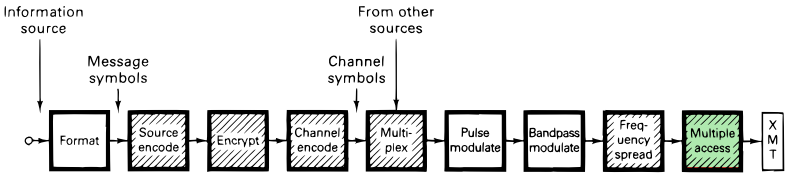
- Fréquences : $0 - 1.104$Mhz divisé en 256 sous canaux espacés de 4.3125kHz
  - Canaux 1-6 utilisés pour le téléphone.
  - Canaux 7-31 : flux montant (upload).
  - Canaux 33-256 : flux descendant (download).
- Pour chaque canal on mesure le RSB, le nombre de symboles $M < 256$ pour le QAM-OFDM est choisi de manière à avoir un Bit-Error-Rate constant.
- Codage canal correcteur : codes de Reed-Solomon.
- L'ADSL 2+ exploite la bande jusqu'à 2,2 MHz

Exemples d'étalement de spectre (3)

ADSL : calcul de débit

- En une période symbole T, si $N = 40$ sous-porteuses sont utilisées, on reçoit N symboles.
- Si tous les canaux ont une qualité telle que $M = 2^8 = 256$ et donc QAM de $b = 8$ bits par symboles alors une **trame** vaut $N * b =$ bits.
- Chaque sous-porteuse est modulée à 4000sym/s. On a donc 4000 trames par secondes. Débit brut :
- Débit brut contenant des redondances, débit utile moindre.
- Toutes les 68 trames est envoyée une trame de contrôle (pour la synchro). Ces 69 trames $=$ 1 supertrame.
- Débit Max théorique :
  - 15bits/sym sur toutes les $N_{max} = 223$ sous-porteuses (sous-porteuses 32 à 255 moins la sous-porteuse pilote 64).
  - $R = 15 * 4000 * 223 =$ kbits/sec

Accés Multiples (1)



- Multiplexage dynamique. Gestion d'un nombre d'utilisateur qui varie dans le temps.
- 3 types principaux d'accès multiples
  - **Frequency Divided Multiple Access (FDMA)**, chacun sa fréquence.
  - **Time Divided Multiple Access (TDMA)**, chacun son tour.
  - **Code Divided Multiple Access (CDMA)**, chacun son code.

Accés Multiples (2)

Frequency Divided Multiple Access (FDMA)

- Multiplexage fréquentiel dynamique.
- Chaque utilisateur a sa bande de fréquence.
- N utilisateurs, $\rightarrow$ 2N fréquences.
- Exemple : voix en GSM.

Avantages

- Transmission continue.
- Faible largeur de bande par utilisateur.
- Faible complexité du terminal mobile.

Inconvénients

- Coût élevé : 1 canal par porteuse.
- Nécessite un duplexeur.
- Complexité du handover (changement de stations).

Accés Multiples (3)

Time Divided Multiple Access (TDMA)

- Multiplexage temporel dynamique. Temps divisé en $\ll$ time slots $\gg$.
- Les utilisateurs utilisent le canal chacun leur tour.
- On appelle $\ll$ trame $\gg$ le séquencement et l'organisation de l'accès à la ressource par les divers utilisateurs. Transmission par salves (**burts**).
- Il est nécessaire de réserver un $\ll$ temps de garde $\gg$ pour tenir compte des temps de propagation (3.10^8 m/s en espace libre).
- L'avance en temps permet de réduire le temps de garde, Elle nécessite la mesure des temps de propagation.

Avantages

- Équipement moins coûteux que FDMA (moins de canaux).
- Pas de duplexeur (émet ou reçoit, pas les 2 en même temps).
- Handover plus simple qu'en FDMA.

Inconvénients

- Trajets multiples (ISI $>$ FDMA).
- Synchronisation (avance en temps)
- Entête important (séquence apprentissage).
- Complexité des trames.

Accés Multiples (4)

Code Divided Multiple Access (CDMA)

- Étalement de spectres à l'aide d'un code.
- Chaque utilisateur a un code $g_i(t)$
  - **FFH-CDMA** le code contrôle les sauts de fréquence.
  - **DSSS-CDMA** le code est la séquence directe pour l'étalement.

DSSS-CDMA

- Signal d'un utilisateur $e_i(t) = v_i(t)c_i(t)$
- Signal sur le canal partagé $s(t) = \sum_i e_i(t)$
- À la réception on multiplie par le code $c_i(t)$.
- On obtient $r_i(t) = v_i(t) + n(t)$ où $n(t)$ est un bruit large bande provoqué par les autres utilisateurs.

FFH-CDMA

- Basé sur le FDMA et le FH.
- Pendant 1 T_c, c'est du FDMA.
- Les sauts de la porteuse de chaque utilisateur varient suivant un code (comme en FH).
- Code conçus pour éviter les collisions de porteuses.

Ressources bibliographiques

- *Digital Communications, Fundamentals and Applications*, B. Sklar, Prentice Hall, 2003.
- *Télécom T1, Vue d'ensemble, Introduction au cryptage, aux codes correcteurs et à l'étalement de spectre*, D. Mary, Université de Nice, 2011.
- *Histoire des codes secrets*, S. Singh, Le Livre de Poche, 2001.