PROJET 2023-2024

Le programme et le rapport sont à réaliser en binôme.
Vous présenterez votre projet lors de la dernière séance de TP le 06/05/2024 ; un planning sera donné.
L'archive sera à rendre le jour même.
Le rapport sera un fichier Nom1_prénom1_Nom2_Prénom2.pdf.
Le programme et le rapport seront dans une archive Nom1_prénom1_Nom2_Prénom2.zip.
L'archive doit être déposée en utilisant l'outil FileSender de votre ENT.
Le lien vers l'archive est à envoyer par mail à richard.genestier@u-bourgogne.fr

Dans les archives de Claude Shannon, Richard Hamming a retrouvé une lettre dont le contenu se trouve dans le fichier `projet_2023_24_lettre_bits.txt`*. Chaque caractère de cette lettre appartient à la table ASCII et est encodée sur 8 bits. Ne parvenant pas à la déchiffrer, il souhaite l'envoyer à son ami David Albert Huffman. Sachant que des erreurs pourraient s'insérer dans la lettre lors de sa transmission, il enrichit le codage binaire (il devient 1,75 fois plus long) pour que le destinataire puisse éventuellement corriger ces erreurs lors de sa réception.*
Une fois la lettre reçue, Huffman détecte deux erreurs (une au début et une à la fin), les corrige, puis supprime les bits de contrôle et l'encode sous forme de caractères alphanumériques. Obtenant une suite de caractères incohérents, il se rend compte, après analyse, qu'elle a été chiffrée par une méthode de chiffrement polyalphabétique du XVI^{ème} siècle. Grand amateur de serpents, il parvient à la décrypter et découvre alors le destinataire de cette lettre.
Decidé à lui faire parvenir, il rechiffre la lettre par une variante du chiffrement précédant, considéré comme "le seul algorithme cryptographique à confidentialité parfaite" par Claude Shannon. De plus, jugeant le poids du fichier trop important, il parvient à rendre le codage binaire optimal et à réduire ce poids de plus d'un quart.
Il envoie alors la lettre chiffrée et compressée à son destinataire, qui parvient finalement à la lire (grâce aux données supplémentaires que lui a fourni Huffman) ...

Il est demandé de produire un programme dans le langage de votre choix permettant d'effectuer les manipulations d'Huffman et du destinataire sur la lettre. Le code doit être commenté. Ce programme comportera des jeux d'essais afin de tester automatiquement toutes les fonctionnalités demandées lors de son lancement (chaque étape sera bien identifiée).
L'archive à rendre comportera le code, le rapport, ainsi que les différentes lettres intermédiaires obtenues après chaque étape sous forme de fichiers d'extension `.txt`.
Le rapport expliquera en détails les techniques d'encodage/décodage/chiffrement/déchiffrement utilisées, ainsi que la démarche choisie pour les implémenter.
Le langage Python, si vous le connaissez un peu, est bien adapté à ce contexte ; dans ce cas, aucune importation de module n'est nécessaire, hormis une fonction du module `random` aidant à générer une clé pseudo-aléatoire. Si vous utilisez un autre langage, limitez au maximum l'importation de bibliothèques.

Face à ces énigmes successives, si vous êtes "coincés", une aide pourra vous être apportée lors des séances de TP encadrées …

Barème : code / 10, rapport+démo / 10