M1 - Télécom T1 TD 1

Rémi Flamary

Exercice 1 Culture générale

1. a) Quelle est la différence fondamentale entre les communications numériques et les communications analogiques ?
   b) Quels sont les principaux avantages et inconvénients des communications numériques par rapport aux communications analogiques ?
2. **Modulation en bande de base**
   a) Qu'appelle-t-on la modulation en bande de base ?
   b) Qu'est-ce qui différencie entre eux les codes PCM ? Donner deux exemples de codes PCM.
3. **Codage de source**
   a) Montrer l'intérêt du codage de source en vous appuyant sur l'exemple de JPEG ou de MPEG. En quoi ces deux techniques entraînent-elles des pertes, et pourquoi ces pertes sont-elles acceptables ?
4. **Cryptage**
   a) Qu'appelle-t-on «confidentialité» et «authentification» ?
   b) Expliquer en quoi consistent des attaques «known text», «chosen text», et «cipher text only», et leur puissances respectives.
   c) Citer un exemple d'algorithme de cryptage par bloc. Est-il sûr opérationnellement ou sans condition ? Pourquoi ?
   d) Quel est le principe d'un système de cryptage à clé publique ?
5. **Codage canal**
   a) Quel est son but ? En quoi tend-il à faire l'inverse du codage de source ?
   b) Qu'appelle-t-on le «code rate» d'un code par bloc ?
6. Expliquer ce qu'on entend par multiplexage FDM, TDM et CD (code orthogonaux).
7. **Modulation passe-bande**
   a) Donner les fréquences caractéristiques en France pour la radio FM, les communications GSM, UMTS et le Wi-Fi.
   b) Donner l'équation des formes d'onde sn(t) transmises en modulation FSK.
   c) Idem que b/ pour la modulation APK (=ASK + PSK).

Exercice 2 Cryptage

A l'aide la table au verso, donnez la séquence chiffrée correspondant au texte en clair « CLAIR » pour :

1. La méthode classique de Trithème (=sans clé).
2. La méthode Vigénère à clé chiffrée autoréférentielle (auto-cipher key) où la clé est K.
3. Proposer un autre code de cryptage que ceux vus en cours [1].
4. Citer un algorithme moderne de cryptage.

Exercice 3 Cryptage et confidentialité parfaite (code de Vernam)

1. Proposer un algorithme qui permette de casser un code de César pour toute séquence cryptée de longueur N et toute clé de longueur unité inconnue.
2. Idem si la clé est de longueur 2 avec 2 valeurs équiprobables (->casse un code de Vigenere type 1, à clé de longueur 2).
3. Que se passe-t-il si la longueur de la clé est n=N, et que chaque valeur est équiprobable ? Montrer que pour une clé parfaitement aléatoire de la longueur du message, la confidentialité est parfaite.
4. On revient au code de Vigenere type 1 avec une clé de longueur n utilisé pour coder un message de longueur N. On suppose que le cryptanalyste ne pourra pas casser le code s'il a plus d'une mole (env. $6x10^{23}$) d'opérations élémentaires à faire pour une recherche exhaustive, et qu'alors le système est sûr opérationnellement. Estimer la longueur minimale de clé à utiliser pour la méthode de Vigenere de type 1 avec clé aléatoire de longueur n soit sûr opérationnellement.
5. Si le processeur du cryptanalyste permettait de faire 10^9 opérations élémentaires par seconde, combien de temps lui prendrait une recherche exhaustive ?

Exercice 4 Code CB

1. Sur 10000 individus qui usurpent une carte bleue dont ils ne connaissent pas le code secret, combien en moyenne parviennent à retirer de l'argent à un distributeur de billets (qui se bloque au 3ème essai infructueux) ?
2. Si des lettres étaient utilisées au lieu de chiffres pour le code, combien en moyenne y parviendraient ?

Exercice 5 Parity Check Code

On considère la séquence binaire : 011000111. On commence à coder par le 1 de droite.

1. Donner la séquence résultante pour un «single parity check code» où k=3.
2. Donner la séquence résultante pour un code rectangulaire (M=3, N=3). Il y a a priori un bit ambigü en construisant les codes rectangulaires. Que ce bit indique la parité verticale ou horizontale change-t-il quelque-chose pour cette séquence ?
3. Quel est le «code rate» des codes en a/ et b/, et lequel est le plus redondant ?

1. on pourra s'inspirer du site http ://www.apprendre-en-ligne.net/crypto/menu/index.html

Exercice 6 Single Parity Check Code (4,3)

On considère un SPCC où n=4 et k=3.

1. Ce code peut-il corriger des erreurs, si oui lesquelles ?
2. Quelles erreurs ce code peut-il détecter ?
3. Calculer la probabilité Pnd d'erreurs non détectées en supposant que les erreurs sont indépendantes et équiprobables.
4. Quelle est la probabilité P1+ d'avoir 1 erreur ou plus ?
5. Si N0 bits sont transmis sans codage, à combien de bits erronés Ne faut-il s'attendre ?
6. Combien de bits N1 sont transmis si on code ces N0 bits avec ce SPCC ?
7. Combien de bits erronés subsistent si les blocs où il y a des erreurs détectées sont retransmis ? On supposera que les données retransmises utilisent le même code SPCC(4,3), que le décodeur signale chaque bloc erroné détecté en envoyant 1 bit d'alerte, et qu'il n'y a pas d'erreur sur les données retransmises.
8. Quel est alors le volume total de bits Ntot effectivement transmis ?
9. Pour un fichier de 1 Mo, et des BER de 0.1, 0.01 et 0.001, comparer numériquement Nombre de bits erronés/Nombre de bits transmis pour un système sans codage, et pour le SPCC(4,3) avec bit d'alerte.

Exercice 7 Single Parity Check Code (k+1,k)

On généralise le cas précédent. On suppose encore les erreurs équiprobables (probabilité p) et indépendantes.

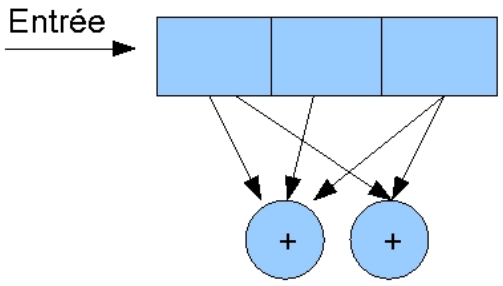
1. Quelle est la probabilité d'avoir j erreurs ?
2. En déduire la probabilité de non détection d'erreur (distinguer n pair et impair).
3. Pour un BER donné, quelle doit être la longueur N d'une séquence pour que la probabilité d'avoir au moins une erreur soit supérieure à 99% ? Comparer binomiale et Poisson pour BER=0,1, 1/100 et 1/10000.

Exercice 8 Double Parity Check Code (n,k)

1. Rappeler le taux de ce code.
2. Supposons que ce code puisse corriger tous les types d'erreur impliquant au plus t bits. Quelle est la probabilité qu'un bloc soit erroné ?
3. Montrer que pour un code rectangulaire, t=1.
4. En déduire la probabilité qu'un bloc soit erroné si le décodeur décide de corriger une seule erreur.
5. Si un bloc de taille (M+1)x(N+1) contient 2 erreurs, quelle est la probabilité que le décodeur ne puisse pas les corriger ?

Exercice 9 Codage convolutif

On considère le codeur convolutif de «constraint length» K=3, et avec k=1 :



Les additionneurs sont modulo 2. On suppose l'état initial à 000 et on injecte la séquence à coder par la gauche.

1. Donner la séquence résultante pour coder la séquence d'entrée : 101.
2. Combien de bits sont transmis ?
3. Quel est le taux de ce code en fonction de la longueur de la séquence l et de K (pour n=2 additionneurs) ?
4. Vers quelle limite le taux de ce code tend-il pour de très grandes longueurs ?
5. Idem que 3 et 4 pour n additionneurs.

Table de Trythemius

	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