ENSIAS *Le 04/02/2013*

Examen "Théorie de l'information et codage"

Documents de cours autorisés Durée : 1h20

I. Une source simple S émet 7 symboles $\{x_1, \ldots, x_7\}$ avec les probabilités données par {0.03 , 0.08, 0.12 , 0.14 , 0.18 , 0.20, 0.25} sur un canal en utilisant des symboles binaires

1) Trouver à l'aide de l'algorithme de Huffman un premier code pour les sept symboles.
2) Appliquer un codage de Shannon-Fano pour cette source et trouver un code irréductible.

II. On décide d'utiliser le système de Merkle-Hellman comme schéma de chiffrement de données dans un réseau. La clef privée utilisée est comme suit :

A=(3 ;12; 17; 33; 74,157; 301), p=69 et u=605.

1) Calculer la clef publique associée.
2) Quel est alors le message chiffré associé au message M =(0, 1, 1, 1, 1, 1, 0).
3) Trouver l'inverse de p=69 modulo u=605.
4) Déchiffrer le cryptogramme C = 459.

III. On considère le code convolutionnel de taux 1/2 et de séquences génératrices les séquences

g1= (100) **g2= (101)**

1) Donner un dessin du circuit codeur associé à ce code.
2) Quelle est la longueur de contrainte de ce code ? est -il systématique ?
3) Construire le diagramme d'état pour ce codeur.
4) Une séquence d'information est codée par ce code et ensuite transmise via un canal binaire symétrique avec une probabilité de transition $p=10^{-3}$. Si la séquence reçue est

r = (11 00 10 10 10 00 01 00).

Appliquer l'algorithme de Viterbi et montrer sur un treillis la procédure d'élimination des chemins non survivants et indiquer le chemin optimal. Retrouver la séquence émise qui a la plus grande vraisemblance.