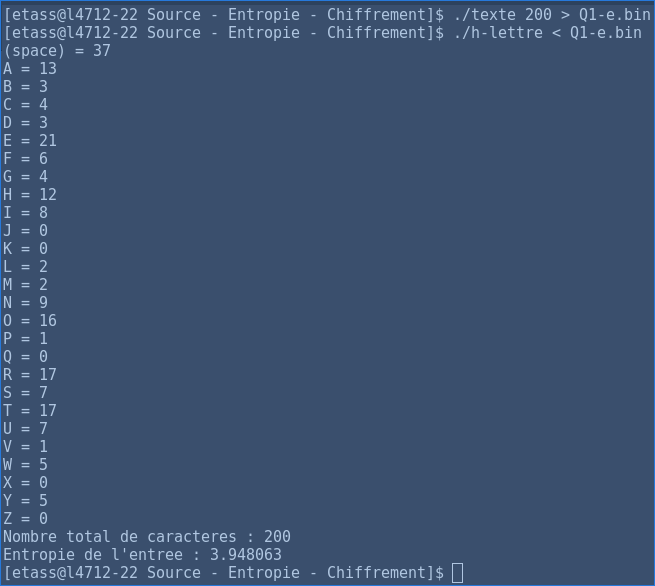
# Partie A

## Question 1 - Entropie

1. **Calculez l’entropie par lettre (h-lettre) d’une chaîne générée avec texte d’une longueur de 200 caractères?**L’entropie par lettre de h-lettre est d’environs 3,94.   
   ****
2. **En vous servant du premier théorème de Shannon, expliquez ce que signifie cette valeur.**

Pour connaitre l’entropie maximal que la source devrait donner nous pouvons utiliser le calcul de l’entropie *H*(*S*) = Σ *i*  *pi* log2 1/*pi.* Dans le cas d’une source optimale, la probabilité pi serait de 1/27 (26 caractères plus l’espace) pour chaque caractère. L’entropie total de la source serait donc de 4,7548 bits avec une source parfaite. On voit donc qu’il y a une différence d’environ 0.8 bits entre les deux entropies. L’entropie est une mesure de la quantité d’information transmise par une source. La valeur de l’entropie trouver est donc une indication de la quantité d’information que la source émet et cette valeur est à 0.8 bits de la valeur maximal qu’elle pourrait atteindre.

1. **Quelle** **serait l’entropie par lettre (en moyenne) d’un fichier qui aurait été généré de la même façon, mais avec les mêmes probabilités (1/27) pour chacun des 27 symboles (lettres majuscules et espace)?**

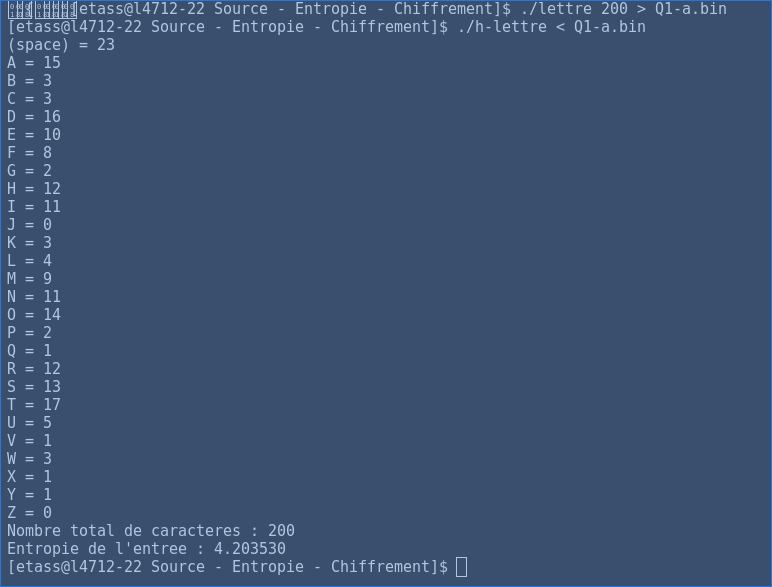
Comme expliquer dans la réponse précédente, l’entropie d’une source avec une probabilité de 1/27 par source serait d’environ 4.948 bits

1. **Que** **représente le quotient de la valeur en a) sur la valeur en c) ?**

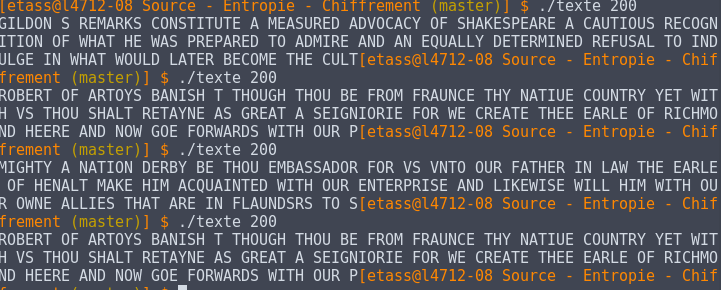
Le quotient de la valeur a) sur la valeur c) est de 83,031 %. Cette valeur nous montre que la source ne distribue pas uniformément sont alphabet.

1. **Refaites la même chose qu’en a) avec la source lettre. Comparez la valeur obtenue avec celle en a). Est-ce que la différence est significative (supérieure à 0.4) ?**

La valeur de l’entropie avec la source lettre est de 4,203 bits. La différence avec la source texte est donc d’environs 0,255 ce qui n’est pas une différence significative.

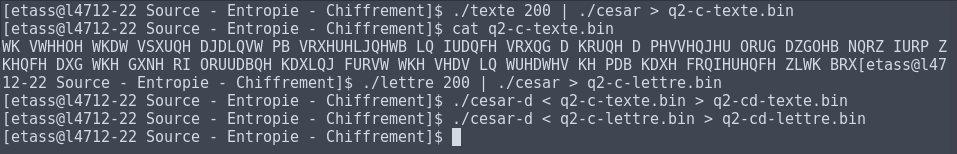


1. **Les chaînes générées par lettre ne sont pas de l’anglais malgré l’utilisation des mêmes fréquences.** **Le résultat obtenu en e) peut donc surprendre. Expliquez cette contradiction apparente (le fait que les deux entropies soient proches).**

Si l’on regarde les résultats que la source texte nous donne, on peut voir que les textes sont constitués de mots en anglais. Comme la source de lettre utilise la même fréquence de lettre que l’anglais, il est donc compréhensif que les deux sources possèdent une entropie similaire.  ****

## Question 2 – Histogrammes

1. **Utilisez les programmes cesar et cesar-d avec les sources texte et lettre, pour chiffrer et déchiffrer des chaînes de 200 caractères.**



1. **Utilisez le programme h-lettre pour obtenir les fréquences des lettres. Construisez des histogrammes de fréquences ordonnées du plus grand au plus petit pour la sortie de chacune des sources ainsi que pour les versions codées.**

1. **Que remarquez-vous en comparant ces quatre histogrammes? Comment seraient les histogrammes des sources lettre et texte si les fréquences étaient comptabilisées sur deux lettres à la fois? Comment devrait être par exemple les fréquences du (ee) et du (th) dans le cas de texte et de lettre.**

À l’aide des histogrammes, on voit très bien que la fréquence des lettres entre la source codé et non codé sont exactement les mêmes. Comme le code de césar n’est qu’un de simplement décalement de lettre, il n’est pas surprenant d’avoir ce résultat. Si les fréquences étaient comptabilisées sur deux lettre à la fois, la source lettre aurait beaucoup plus de chance de produire un graph mieux distribuer puisqu’elle ne respecte pas la grammaire de la langue anglaise. La fréquence des pairs « ee » et « th » pour la source lettre serait similaire à n’importe quelle autre combinaison. La source texte cependant produirait un graph similaire à se que l’on pourrait s’attendre d’un graph de fréquences normales de pair de lettre d’un texte anglophone. La fréquence des pairs « ee » et « th » pour la source texte serait donc similaire à la fréquence des pairs « ee » et « th » dans n’importe quel autre texte anglophone.

1. **En vous référant au point précédent ainsi qu’à la question 1 f), est-ce que cette méthode (comptabiliser les fréquences sur deux lettres) facilite le déchiffrement du message dans le cas de la source texte ? Et dans le cas de lettre ? Expliquez la différence s’il y en a une. Pour chacune des deux sources, si cette méthode n’augmente pas la facilité de déchiffrement du message, quelle solution proposez-vous ?**

L’analyse de pair de lettre peut aider au déchiffrement dans le cas de la source texte puisque cette source produit effectivement de vrais textes anglophones. La fréquence de pair de lettre devrait donc être similaire à la fréquence de pair de lettre en général en anglais. La même analyse ne serait pas efficace pour la source lettre cependant puisque malgré le fait que les lettres générées par la source lettre aient la même fréquence que ceux de l’anglais, leurs alignements n’est pas garantie. En d’autres mots, les lettres provenant de la source lettre ont la même fréquence que ceux d’un texte anglais sans suivre les règles de grammaire de l’anglais.

Pour la solution à proposer, il n’y a pas de réelle solution. Si l’analyse de fréquence de pair ne donne rien, l’analyse de triplet ou de tout autre combinaison n’est pas non plus une possibilité. La solution est donc de simplement se fier à la fréquence de lettre singulière.

## Question 3 -Masque jetable

1. **Générez un fichier de 1024 octets avec monnaie et un avec binaire. Calculer l’entropie par bit (hbit) et l’entropie par octet (h-ascii) sur les deux fichiers créés.**
   1. Fichier binaire – hbit :

0 = 5200

1 = 2992

Nombre total de bits : 8192

Entropie du texte entre : 0.946943

* 1. Fichier monnaie – hbit :

0 = 4124

1 = 4068

Nombre total de bits : 8192

Entropie du texte entre : 0.999966

* 1. Fichier binaire – hascii :

Nombre total d'octets : 1024

Entropie de l'entree : 0.778828

* 1. Fichier monnaie – ascii :

Nombre total d'octets : 1024

Entropie de l'entree : 7.831431

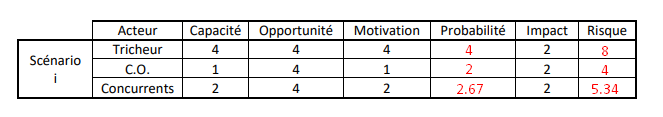


## Question 4 – Analyse de risque

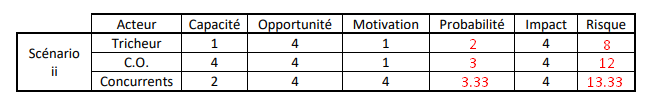
1. **Quelle serait votre recommandation et pourquoi ?**

Si on commence par faire une analyse de capital, il faut prévoir l’argent requis pour rebâtir tous les serveurs et les installations à chaque 4 ans si l’on décide de s’installer sur le site B. Pendant la reconstruction sur le site B, il ne faut pas oublier que le service PokerMaxProUltime ne sera plus disponible si aucunes autres installations de secours ne sont prévues. Ces installations de secours engendrent des couts supplémentaires pour le site B à prendre en compte. Nous estimons que les couts ainsi que les problèmes engendrés par le risque élever d’un ouragan sur le site B justifie la différence initiale de 400 000$ pour le site A.

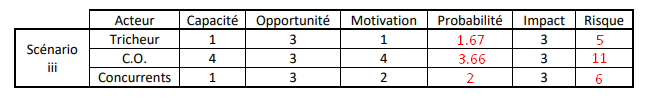
1. **Pour chacun de ces scénarios, précisez s’il s’agit principalement d’un scénario touchant l’intégrité, la confidentialité ou la disponibilité.**
2. Le fait d’avoir un tricheur sur le site diminue l’intégrité du site.
3. Si les joueurs légitimes n’arrivent plus à se connecter cela relève de la disponibilité du service.
4. Si des informations confidentielles sont accessible par quelqu’un qui n’a pas l’autorisation d’accéder à ces données, cela est un problème de confidentialité.
5. **Commentez, pour chaque scénario de risque, quel serait l’acteur qui constitue la plus grande menace pour votre entreprise.**

Pour le premier scénario, le tricheur professionnel serait la plus grande menace.

Pour le deuxième scénario, les sites de poker concurrents constituent la plus grande menace.



Pour le troisième scénario, c’est le crime organisé qui est la plus grande menace.



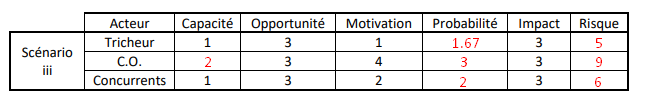
1. **Pour chacune des situations suivantes expliquez quel(s) paramètre(s) changerai(en)t et dans quel sens (plus grand, plus petit). Quelle(s) conséquence(s) pour la gestion du risque ?**
2. *Votre compagnie de poker remporte un très grand succès et dépasse tous vos concurrents.*  
   La motivation des concurrents va augmenter.
3. *Votre patron a refusé de payer les pots-de-vin réclamés par la mafia locale.*

La motivation du crime organisé va augmenter.

1. *Votre patron fait l’acquisition d’un tout nouveau système de détection des tricheurs très performant.*

La capacité des tricheurs à pouvoir tricher diminue.

1. **Refaites la grille de la question c) pour le scénario iii) en prenant en compte la mesure proposée. Est-ce que vous croyez que cette offre en vaut la chandelle ? Est-ce que votre recommandation s’applique dans toutes les circonstances ?**

Nous ne croyons pas que cette offre en vaut la chandelle. L’ajout d’un système de détection d’intrusion sur nos serveurs ne fait seulement qu’influencer la capacité de quelqu’un à tricher. Dans le scénario iii, seulement la capacité du crime organisé diminue. De plus, le fait que des employer de l’ex-Union Soviétique on les mains sur un logiciel qui est installer sur nos serveur n’est pas très rassurant. Nous ne recommandons pas ce logiciel et cette non recommandation s’applique dans toutes les circonstances.