CONCOURS INTERNE POUR LE RECRUTEMENT D'INGENIEURS D'ETUDES ET DE FABRICATIONS DU MINISTERE DE LA DEFENSE, AU TITRE DE L'ANNEE 2005

EPREUVE DE SPECIALITE

TELECOMMUNICATIONS

Le mercredi 28 septembre à 8H30

Durée : 4 heures

Coefficient : 3

AVERTISSEMENTS

L'épreuve est notée sur 20 points.

Le barème est donné à titre indicatif.

L'épreuve comporte 10 exercices.

Calculatrice scientifique autonome (sans périphérique) est autorisée.

Une table des transformées en Z est jointe à la fin du dossier.

Aucune autre documentation n'est autorisée.

Ce sujet comporte 10 pages.

Exercice n° 1 :

Chiffrement (3 points)

Système RSA

Le système à clé asymétrique RSA repose sur l'arithmétique des grands nombres. Les fonctions de chiffrement/déchiffrement sont de la forme :

Chiffré = clair ^{CléC} modulo n

Déchiffré = chiffré ^{cléD} modulo n

Dans lesquels :

- Clair est le message à coder
- Clé C la clé de chiffrement
- Clé D, la clé de déchiffrement
- n un produit de deux nombres premiers (grands dans la réalité) : n = p*q
- L'algorithme de détermination des clés est indiqué ci-après :
  - p et q doivent être grands ($>10^{100}$) et différents ;
  - choisir les clés telles que C.D = 1 + (M[(p-1)(q-1)] où M est un entier ;
  - la longueur maximale du bloc de bits sur lesquels on applique l'opération est telle que $2^L<n$.

Dans l'exemple ci dessous, l'utilisateur A a choisi une clé publique constituée de : C=3, n=33.

Questions :

1. Sachant que n = 11 * 3, déterminer D.
2. L'utilisateur B veut lui envoyer la valeur 29 ; chiffrer cette valeur avec C et n, et la déchiffrer.
3. L'utilisateur A répond avec la valeur 14. Expliquer comment, dans un tel système, A peut prouver qu'il est bien l'auteur d'un message (fonction de signature), donner la valeur signée transmise en ligne et la déchiffrer.
4. Quelle est la valeur maximale du bloc de bits que l'on peut chiffrer ?
5. Sachant que, en ASCII les lettres M = $4D_{(H)}$, O=$4F_{(H)}$, D = $44_{(H)}$, E=$45_{(H)}$, chiffrer le mot « MODEM » pour l'utilisateur A.

Exercice n° 2 :

Chiffrement (0,5 point)

Système DES

Question :

Sachant que les clés DES sont sur 56 bits, et que votre machine met 1µs à essayer une clé DES, combien de temps mettrez vous en moyenne pour trouver la bonne clé ?

Exercice n° 3 :

Réseaux informatiques (4 points)

Questions :

1. Lister et expliquer succinctement les couches du modèle OSI. Dans ce cadre, expliquer ce qu'est un protocole de niveau N.
2. Indiquer les niveaux (au sens OSI) des protocoles IP, TCP, UDP, MAC et LLC.
3. Comparer TCP et UDP ; sur lequel est basé le protocole SNMP, et à quoi sert-il ?
4. Dans un réseau de classe C, on désire créer 8 sous réseaux ; quel sera le masque de sous réseau à appliquer sur les stations de travail, et combien de machines pourront être intégrées à chaque sous-réseau ? Le routeur est à l'adresse X.X.X.6 ; quelle sera la passerelle par défaut pour le premier et pour le dernier sous réseau ?
5. Quelles fonctions se cachent derrière les termes suivants : LAG, VRRP, Spanning Tree, 802.1p, 802.1q ?
6. Dans le service DNS, expliquer les rôles des zones "forward" et "reverse", ainsi que la fonction de la commande "nslookup".
7. Qu'est-ce que le protocole LDAP ? Comment est organisée l'arborescence d'informations ? Qu'est-ce qu'un fichier LDIF ?
8. RNIS : accès de base et accès primaire ; donner le type et le débit de chacun des canaux.

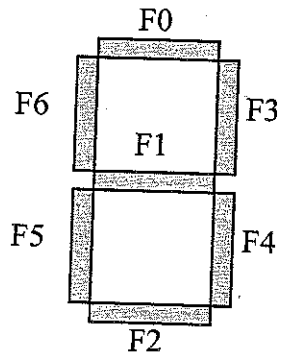
Exercice n° 4 :

Logique (2 points)

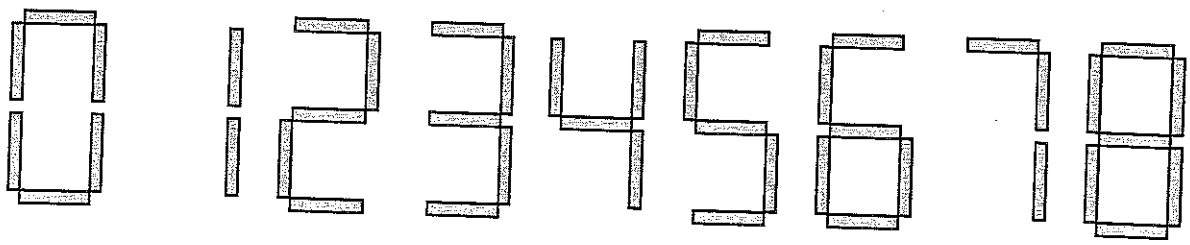
On veut, à l'aide d'un afficheur 7 segments, pouvoir afficher les chiffres de 0 à 9. Pour cela, on associe à chaque segment une fonction Fi avec i = 0, …, 6, qui a pour argument le chiffre à afficher et renverra 1 si le segment correspondant à la fonction doit s'allumer et 0 s'il doit rester éteint.
On utilise le code ci-dessous :

ABCD	Chiffre
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	Indéfini
….	…
1111	Indéfini

L'afficheur se présente ainsi :



Les chiffres seront représentés de la manière suivante :



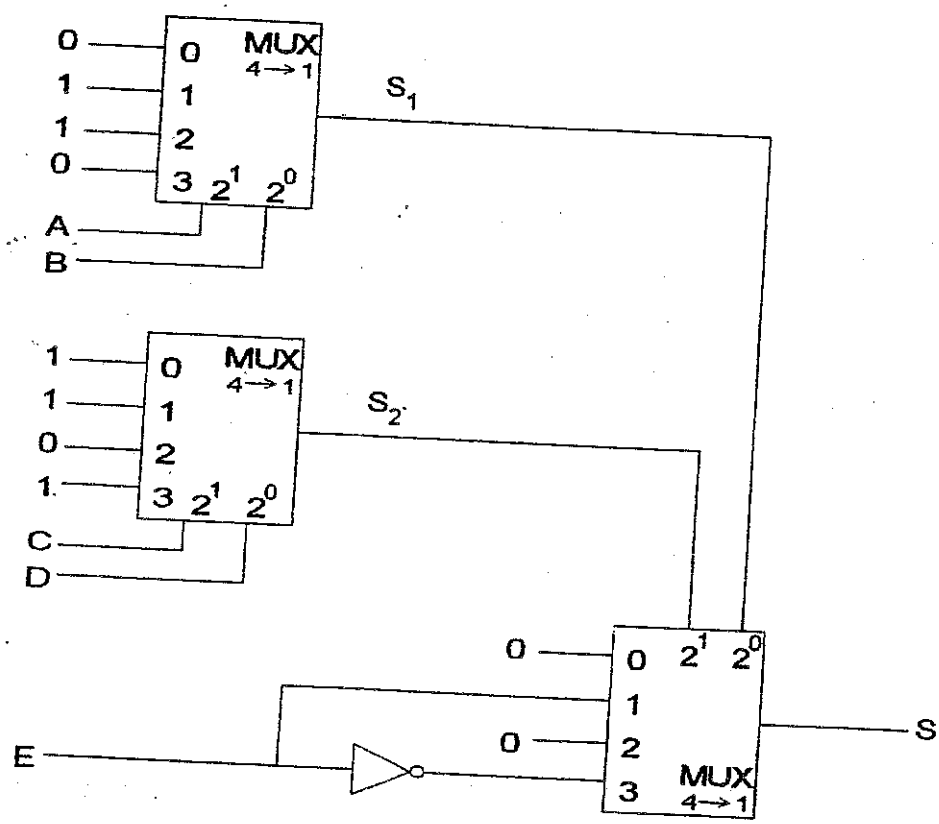
Questions :

1. Ecrire les équations des fonctions Fi (A,B,C,D) avec i = 0, …, 6.
2. Simplifier ces équations.

Exercice n° 5 :

Logique (1 point)

On réalise la fonction S à l'aide de multiplexeurs dans le montage suivant :



Questions :

1. Donner l'expression de S en fonction de S1 et S2.
2. Déterminer l'expression de S en fonction des différentes entrées.
3. En déduire l'équation logique de la fonction réalisée par ce montage.

Exercice n° 6 :

Logique (1 point)

La figure ci-dessous indique comment il est possible d'agencer quatre 74F138 (ou 74LS138) pour obtenir un décodeur de 1 parmi 32. Ces décodeurs sont notés de Z1 à Z4.

Les huit sorties de chacun sont combinées pour donner un total de 32 sorties nommées respectivement O_0 à O_7, O_8 à O_{15}, O_{16} à O_{23}, O_{24} à O_{31}. Un code d'entrée de 5 bits $A_4A_3A_2A_1A_0$ n'ouvre qu'une seule des 32 sorties pour chacune des représentations d'entrée possible.

Questions :

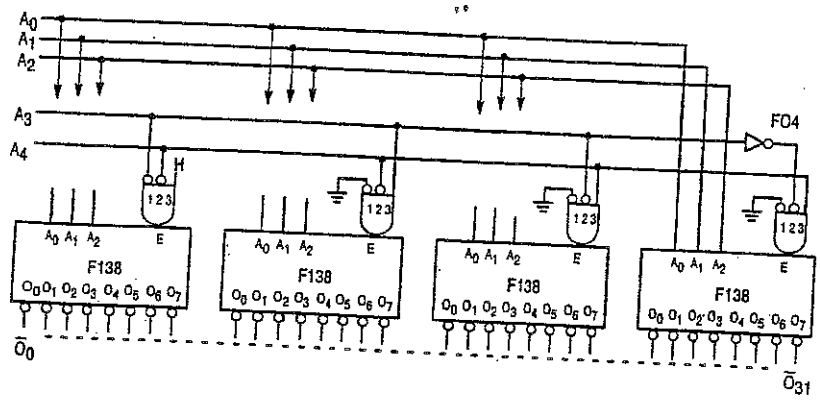
1. Dire quelle sortie est active si $A_4A_3A_2A_1A_0 = 01101$.
2. Indiquer la plage des codes d'entrée qui rend active toutes les sorties de la puce Z4.

MC54/74F138

FUNCTION TABLE

Inputs						Outputs							
$\overline{E}_1$	$\overline{E}_2$	E_3	A_0	A_1	A_2	$\overline{O}_0$	$\overline{O}_1$	$\overline{O}_2$	$\overline{O}_3$	$\overline{O}_4$	$\overline{O}_5$	$\overline{O}_6$	$\overline{O}_7$
H	X	X	X	X	X	H	H	H	H	H	H	H	H
X	H	X	X	X	X	H	H	H	H	H	H	H	H
X	X	L	X	X	X	H	H	H	H	H	H	H	H
L	L	H	L	L	L	L	H	H	H	H	H	H	H
L	L	H	H	L	L	H	L	H	H	H	H	H	H
L	L	H	L	H	L	H	H	L	H	H	H	H	H
L	L	H	H	H	L	H	H	H	L	H	H	H	H
L	L	H	L	L	H	H	H	H	H	L	H	H	H
L	L	H	H	L	H	H	H	H	H	H	L	H	H
L	L	H	L	H	H	H	H	H	H	H	H	L	H
L	L	H	H	H	H	H	H	H	H	H	H	H	L

H = HIGH Voltage Level
L = LOW Voltage Level
X = Don't Care



Exercice n° 7 :

Télécommunications (2 points)

Considérons un signal audio dont le spectre s'étend de 300 à 3300 Hz. On le transmet en PCM avec une fréquence d'échantillonnage de 8000 échantillons par seconde. On spécifie un rapport Signal sur Bruit de quantification en sortie de 30 dB.

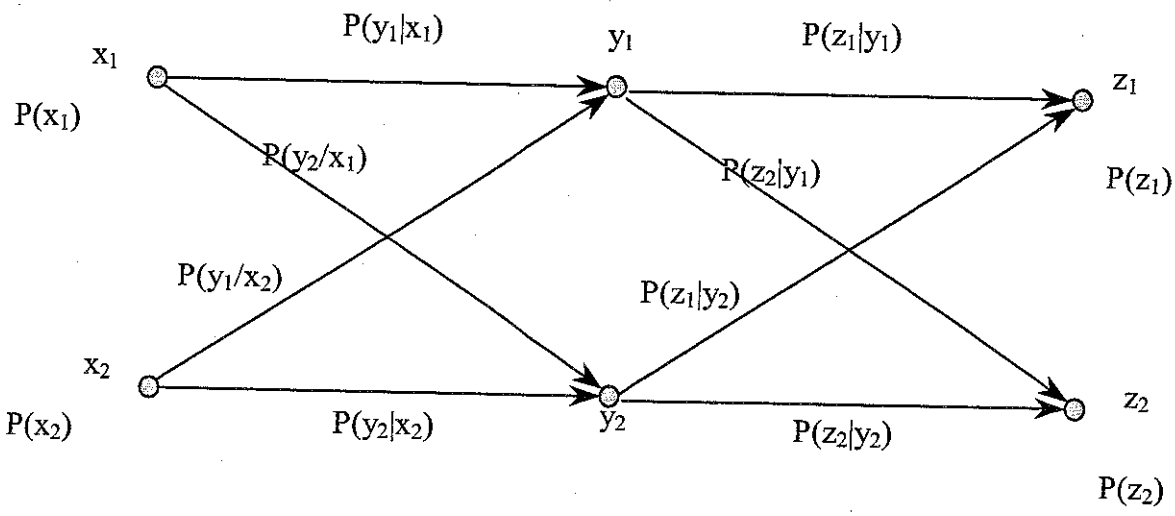
Questions :

1. Quels sont le nombre minimal de niveaux de quantification et le nombre minimal de bits par échantillon requis pour respecter cette spécification ?
2. Calculer la bande passante minimale requise pour transmettre le signal modulé.
3. Reprendre les questions précédentes dans le cas où l'on utilise un compresseur-expanseur de loi μ avec μ=255.

Exercice n° 8 :

Télécommunications (2,5 points)

Deux liaisons numériques en série fonctionnent en binaire, transmettant des 0 et des 1. Le bruit de cette liaison induit une confusion, ce qui conduit à interpréter un 1 comme un 0 et réciproquement. Soient respectivement x_1 et x_2 les évènements « transmission d'un 0 » et « transmission d'un 1 » ; soient y_1 et y_2 les évènements « réception d'un 0 » et « réception d'un 1 » à la sortie de la première liaison et z_1 et z_2 les évènements « réception d'un 0 » et « réception d'un 1 » à la sortie de la deuxième.



Soit P(évènement) la probabilité de cet évènement.

En considérant :

$P(x_1) = P(x_2) = 0,5$;
$P(y_2|x_1) = 0,1$;
$P(y_1|x_2) = 0,2$;
$P(z_2|y_2) = 0,8$;
$P(z_1|y_1) = 0,9$;

Questions. :

1. Calculer $P(y_1|x_1)$; $P(y_2|x_2)$; $P(z_2|y_1)$; $P(z_1|y_2)$
2. Calculer la matrice de transition de cet assemblage et tracer le schéma équivalent de ce canal.
3. Calculer $P(z_1)$et $P(z_2)$
4. Si l'on reçoit un 0, quelle est la probabilité que ce soit bien un 0 qui ait été transmis ? Si l'on reçoit un 1, quelle est la probabilité que ce soit bien un 1 qui ait été transmis ?
5. Calculer la probabilité d'erreur P_e et la probabilité P_c pour que le signal transmis soit reçu correctement par le récepteur.

Exercice n° 9 :

Systèmes (2 points)

On considère un établissement bancaire dans lequel le client dépose chaque mois une somme d'argent *u(n)* (s'il s'agit d'un retrait, *u(n)* sera négatif), placée au taux d'intérêt mensuel *I* ; le mode de calcul des intérêts est le suivant : le $i^{ème}$ mois, l'intérêt est calculé sur l'argent du capital en dépôt à la fin du $(i-1)^{ème}$ mois.

Chaque mois, le client dispose donc d'une somme d'argent *y(n)* qui représente la totalité de ses dépôts augmentée des intérêts acquis.

Questions :

1. Déterminer l'équation de fonctionnement de cet établissement bancaire, c'est à dire *y(n)* en fonction de *y(n-1), u(n) et I.* Cette équation récurrente est du premier ordre : elle nécessite la connaissance d'une condition initiale ; quelle est la condition initiale *y(-1)* sachant que le premier dépôt intervient à partir du mois 0 ?

Le client dépose 100 euros chaque mois dès le mois 0.

2. Après avoir calculé $y(0)$; $y(1)$ et $y(2)$, trouver *y(n)* en fonction de *n* et de *I*, et calculer $y(11)$, le capital au bout d'un an (on prendra $I=0,005$).
3. En utilisant la transformée en *Z*, exprimer *Y(z)* en fonction de *U(z)*. En prenant pour U(z) la transformée du signal *u(n)* appliqué et en cherchant la transformée inverse de *Y(z),* exprimer *y(n)*. Comparer au résultat précédent.
4. Le client dépose 100 euros chaque mois uniquement pendant 3 mois. Calculer *y(n)*, la réponse à ce nouveau signal ; en déduire $y(11)$.

Exercice n° 10 :

Systèmes (2 points)

Pour augmenter la résistance d'entrée d'un amplificateur inverse, on utilise le montage de la figure 1 :

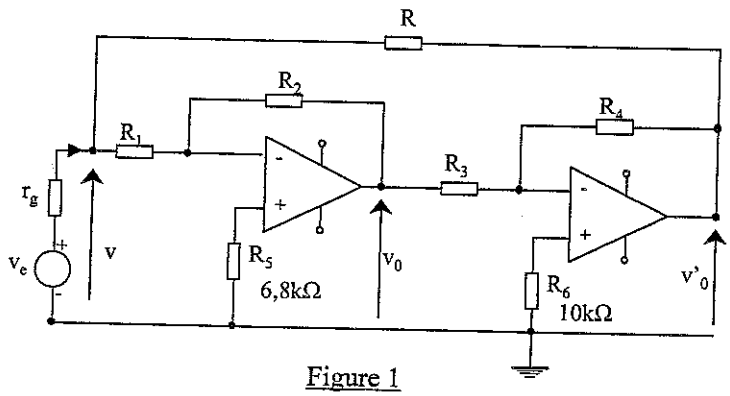


Figure 1

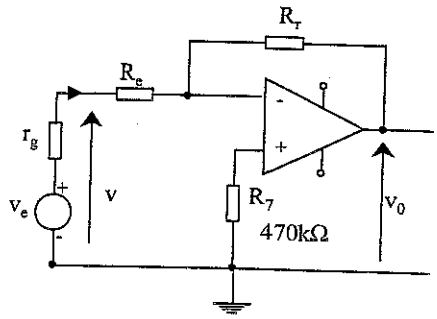
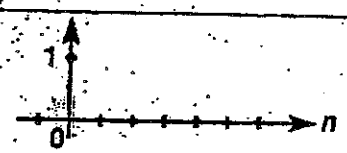
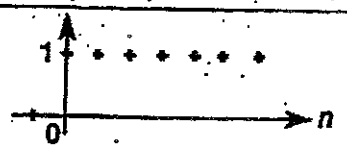
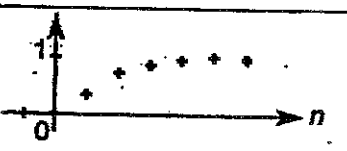
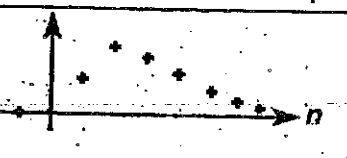
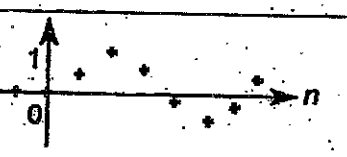
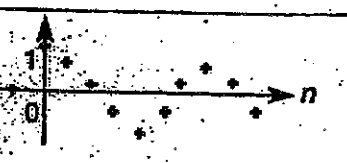
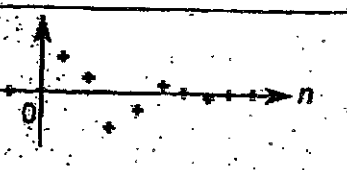
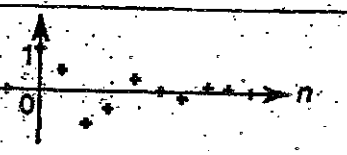


Figure 2

Questions :

1. Exprimer sa résistance d'entrée et en déduire un encadrement du rapport $R_2.R_4/R_3$ en fonction des résistances R et R_1, pour que la résistance d'entrée du montage soit supérieure à R_1
2. Déterminer les gains en tension v0/v et v0/ve suivant que le montage est attaqué par une source idéale de tension, ou une source réelle de résistance interne rg.
3. Quelles doivent être la résistance d'entrée Re et la résistance de réaction R pour que ces deux gains ne diffèrent que de 1% lorsque rg = 10 kΩ ?
4. Dans ce cas, pour R4 = 3 kΩ et R1 = R3 = 10 kΩ, déterminer R lorsque le module du gain est de 20.
5. Comment faudrait-il choisir la résistance d'entrée Re et la résistance de réaction Rr d'un inverseur classique (voir figure 2) pour obtenir les mêmes résultats ? Est ce que cela pose problème ?

Table des transformées en z

	$\{x_n\}$	$X(z)$
	$\{\delta_n\}$	1
	$\{\Gamma_n\}$	$\dfrac{z}{z-1}$
	$\{a\,n\,T_E\}$	$a\,T_E\dfrac{z}{(z-1)^2}$
	$\{e^{-nT_E/\tau}\}$	$\dfrac{z}{z-e^{-T_E/\tau}}$
	$\{1-e^{-nT_E/\tau}\}$	$\dfrac{z\,(1-e^{-T_E/\tau})}{(z-1)\,(z-e^{-T_E/\tau})}$
	$\{n\,T_E\,e^{-nT_E/\tau}\}$	$\dfrac{T_E z\,e^{-T_E/\tau}}{(z-e^{-T_E/\tau})^2}$
	$\{\sin(n\,\omega_0\,T_E)\}$	$\dfrac{z\sin\omega_0 T_E}{z^2-2z\cos\omega_0 T_E+1}$
	$\{\cos(n\,\omega_0\,T_E)\}$	$\dfrac{z\,(z-\cos\omega_0 T_E)}{z^2-2z\cos\omega_0 T_E+1}$
	$\{e^{-m(nT_E)}\sin(\omega_0\,n\,T_E)\}$	$\dfrac{z\,e^{-mT_E}\sin\omega_0 T_E}{z^2-2z\,e^{-mT_E}\cos\omega_0 T_E+e^{-2mT_E}}$
	$\{e^{-m(nT_E)}\cos(\omega_0\,n\,T_E)\}$	$\dfrac{z^2-z\,e^{-mT_E}\cos\omega_0 T_E}{z^2-2z\,e^{-mT_E}\cos\omega_0 T_E+e^{-2mT_E}}$