Exament de l'unité TACN. Durée : 4h **Nom :**

Tous documents (notes de cours, polys, livres, etc) autorisés

Il s'agit d'un examen QCM de type « une bonne réponse parmi N ». Sur chacune des réponses possibles, énumérées (a), (b), (c), etc, **entourez ou soulignez** la lettre correspondant à la bonne réponse (de manière non ambigüe). Bon courage.

Codage (C. Renaud)

1. Les codes convolutifs sont largement employés en radiocommunications car:
   (a) Ils peuvent être décodés grâce à l'algorithme de Viterbi qui est simple à mettre en oeuvre soit dans un microprocesseur soit dans un circuit spécialisé
   (b) Naturellement, ils sont insensibles aux paquets d'erreurs et les corrigent donc très bien, sans précaution supplémentaire
   (c) Ils permettent d'obtenir d'excellents rendements et donc de hauts débits de transmission de données
   (d) Ils ont naturellement une excellente capacité de détection d'erreurs et ne nécessitent pas l'emploi de CRC pour détecter que le nombre d'erreurs à corriger dépasse leur capacité de correction

2. Le soft decoding
   (a) permet systématiquement un gain de 3 dB par rapport au hard decoding.
   (b) n'est pas mis en œuvre pour les codes convolutifs car nécessite beaucoup de calculs supplémentaires par rapport au hard decoding .
   (c) comporte une étape de calculs de syndromes.
   (d) nécessite que la démodulation effectue un calcul de vraisemblance sur les bits décidés.

3. Les turbo codes
   (a) ont l'inconvénient d'être plus complexes que les techniques de codage usuelles
   (b) au fur et à mesure des itérations affinent l'estimation des bits d'information
   (c) sont construits uniquement à partir de codes convolutifs

(d) parallèles ont un rendement R = R1 + R2, où R1 et R2 sont les rendements des codes constituants.

4. Afin de décorréler les erreurs et améliorer ainsi l'efficacité du décodage, il est important d'entrelacer les bits :

   (a) à l'intérieur d'un bloc de Reed-Solomon
   (b) à l'intérieur d'un bloc BCH
   (c) après un codage convolutif
   (d) avant de procéder au codage convolutif

5. Un code de Reed-Solomon de longueur 255 symboles de 8 bits (dimension du code = 8), comprenant 231 symboles utiles, peut:

   (a) corriger 8 symboles faux (la dimension) et en détecter 16 faux, au maximum
   (b) corriger 8 bits faux et en détecter 16 faux, au maximum
   (c) corriger 24 symboles faux (255 moins 231) et en détecter 48 faux, au maximum
   (d) corriger 12 symboles faux (255 moins 231, divisé par 2) et en détecter 24 faux, au maximum

Égalisation (C. Vignat)

1. les critères "Zero-Forcing" et "Erreur Quadratique Minimale" sont, en absence de bruit

   (a) équivalents
   (b) asymptotiquement équivalents
   (c) distincts

2. l'égalité des filtres d'émission et de réception permet d'obtenir, en sortie du filtre de réception

   (a) un rapport signal à bruit optimal
   (b) un taux d'erreur par bit minimal
   (c) une erreur de prédiction minimale

3. en absence de bruit, quel que soit le canal, et avec un égaliseur linéaire:

   (a) on peut toujours reconstituer exactement les symboles
   (b) on peut reconstituer exactement les symboles s'ils sont Gaussiens
   (c) on peut reconstituer les symboles émis sous certaines hypothèses

4. afin d'éviter les interférences intersymboles, il suffit

   (a) d'utiliser un filtre émetteur en cosinus surélevé
   (b) d'utiliser un filtre émetteur qui vérifie le critère de Nyquist
   (c) d'utiliser des filtres émetteurs et récepteur en racine de cosinus surélevé
   (d) d'utiliser un équaliseur linéaire optimisé selon le critère "Zéro Forcing"

5. lorsque le critère de Nyquist n'est pas vérifié,

   (a) on peut transmettre les données à un débit quelconque

   (b) il est impossible, sans autres hypothèses, de reconstituer avec une erreur arbitrairement faible les données émises
   (c) il est possible, sous certaines hypothèses, de reconstituer les données émises avec une erreur arbitrairement faible

6. dans le cas non-bruité, et sans aucune autre hypothèse, le récepteur optimal est
   (a) un filtre linéaire à réponse impulsionnelle finie
   (b) un filtre linéaire à réponse impulsionnelle infine
   (c) un filtre non-linéaire instantané

Crypto (D. Samyde)

1. La génération de nombres pseudo-aléatoires en quantité peut s'effectuer grâce au résultat partiel d'une fonction de hachage reconnue comme sûre (Exemple SHA) ?
   (a) Oui en prenant des bits quelconques dans le résultat du hachage et en ayant une entrée non constante (Heure ou Timer, Intervalle entre deux interruptions,...).
   (b) Oui en prenant des bits fixes et en maintenant toujours la même entrée. Car une fonction de hachage n'est pas déterministe.
   (c) Non, une fonction de hachage ne permet pas d'obtenir des nombres pseudo-aléatoires. Car elle est déterministe et l'on peut prévoir sa sortie aisément.
   (d) Non, car on peut inverser n'importe quelle fonction de hachage de manière simple et donc il n'y a pas de pseudo-aléa.
2. Une machine parcourant par force brute (totalité du parcours par essais successifs) un espace de clés de 512 bits est réalisable :
   (a) Oui, grâce à un supercalculateur de type Cray
   (b) Oui, en parallélisant des PC monoprocesseurs (Pentium III 500) pendant environ 1 mois.
   (c) Oui, car une clé RSA de 512 bits a été cassée par force brute en juillet dernier (Equipe française liée à Polytechnique).
   (d) Non, les lois de la thermodynamique l'interdisent (Impossible de dépasser 220 bits).
3. L'algorithme RSA est un algorithme a clé publique,clé privée, inconditionnellement sûr :
   (a) Oui, RSA est sûr dans tous les cas
   (b) Non RSA nécessite juste une taille de clé supérieure à 512 bits.
   (c) Non RSA, n'est pas sûr lors de signatures provenant de l'extérieur et n'ayant pas utilisé de fonction de hachage sûre pour générer le résidu à signer. De plus la taille des clés doit être supérieure à 512 bits.
   (d) Non, RSA est un algorithme à clé secrète.
4. Le seul chiffrement inconditionnellement sûr est le chiffrement de Vernam ou OTP ou encore appelé Masque Jetable :
   (a) Oui, car la taille de la clé (clé purement aléatoire et utilisable une fois et une seule), égale la taille du message. Toutefois il pose le problème de l'acheminement préalable des clés.
   (b) Non, ce chiffrement est facilement cassable par collisions même avec des clés purement aléatoires (Attaques des anniversaires).

5. L'algorithme DES (Data Encryption System) est un algorithme actuellement sûr, et résistant aux plus grandes puissances de calcul connues :

   (a) Oui, DES est encore sûr, son utilisation massive le prouve.

   (b) Non, il a été récemment prouvé que cet algorithme n'est pas sûr.

6. Un protocole utilisant une fonction de hachage permet à Alice et Bob ne s'assurer qu'Estelle (Espion actif) ne modifie pas le message :

   (a) Vrai, car Alice envoie d'abord le hachage d'une question avant de poser cette dernière.

   (b) Faux, car Estelle utilisant l'attaque (Man in the middle) , ne peut jamais être contournée.

Séquences PN a bonnes propriétés.... (G. Baudoin)

1. Un registre à décalage de longueur N permet de générer des séquences binaires périodiques de période maximale égale à :

   (a) 2^N

   (b) $2^N - 1$

2. Le polynôme générateur d'une séquence PN de longueur maximale générée avec un registre à décalage de longueur N:

   (a) divise le polynôme $x^N - 1$

   (b) divise le polynôme $x^M - 1$ avec $M = 2^N - 1$

   (c) est multiple de $x^M - 1$.

3. Avec un registre à décalage de longueur N, on peut générer un nombre K de séquences PN à longueur maximale, avec :

   (a) $K = N$

   (b) $K = 2^N - 1$

   (c) $K = \Phi(2^N - 1)$

   (d) $K = \Phi(2^N - 1)/(2^N - 1)$

   (e) $K = \Phi(2^N - 1)/N$ Où on note $\Phi(k)$ la fonction de Euler de l'entier k, c'est-à-dire le nombre d'entiers strictement inférieurs à k premiers avec k.

4. L'autocorrélation d'une séquence PN à longueur maximale peut prendre :

   (a) 2 valeurs

   (b) 3 valeurs

   (c) N valeurs

5. L'intercorrélation de 2 séquences de Gold de même longueur peut prendre :

   (a) 2 valeurs

   (b) 3 valeurs

   (c) N valeurs

6. Avec 2 registres à décalage de longueur N, on peut générer :

(a) N séquence de Gold
(b) 2^N séquences de Gold
(c) $2^N + 2$ séquences de Gold.

Modulations codées, multiporteuses et applications (F. Belveze)

1. Un récepteur pour modulation codée:
   (a) effectue la démodulation, puis le décodage
   (b) effectue plusieurs passes de démodulation et de décodage, jusqu'à convergence
   (c) effectue en une seule passe une démodulation et un décodage simultanés
   (d) nécessite la connaissance du treillis de la modulation et du treillis du code
2. Quel est le lien entre le temps de cohérence d'un canal et l'élargissement spectral que le canal apporte au signal reçu (ou encore la bande Doppler):
   (a) le premier est l'inverse du second
   (b) leur produit est très supérieur à 1 en général
   (c) il n'y a aucun lien a priori entre ces deux grandeurs
   (d) leur produit est très inférieur à 1 en général
3. A quoi sert le temps de garde en OFDM:
   (a) à contrôler le spectre du signal émis
   (b) à améliorer la résistance au bruit de réception
   (c) à pouvoir s'adapter plus facilement aux variations rapides du canal de propagation
   (d) à éviter d'avoir de l'interférence entre symboles
4. Pourquoi un entrelacement en fréquences dans le DAB:
   (a) comme dans tout système COFDM, on répartit un flux d'information sur tout le spectre disponible, pour éviter de rester longtemps sur une sous-porteuse effacée par le canal
   (b) pour des raisons de cryptage (cryptage par saut de fréquence)
   (c) c'est le seul moyen de garantir un spectre étroit en émission, n'interférant pas avec les porteuses voisines à +/- 1.5 MHz
   (d) c'est la seule possibilité, à cause du multiplex de plusieurs services dans une seule bande de 1.5 MHz
5. Dans une modulation codée standard (par exemple, une 16-QAM codée 3/4)
   (a) tous les bits d'information sont nécessairement codés, pour garantir la plus grande distance minimale posible
   (b) certains bits non codés sélectionnent un signal dans un sous-ensemble, qui lui est désigné par les bits codés
   (c) la méthode du set partitioning permet de simplifier la concaténation du treillis du code et du treillis de la modulation, quand celle-ci a une mémoire
   (d) la méthode du set partitioning classe les signaux possibles en les sub-divisant en sous-ensembles successifs de distances minimales internes décroissantes.

Diversité (A. Chevreuil)

1. On observe T échantillons du modèle

$$Y_n = As + W_n$$

où A est un vecteur (connu) à P composantes et W_n une suite de vecteurs Gaussiens, blancs spatialement et temporellement de variance $\sigma^2 I_P$. La variance de l'estimateur de s au sens du maximum de vraisemblance est de la forme

   (a) $\frac{\sigma^2}{T^2\|A\|_2^2}$

   (b) $\frac{\sigma^2}{T\|A\|_2^2}$

   (c) $\frac{\sigma^2}{T\|A\|_2}$

2. Dans un modèle de transmission de symboles binaires où l'on suppose disposer de P canaux de Rayleigh indépendants (le bruit additif est supposé Gaussien, blanc spatialement et temporellement), la probabilité d'erreur est

   (a) une fonction croissante de P

   (b) de l'ordre de $(\frac{1}{\gamma})^P$ où γ est le rapport signal-sur-bruit moyen sur chaque voie.

3. Dans un modèle de diversité d'antennes (le bruit additif est toujours Gaussien et blanc), le nombre de ces antennes

   (a) laisse invariante la capacité de Shannon

   (b) permet d'éviter les phénomènes d'évanouissements dans une bande de fréquences

   (c) n'a pas d'effet sur les performances d'un récepteur MMSE-DFE

Synchronisation (J.-M. Brossier)

1. Pour un signal modulé en BPSK (modulation de phase discrète à deux états). Est-il possible d'estimer la phase modulo 2π (*i.e.* sans l'ambiguité de π) ?

   (a) Non, il existe toujours une indétermination de π due à la symétrie de la constellation.

   (b) Oui à condition que les données (a_k) soient connues (au moins partiellement).

   (c) Oui même si les données ne sont jamais observées.

2. Dans un algorithme tel que la boucle de Costas $\varphi_k = \varphi_{k-1} + \gamma \Im\left(y_k^2 e^{-i2\varphi_{k-1}}\right)$, quel est l'intérêt de remplacer le pas scalaire γ par un filtre de la forme $\gamma_1 + \frac{\gamma_2}{1-z^{-1}}$:

   (a) Si la dérive de phase est linéaire, ce filtre permet d'annuler le biais asymptotique.

   (b) La convergence initiale est meilleure.

   (c) Cela évite les glissements de cycle.

3. Pour un système de transmission qui respecte le critère de Nyquist (*e.g.* réponse en cosinus surélevé), quel est l'effet d'une désynchronisation (décalage constant) du peigne d'échantillonnage ?

   (a) Aucun si le décalage est constant au cours du temps.

   (b) Aucun dans tous les cas.

   (c) Cela génère des interférences entre symboles.

4. Comment peut-on faire apparaître une raie spectrale à la fréquence symbole pour un signal BPSK ?

   (a) Par filtrage linéaire passe-bande.

   (b) Par filtrage linéaire passe-bas.

   (c) En utilisant un non linéarité.

5. Lors de la conception d'une boucle à verrouillage de phase, comment est-il possible de prendre en compte des informations *a priori* très fortes telles que le fait que l'émetteur suit une trajectoire connue dans l'espace ?

   (a) En choisissant une fonction de coût adaptée.

   (b) En choisissant un filtre de boucle adapté.

   (c) En modifiant l'algorithme de minimisation de la fonction de coût.