Exercice 1.
Dans cet exercice on se propose d'écrire les fonctions Python correspondant au chiffrement de César. On suppose que les messages sont composés uniquement de majuscules qui seront chiffrées et d'espaces qu'on ne modifie pas.

1. Ecrire en Python une fonction `chiffre_cesar(msg, clef)` qui prend en arguments une chaîne de charactère `msg` et un entier `clef` et renvoie une chaîne de caractère correspondant au chiffrement de César de la chaîne `msg` avec un décalage égal à `clef`.

```
>>> chiffre_cesar("L INFORMATIQUE C EST SUPER",5)
'Q NSKTWRFYNVZJ H JXY XZUJW'
```

2. Ecrire une fonction Python `dechiffre_cesar(msgc, clef)` qui réalise le déchiffrement du message chiffré `msgc` avec le code de César pour un décalage égale à `clef`.

```
>>> dechiffre_cesar("Q NSKTWRFYNVZJ H JXY XZUJW",5)
'L INFORMATIQUE C EST SUPER'
```

3. En utilisant la fonction `chiffre_cesar`, écrire un programme Python qui essaye toutes les clefs possibles et retrouver alors le message d'origine correspondant au message chiffré :

   `'QNAF Y NEVGUZRGVDHR QR Y NZBHE HA CYHF HA RTNYR GBHG RG QRHK ZBVAF HA RTNYR EVRA'`

Indication La fonction `ord` permet d'avoir l'unicode correspond à un caractère.

```
>>> ord('A')
65
```

La fonction `chr` permet d'avoir le charactère correspondant à un unicode donné.

```
>>> chr(65)
'A'
```

L'opérateur «`a%b`» permet de calculer le reste de la division euclidienne de `a` par `b`.

```
>>> 30%26
4
```

Exercice 2.
Ecrire une fonction Python `chiffre_xor(msg, clef)` qui pren en argument eux chaînes d'octets (type `bytes`) et qui renvoie le chiffrement XOR du message avec la clef, sous la forme d'une chaîne d'octets.

```
>>> msg = "L'informatique c'est super!".encode()
>>> clef = "NSI".encode()
>>> msgc = chiffre_xor(msg,clef)
>>> msgc
b"\x02t  5&<>(::8;6i-t,='i=&9+!h"
>>> chiffre_xor(msgc,clef).decode()
"L'informatique c'est super!"
```

Indication Le constructeur `bytes` créer une chaîne d'octets à partir d'une liste d'entiers.

```
>>> L = [1, 2, 3, 4, 5]
>>> bytes(L)
b'\x01\x02\x03\x04\x05'
```

Exercice 3.
Soit la chaîne d'octets chiffrée à l'aide du chiffrement XOR :

```
b'\x0e6/+y;.<x-(7,,\x9b\xf0z48z:646<z*\x9a\xf3(64+<{'
```

On sait que les 4 derniers caractères du message en clair sont `nse!`. On sait aussi que la clef fait exactement 3 caractères et que ce sont des lettres majuscules sans accent.
Ecrire un programme Python, utilisant la fonction `chiffre_xor` de l'exercice précédent, qui essaye toutes les combinaisons de clef jusqu'à trouver la bonne. Mesurer le temps d'exécution.

Exercice 4.
Ecrire une fonction `factorisation(n)` qui prend en paramètre un entier n et renvoie un couple d'entier (p, q) tel que $n = p \times q$ avec $1 < p <= q$ si n n'est pas premier et $p = 1$, $q = n$ si n est premier.
Trouver alors deux nombres p et q tels que $p \times q = 906555947934709$ puis tels que $p \times q = 17063866208590147$.
Mesurer le temps d'exécution.

Exercice 5.
Ecrire une fonction `log_discret(gu, g, p)` qui déterminer l'entier u tel que le reste de la division euclidienne de g^u par p soit égale à gu.
Mesurer alors le temps d'exécution des appels suivants :

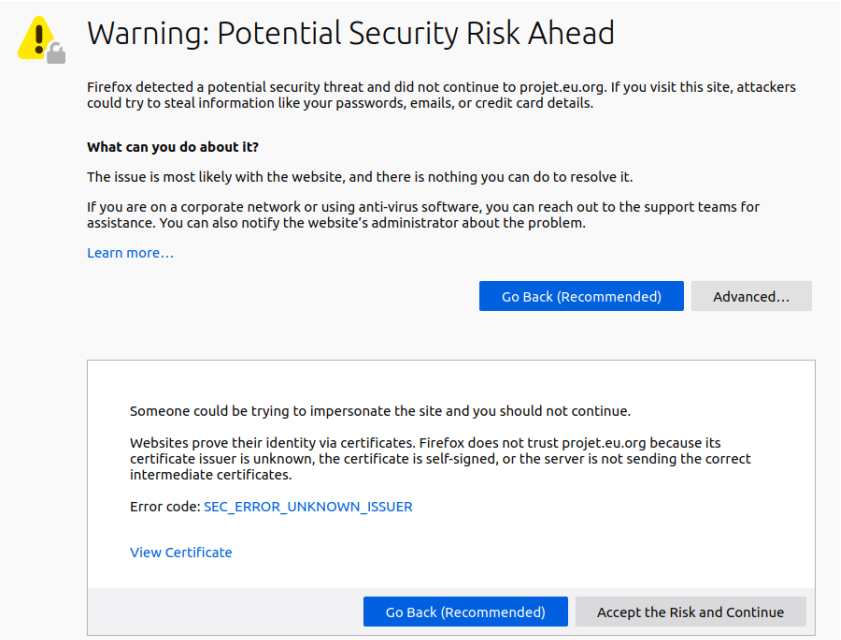
```
>>> log_discret(273213231, 7, 934741963)
>>> log_discret(360223736, 7, 934741963)
```

Indication pour calculer le reste de la division euclidienne de g^u par p on pourra utiliser `pow(g, u, p)`.

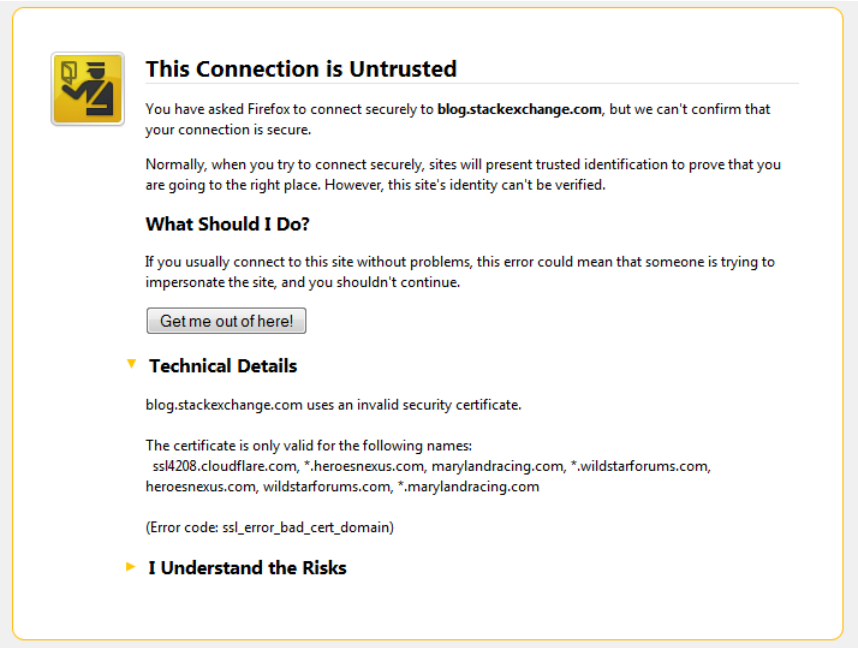
Exercice 6.
Télécharger le certificat du site `education.gouv.fr`. Utiliser la commande `openssl` pour déterminer les informations de ce certificat.

Exercice 7.
Donner une explication détaillée aux messages d'erreurs suivants :

1. Connexion au site `https://projet.eu.org`



2. Connexion au site blog.stackexchange.com



Exercice 8.
1. Qu'est ce qu'un certificat X.509 et quelles sont les pricipales informations qu'il contient ?
2. Discuter les scénarios suivants en termes de sécurité :
   (a) Deux certificats différents sont signés par la même clef privée.
   (b) Deux certificats différents contiennent la même clef publique.
   (c) Deux certificats différents ont le même sujet.
   (d) Deux certificats différents ont le même émetteur.

Exercice 9.
On considère le cas d'un site Intrnet `https///www.monsite.fr`. Ce dernier a été mal configuré et le fichier `privkey.pem`, contenant la clef privée correspondant à la clef publique contenue dans le certificat, est téléchargeable. Indiquer ce que peut faire un utilisateur malveillant en possession de cette clef.