CERTIF ACADEMY

HTTPS

CERTIF ACADEMY

1. Attaque MITM
2. Architecture de la solution
3. Exposition NAT du port 443 et configuration de la clé publique et de la clé privée

CERTIF ACADEMY

Attaque MITM

CERTIF ACADEMY

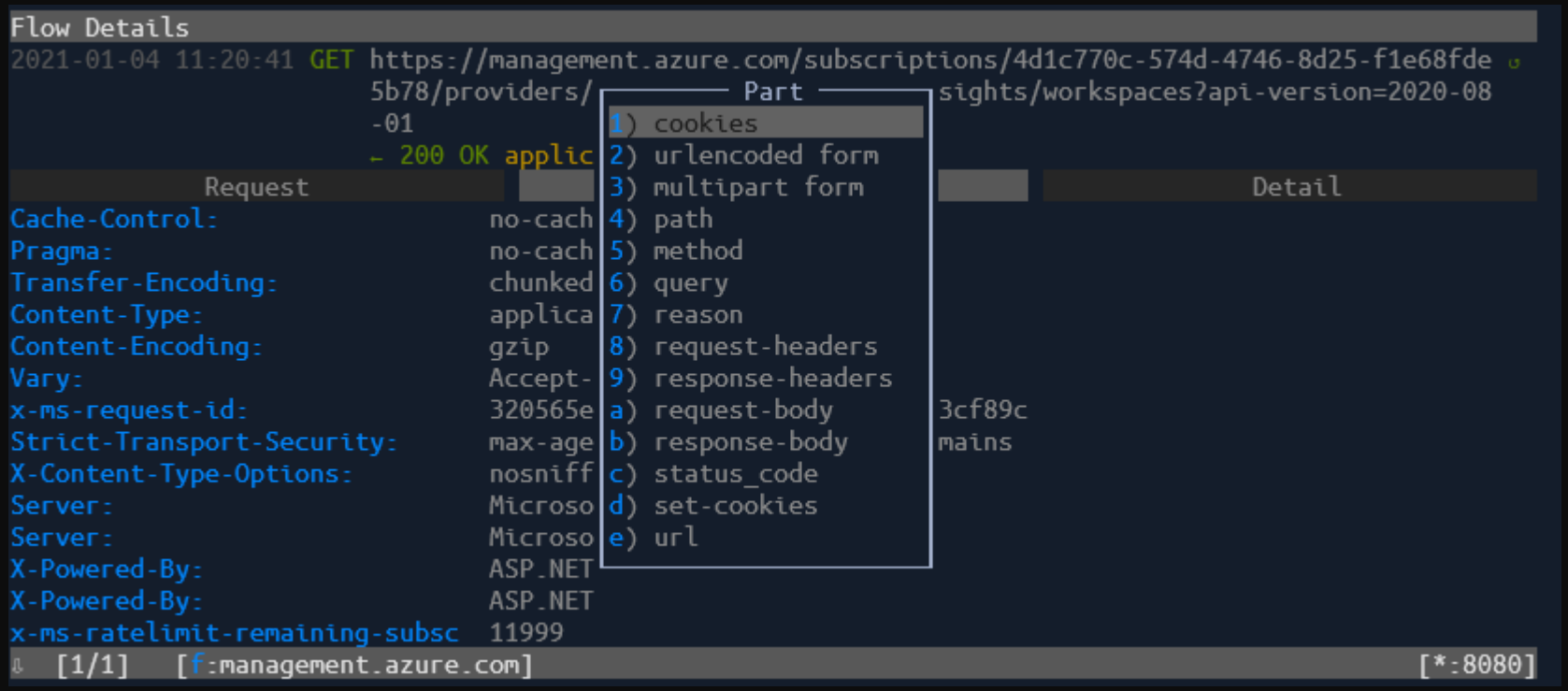
Payload

HTML

CERTIF ACADEMY

Starbucks Fibre
(fake)

CERTIF ACADEMY



On peut consulter les cookies, forcer un setcookie etc. nous pouvons tout faire

CERTIF ACADEMY

Architecture de la solution

CERTIF ACADEMY

A votre avis, qu‘est-ce que HTTPS a en plus que HTTP ?

CERTIF ACADEMY

Le protocol HTTPS spécifie les conventions suivantes dans une communication :

- Le destinataire est spécifié par une URL (un lien)
- Une méthode spécifie le moyen de transport des données (GET ou POST)
- Les données seront cryptées par une clé symétrique

CERTIF ACADEMY

A votre avis qu‘est-ce qu‘une clé ?

CERTIF ACADEMY

La cryptographie symétrique

CERTIF ACADEMY

Un petit exemple …

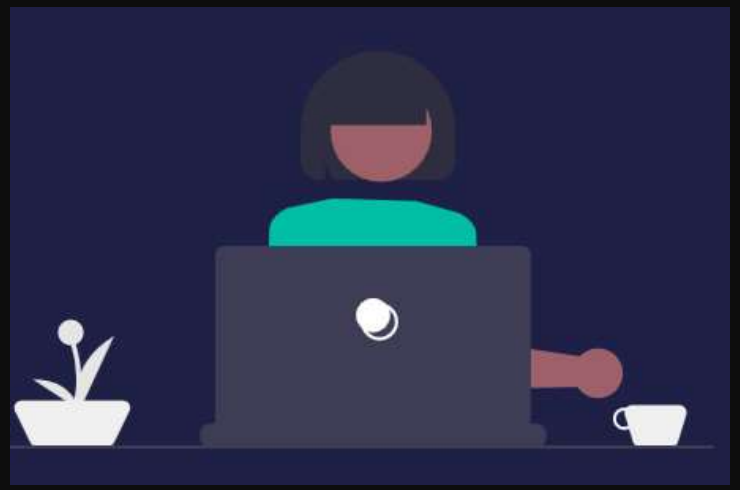
Pour simplifier le problème, nous allons prendre un exemple basé sur le décalage des lettres dans un message.

Dans la réalité, c'est beaucoup plus compliqué et implique beaucoup de mathématiques !

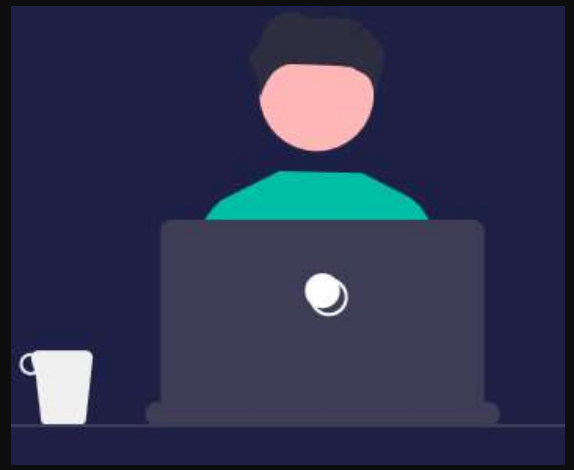
CERTIF ACADEMY

Je vous présente ...

Alice



Bob



CERTIF ACADEMY

Besoin : Alice souhaite communiquer avec Bob sur la sale coupe de cheuveux de son responsable Colin

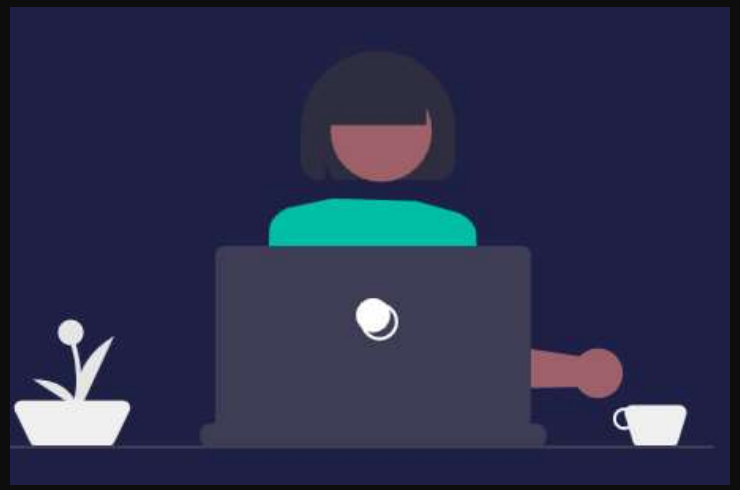
Problème : Alice a peur que son responsable Colin fasse une attaque MITM et lise son message pour Bob

Solution : Alice communique une clé et un cipher à Bob pour cacher leur message (crypter le message)

CERTIF ACADEMY

Exemple cryptographie symétrique

Alice



Alice choisit « 5 » comme clé

Alice choisit « le decalage de lettres » comme cipher

Alice transmet ces 2 choses à Bob à l'avance en cachette

CERTIF ACADEMY

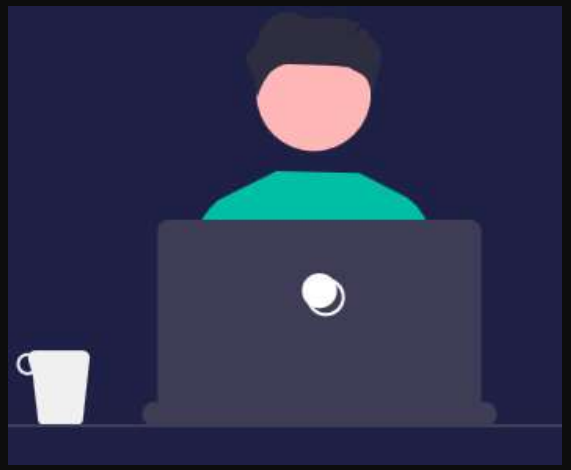
Exemple cryptographie symétrique

Bob dit :

Ok Alice, la clé est « 5 »

Ok Alice, le cipher est le « décalage de lettres »

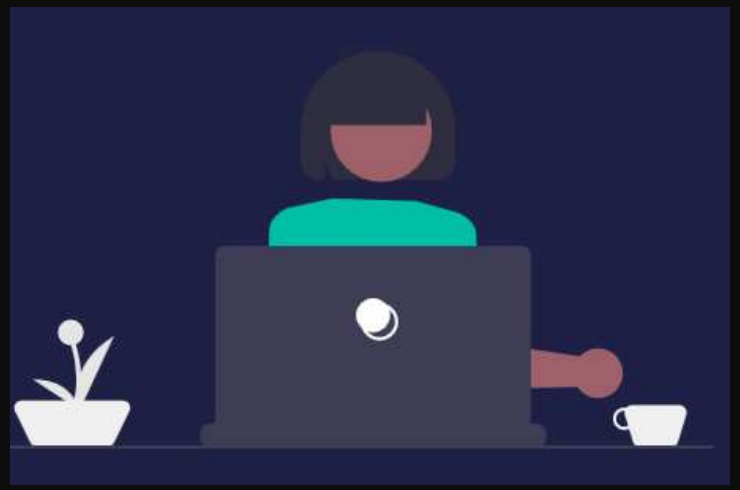
Bob



CERTIF ACADEMY

1. Processus de chiffrage symétrique

Alice



Alice veut dire « Colin a une sale coupe » à Bob.

Elle va exécuter le cipher avec la clé, donc elle va décaler les lettres de 5 et obtenir :
« Htqns%f%zsj%xfqj%htzuj »

CERTIF ACADEMY

Pourquoi « Colin a une sale coupe » donne « Htqns%f%zsj%xfqj%htzuj » une fois chiffré ?

CERTIF ACADEMY

On utilise le cipher (c'est la méthode de cryptage) :
« décalage de lettres »

On utilise la clé (c'est un nombre) pour savoir de combien de lettres on doit décaler : c'est 5

Donc « Colin », donne « Htqns » car :
« C » 5 lettres après, donne « H »
« o » 5 lettres après donne « t »,
« l » 5 lettres après donne « q »,
« i » 5 lettres après donne « n »,
« n » 5 lettres après donne « s »

Et ainsi de suite …

CERTIF ACADEMY

Donc le message :

« Colin a une sale coupe »

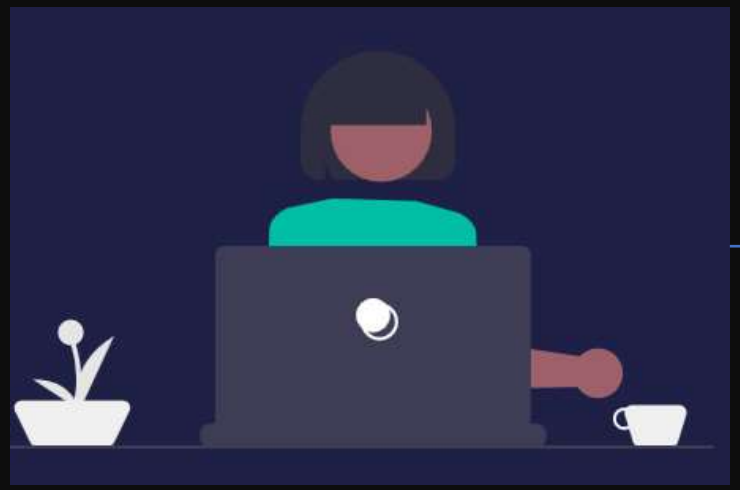
Est crypté en :

« Htqns%f%zsj%xfqj%htzuj »

CERTIF ACADEMY

Alice a chiffré son message !

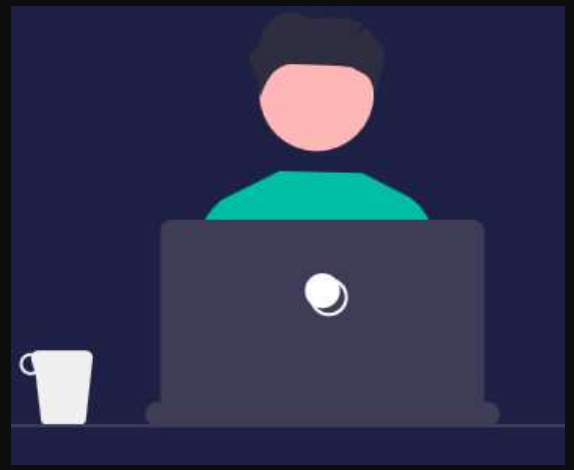
Alice



« Colin a une salle coupe »

« Htqns%f%zsj%xfqj% htzuj »

Bob

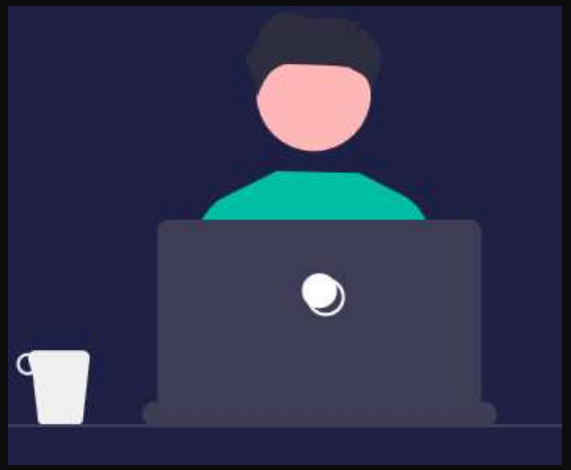


CERTIF ACADEMY

2. Processus de déchiffrage symétrique

Bob a recu «Htqns%f%zsj%xfqj%htzuj » de la part d'Alice, il va donc utiliser la clé et le cipher pour déchiffrer le message.

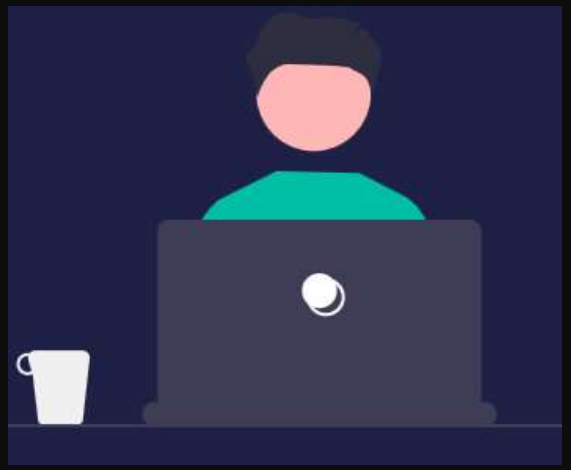
Bob



CERTIF ACADEMY

Bob fait donc l’opération inverse :
Donc « Htqns », donne « Colin » car :
« H » 5 lettres avant, donne « C »
« t » 5 lettres avant donne « o »,
« q » 5 lettres avant donne « l »,
« n » 5 lettres avant donne « i »,
« s » 5 lettres avant donne « n »

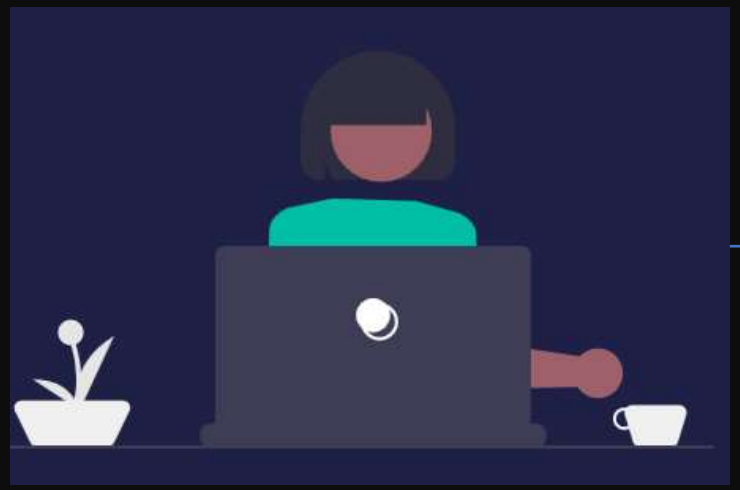
Bob



CERTIF ACADEMY

Bob a déchiffré le message !

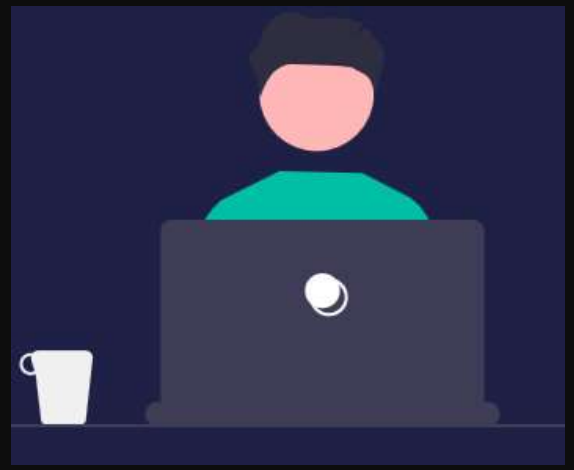
Alice



« Colin a une salle coupe »

« Htqns%f%zsj%xfqj% htzuj »

Bob



« Colin a une salle coupe »

CERTIF ACADEMY

Que se passe-t-il si Colin fait une attaque MITM ?

CERTIF ACADEMY

Colin ne va rien comprendre !!

CERTIF ACADEMY

Lorsque les messages sont cryptés, une attaque MITM est-elle possible ?

CERTIF ACADEMY

Il n‘est pas possible (ou très difficilement) de faire une attaque MITM lorsque la communication est chiffrée symétriquement

CERTIF ACADEMY

Fin de l‘exemple sur la cryptographie symétrique

CERTIF ACADEMY

On appelle cryptographie symétrique toute cryptographie entre 2 parties (comme Alice et Bob) impliquant 1 même clé des 2 côtés (Alice utilise la même clé que Bob)

CERTIF
ACADEMY

CERTIF ACADEMY

Quelqu’un voit-il un problème ?
Est-ce que la cryptographie symétrique suffit ?

CERTIF ACADEMY

Sauf … que se passe-t-il si Colin fait une attaque MITM au moment où Alice donne la clé et la cipher à Bob ?

CERTIF ACADEMY

Colin sera aussi dans la capacité de déchiffrer les messages !! Zut !! =(

CERTIF ACADEMY

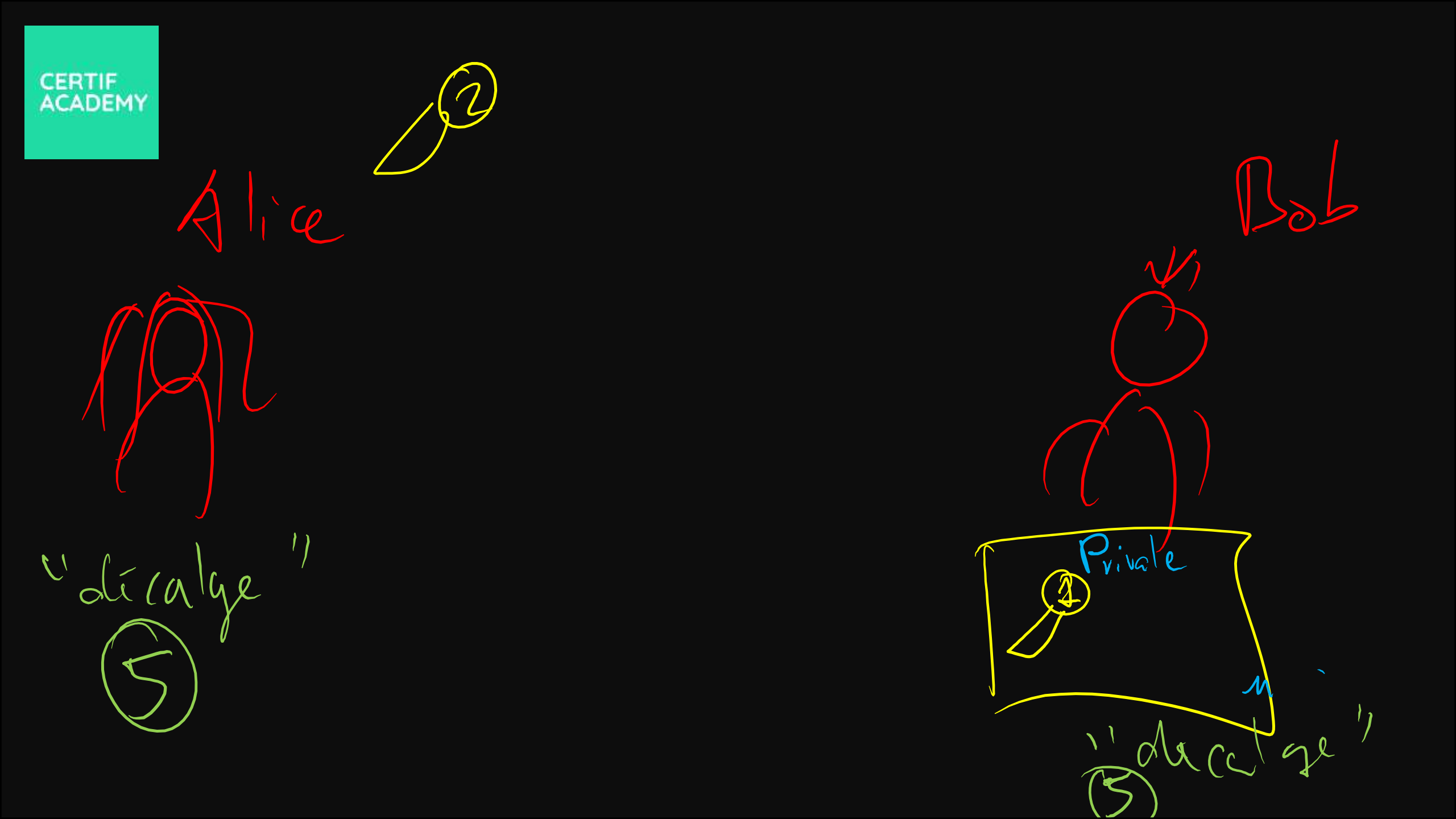
A votre avis, comment peut-on empêcher Colin de voir l'échange de la clé symétrique de Alice vers Bob ? (attention c'est plus dur)

CERTIF ACADEMY

Pour s'assurer que Alice donne sa clé et son cipher en cachette à Bob, nous alons utiliser la cryptographie asymétrique !

La cryptographie asymétrique est lente (alors que la cryptographie symétrique est rapide), mais assure à 100% (en théorie) que les informations sont données en cachette

CERTIF ACADEMY



CERTIF
ACADEMY

CERTIF ACADEMY

L‘idée globale devient ainsi que :

1. Alice choisisse la clé et le cipher
2. Alice envoie tout ca à Bob en cryptographie asymétrique (même si c‘est lent) 100% en cachette
3. Bob recoit la clé et le cipher
4. Alice et Bob communique en cryptographie symétrique avec cette clé et le cipher (c‘est rapide)

CERTIF ACADEMY

Pre-master key

L'idée globale devient ainsi que :

1. Alice choisisse la clé et le cipher
2. Alice envoie tout ca à Bob en cryptographie asymétrique (même si c'est lent)
3. Bob recoit la clé et le cipher
4. Alice et Bob communique en cryptographie symétrique avec cette clé et le cipher (c'est rapide)

Negociation process

Bulk encryption-decryption process

CERTIF ACADEMY

Une cryptographie asymétrique se base sur 2 clés différentes :

- Une clé dite publique
- Une clé dite privée

CERTIF ACADEMY

Nous n‘allons pas voir la cryptographie asymétrique qui est plus compliquée et nécessite davantage de mathématiques.

CERTIF ACADEMY

Ce processus global est le mécanisme du chiffrage des données utilisées par HTTPS :

1. Alice choisisse la clé et le cipher
2. Alice envoie tout ca à Bob en cryptographie asymétrique (même si c'est lent)
3. Bob recoit la clé et le cipher
4. Alice et Bob communique en cryptographie symétrique avec cette clé et le cipher (c'est rapide)

CERTIF ACADEMY

On remplace Alice par le navigateur et Bob par le serveur et on obtient :

1. ~~Alice~~ Le navigateur choisisse la clé et le cipher
2. ~~Alice~~ Le navigateur envoie tout ca ~~à Bob~~ au serveur en cryptographie asymétrique (même si c'est lent)
3. ~~Bob~~ Le serveur recoit la clé et le cipher
4. ~~Alice et Bob~~ Le navigateur et le serveur communique en cryptographie symétrique avec cette clé et le cipher (c'est rapide)

CERTIF ACADEMY

La seule clé nécessaire pour faire démarrer tout le processus de cryptographie des données est la clé publique de la cryptographie asymétrique.

Tout le reste en découle automatiquement entre le navigateur et le serveur.

CERTIF ACADEMY

La clé publique est détenue par le serveur et est consignée dans un fichier appelé : certificat SSL

Le certificat SSL contient donc la clé publique qui permet tout le processus de cryptographie des données entre le navigateur et le serveur

CERTIF ACADEMY

Le SSL (Secure Sockets Layer) et son successeur TLS (Transport Layer Security) sont des protocols cryptographiques utilisés pour crypter les communications entre logiciels

CERTIF ACADEMY

HTTPS = HTTP + TLS !

CERTIF ACADEMY

Conclusion : comment faire pour parer les attaques MITM ?

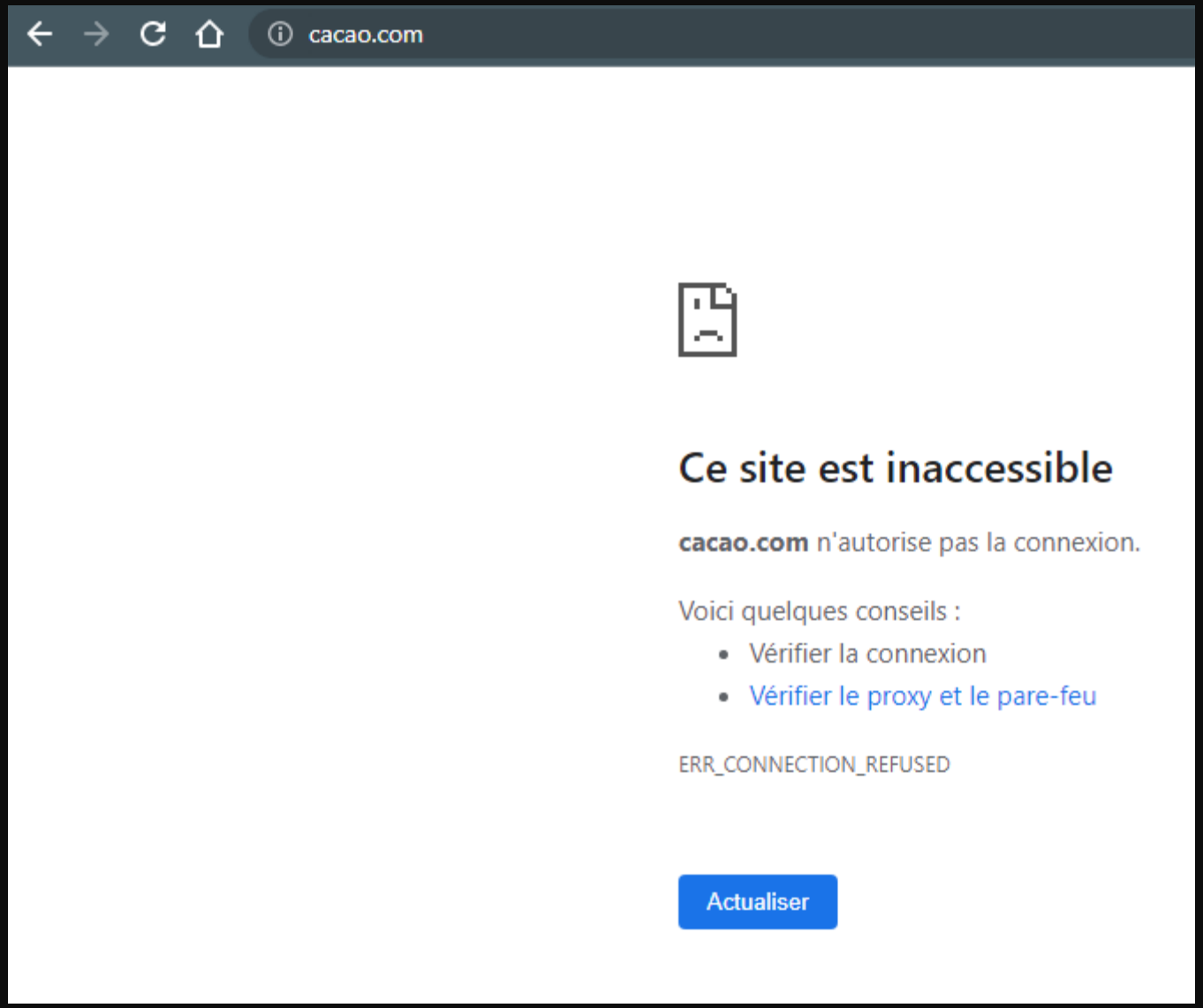
CERTIF ACADEMY

Utiliser le protocol HTTPS !

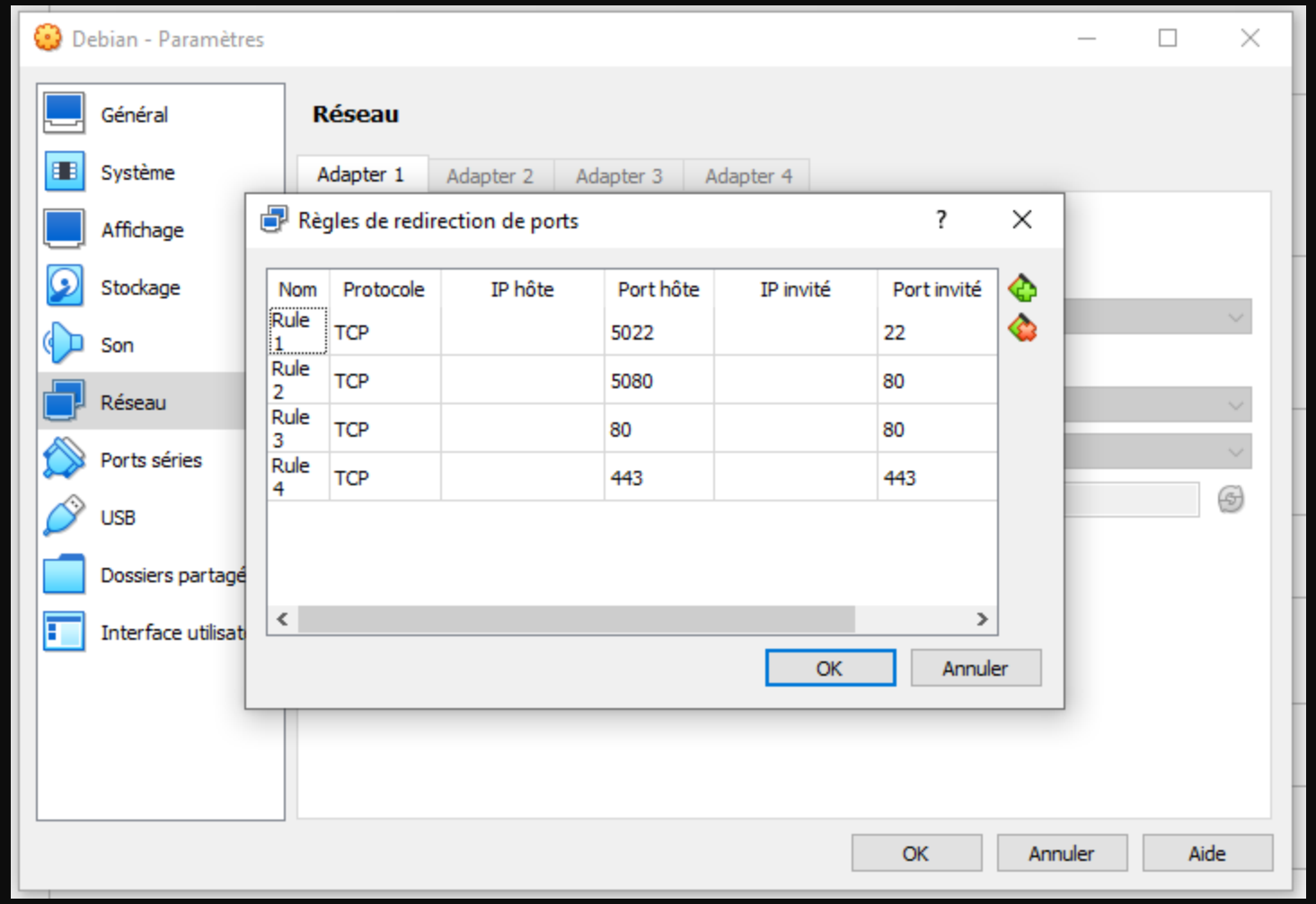
CERTIF ACADEMY

Exposition NAT du port 443 et configuration de la clé publique et privée

CERTIF ACADEMY



CERTIF ACADEMY



CERTIF ACADEMY

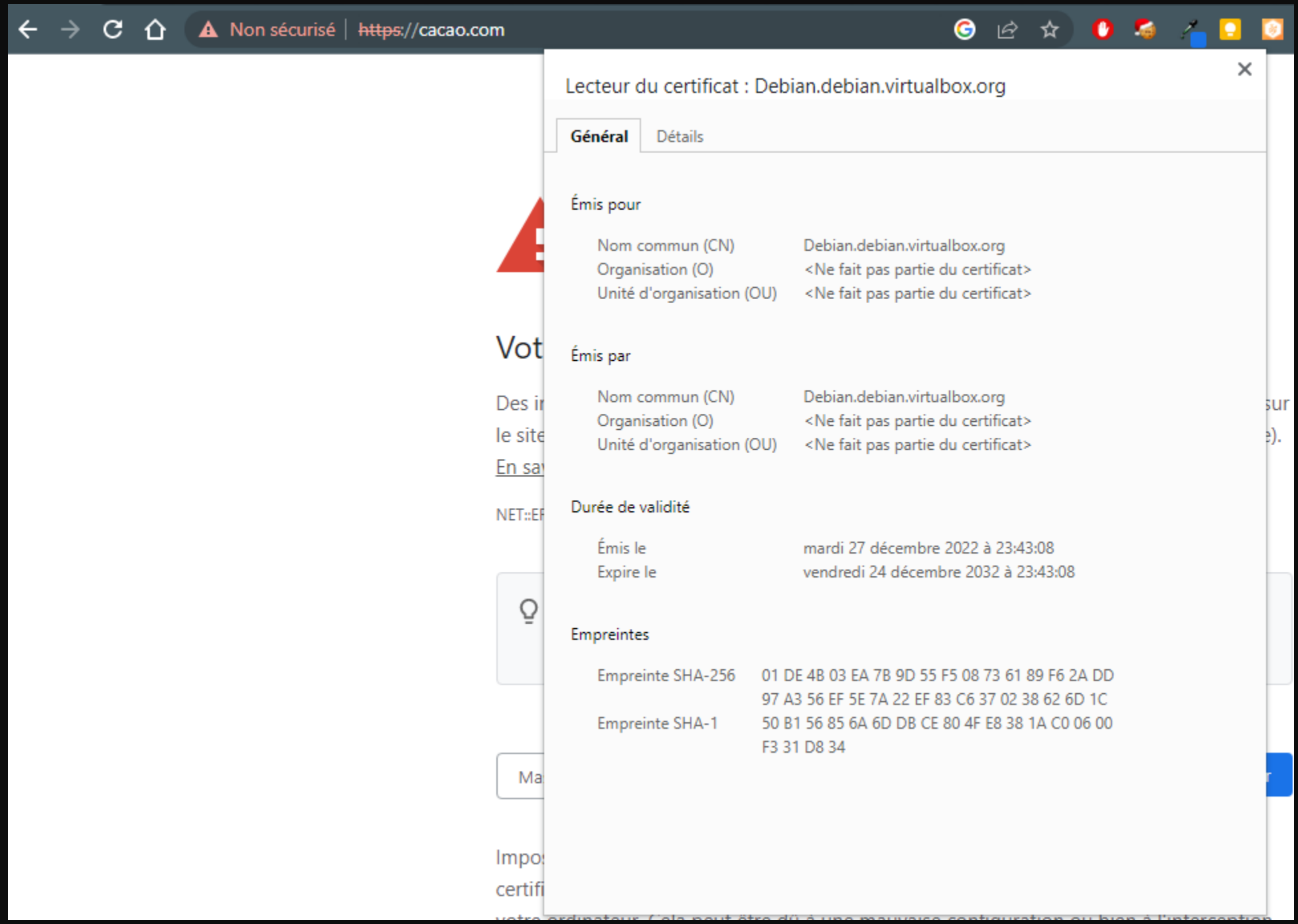
```
a2enmod ssl
```

CERTIF ACADEMY

```
<VirtualHost *:443>
    ServerName cacao.com
    ServerAlias www.cacao.com
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/cacao.com
    ErrorLog ${APACHE_LOG_DIR}/error-cacao.com.log
    CustomLog ${APACHE_LOG_DIR}/access-cacao.com.log combined

    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
    SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
</VirtualHost>
```

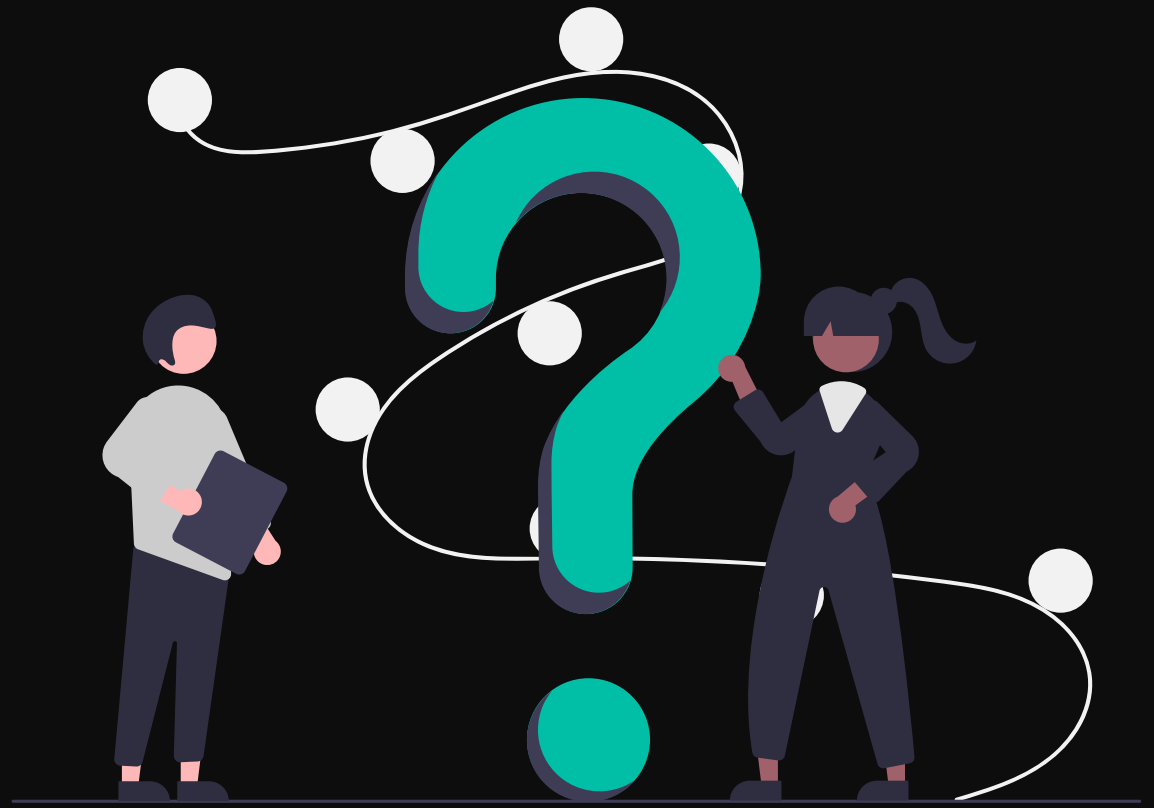
CERTIF ACADEMY



CERTIF ACADEMY

Sécurisez vos applications en HTTPS

CERTIF ACADEMY



CERTIF
ACADEMY