



Une formation
Alphorm.com

Formation OpenSSL *Cryptage des données*



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan de la formation

Introduction

1. Introduction au OpenSSL
2. Crypter et décrypter avec OpenSSL
3. Gérer les certificats
4. Signer un message
5. Tester avec Openssl

Conclusion



Public concerné

Toutes personne qui a peu ou pas d'expérience dans le domaine de la cryptographie, et qui est curieuse de comprendre enfin les concepts pratiques
Ingénieurs qui sont intéressés par les techniques du cryptage et le hashing

Une formation
Alphorm.com



Connaissances requises

Les bases du cryptage et avoir quelques connaissances dans le domaine des certificats et les signatures

Avoir des connaissances sur la sécurité et la cryptographie

Une formation
Alphorm.com



Formations pour les prérequis



Une formation
Alphorm.com





Présentation du Lab de travail



Mohamed Anass EDDIK

Une formation
Alphorm.com



Les prérequis du Lab

Une machine Windows

Une machine linux CentOS

L'exécutable de l'OpenSSL (*dossier
ressources*)

Une formation
Alphorm.com



Vous êtes prêt(e)s ?



Installer OpenSSL sur Windows



Mohamed Anass EDDIK



Plan

Prérequis

Téléchargement

Le fichier **openssl.cfg**

Une formation
Alphorm.com



Prérequis

Windows XP+

Windows Lite + quelques composants

128MB RAM

1GHz CPU

Une formation
Alphorm.com



Téléchargement

<https://slproweb.com/products/Win32OpenSSL.html>

<https://wiki.openssl.org/index.php/Binaries>

Une formation
Alphorm.com

Le fichier openssl.cfg

```
OPENSSL_CONF=C:\OpenSSL-Win32\bin\openssl.cfg
```

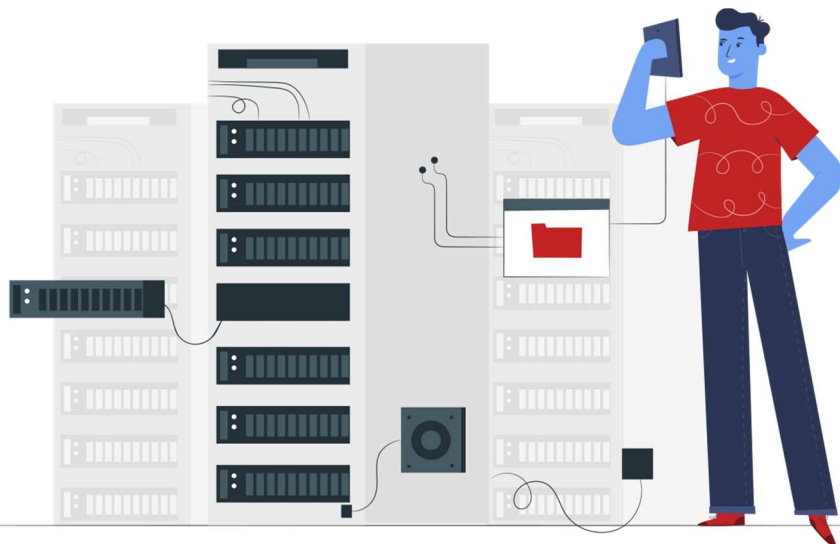
OpenSSL

Cryptography and SSL/TLS tools

Cryptage des données

Une formation
Alphorm.com

Démo



OpenSSL

Cryptography and SSL/TLS tools

Cryptage des données

Une formation
Alphorm.com

Installer OpenSSL sur Linux



Mohamed Anass EDDIK



Plan

Etapes à suivre
Configurer la Librairie
partagée OpenSSL

Une formation
Alphorm.com



Etapes à suivre

Mise à jour du système (recommandé)
Installer l'outil de développement
Télécharger l'OpenSSL
Installer l'OpenSSL

Une formation
Alphorm.com

OpenSSL

Cryptage des données

Configurer la Librairie partagée OpenSSL

Librairie de partage

```
cd /etc/ld.so.conf.d/
```

Binaire OpenSSL

```
sudo mv /bin/openssl /bin/openssl.backup
```

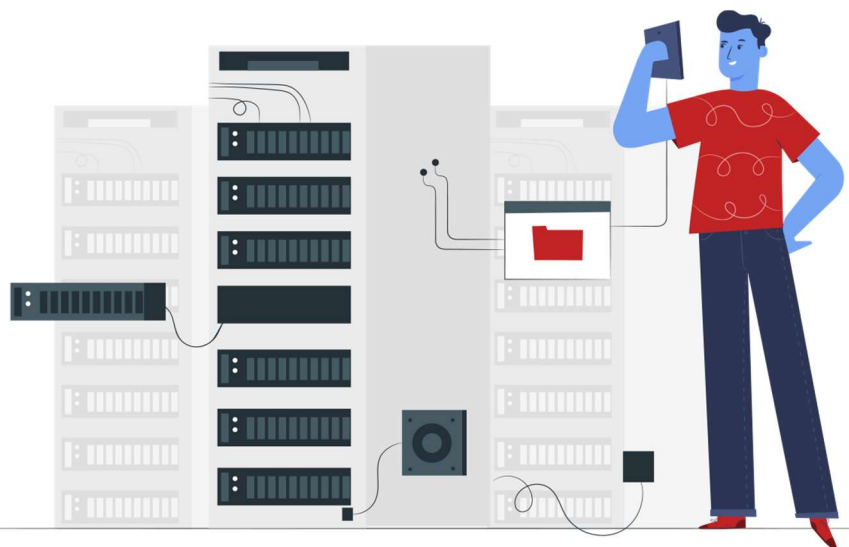
```
sudo nano /etc/profile.d/openssl.sh
```

Une formation
Alphorm.com

OpenSSL

Cryptage des données

Démo



Une formation
Alphorm.com



Installer OpenSSL sur Linux Partie 2



Mohamed Anass EDDIK

Une formation
Alphorm.com



Comprendre le cryptage symétrique



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Principes de base
Modes Opérationnels
Avantages et limitations

Une formation
Alphorm.com



Principes de base

Une formation
Alphorm.com



Une formation
Alphorm.com

Modes Opérationnels

Cryptage par flux (Stream Cipher)

Traite les éléments d'entrée de façon continue, produisant un élément de sortie (crypté)

Ce mode est adapté pour la communication en temps réel : pas besoin du bloc entier

Implémenté en général sur de support hardware

Cryptage par bloc (Bloc Cipher)

Le texte est divisé en plusieurs blocs de taille fixe, chaque bloc est traité à la fois, ce qui va produire un block de données cryptées

Implémentation d'une manière logicielle en général



Une formation
Alphorm.com

Avantages et limitations

Avantages

Confidentialité des données

Rapidité et facilité de mise en œuvre sur des circuits

Limitations

Problème de l'échange de la clé de chiffrement

La partie tierce ne peut pas s'assurer de l'authenticité des messages

Problème de la distribution des clés de cryptages

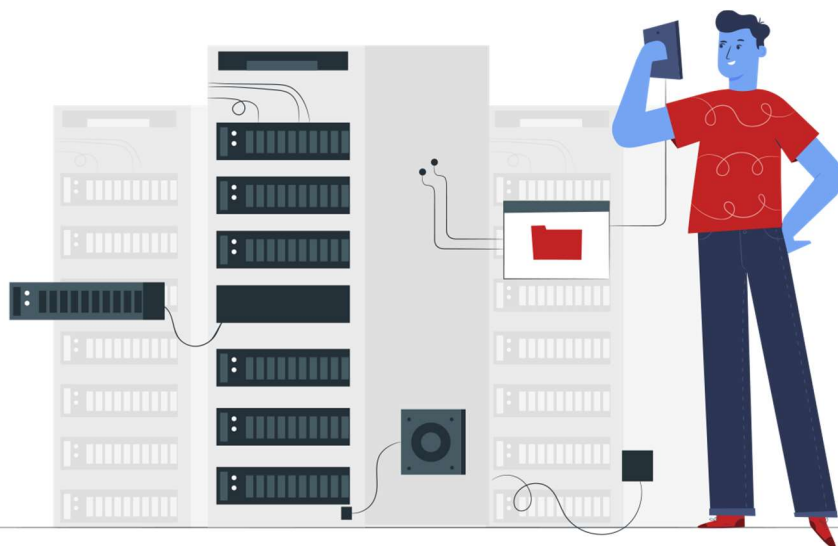
OpenSSL

Cryptography and SSL/TLS tools

Cryptage des données

Une formation
Alphorm.com

Démo



OpenSSL

Cryptography and SSL/TLS tools

Cryptage des données

Une formation
Alphorm.com

Comprendre le décryptage symétrique



Mohamed Anass EDDIK



Plan

Caractéristique du
chiffrement par flux
Fonctionnement

Une formation
Alphorm.com



Caractéristique du chiffrement par flux

Pas besoin de lire le message ni
d'avoir sa longueur pour commencer
à chiffrer

Génération du flux de clé (keystream)
que l'on combine avec le flux de
données

Une formation
Alphorm.com



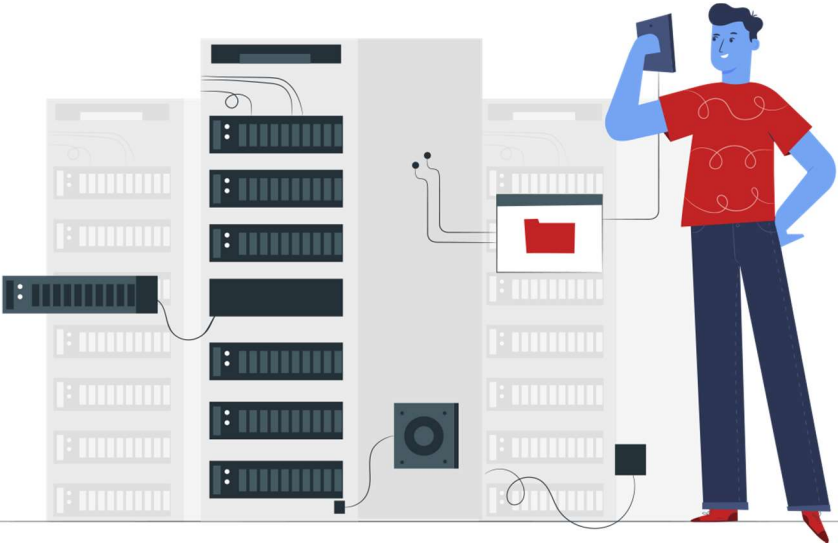
Fonctionnement

Une formation
Alphorm.com



Démo

Une formation
Alphorm.com





Une formation
Alphorm.com

Comprendre le cryptage asymétrique



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

La Différence du Symétrique
Scénario de fonctionnement
Avantages et inconvénients



Une formation
Alphorm.com

La différence du Symétrique

Révolution dans l'histoire de la cryptographie

Utilise deux clés :

1. Clé publique
2. Clé privé

Si on crypte avec l'une des ces clés le
décryptage se fait uniquement avec l'autre

Impossible de trouver la clé privée à partir de la
clé publique



Une formation
Alphorm.com

Scenario de fonctionnement

OpenSSL

Cryptography and SSL/TLS tools

Cryptage des données

Une formation
Alphorm.com

Avantages et inconvénients

Avantages

Pas besoin d'établir un canal sûr pour la transmission de la clé
Plusieurs fonctions de sécurité: confidentialité, authentification, et non-répudiation

Inconvénient

Généralement dix fois plus lent que le cryptage symétrique
Problème d'implémentation sur les équipements disposants de faible puissance de calcul (carte bancaire, stations mobiles,...)

OpenSSL

Cryptography and SSL/TLS tools

Cryptage des données

Une formation
Alphorm.com

Démo





Comprendre le décryptage asymétrique



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

L'authentification Algorithme

Une formation
Alphorm.com



L'authentification

Le cryptage asymétrique permet aussi l'authentification :

- Quand l'émetteur chiffre avec la clé publique du récepteur, seul ce dernier peut déchiffrer avec sa clé privée
- Seul le récepteur qui peut déchiffrer avec sa clé privée

Une formation
Alphorm.com



Algorithme

RSA

Le plus connu et le plus utilisé comme algorithme de cryptage asymétrique, il est utilisé pour le cryptage et la signature électronique

Diffie-Hellman

Algorithme utilisé pour l'échange et la distribution des clés symétriques

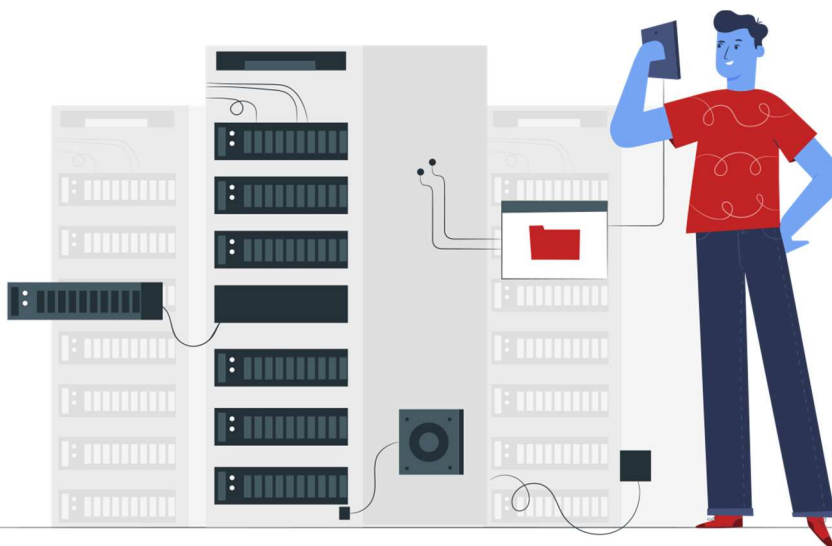
Une formation
Alphorm.com

OpenSSL

Cryptography and SSL/TLS tools

Cryptage des données

Démo



Une formation
Alphorm.com

OpenSSL

Cryptography and SSL/TLS tools

Cryptage des données

Créer un CSR avec OpenSSL



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

C'est quoi un CSR ? Etapes de création de CSR

Une formation
Alphorm.com



C'est quoi un CSR ?

CSR : Certificat Signature Request (demande de signature de certificat)

Une demande de signature de certificat (CSR) est l'une des premières étapes à accomplir pour obtenir un certificat SSL, elle doit être créée sur le serveur sur lequel le certificat sera installé et que l'autorité de certification (AC) utilisera pour créer le certificat

Une formation
Alphorm.com

OpenSSL

Cryptography and SSL/TLS tools

Cryptage des données

Etapes de création de CSR

Avant de créer un CSR on a besoin impérativement de la clé privé du serveur :

```
genrsa-des3-out www.alphorm.com.key 2048
```

Générer mon CSR avec la cmd :

```
req-new-key www.alphorm.com.key -out  
www.alphorm.com.csr
```

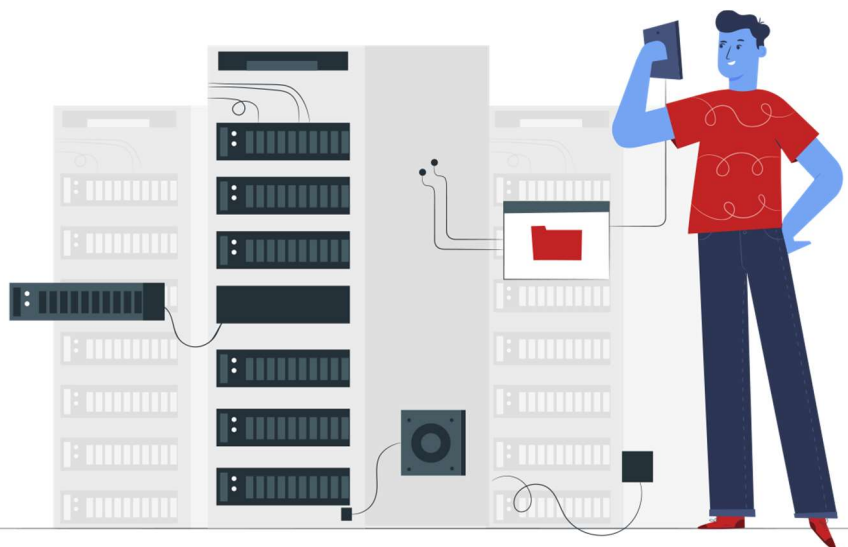
Une formation
Alphorm
com

OpenSSL

Cryptography and SSL/TLS tools

Cryptage des données

Démo



Une formation
Alphorm
com



Créer CSR depuis un certificat existant



Mohamed Anass EDDIK

Une formation
Alphorm.com



Inconvénient

Sauf si vous utilisez une certaine forme d'épinglage de clés publiques et que vous souhaitez continuer à utiliser la clé existante, il est préférable de générer une nouvelle clé à chaque fois que vous postulez pour un nouveau Certificat

La génération des clés est rapide et peu coûteuse et réduit votre exposition

Une formation
Alphorm.com

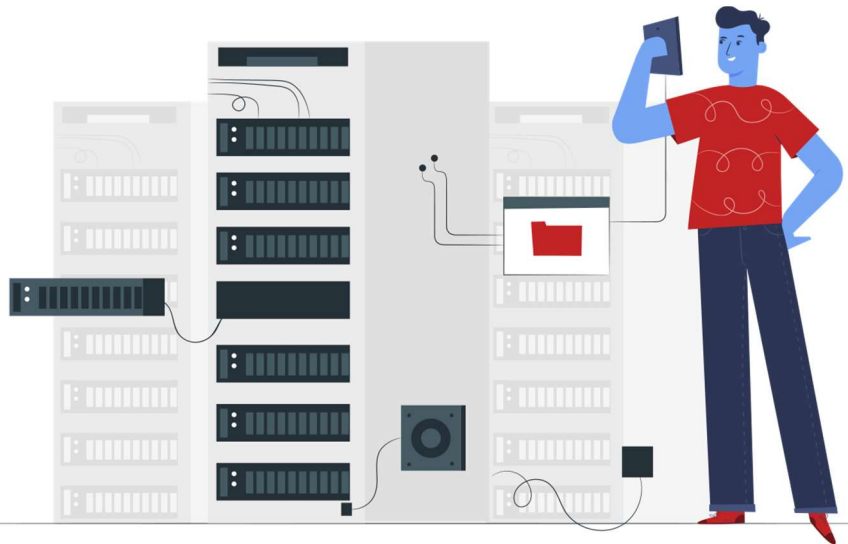
OpenSSL

Cryptography and SSL/TLS tools

Cryptage des données

Une formation
Alphorm.com

Démo



OpenSSL

Cryptography and SSL/TLS tools

Cryptage des données

Une formation
Alphorm.com

Signer un message



Mohamed Anass EDDIK



Plan

Pourquoi il faut une signature
Génération de la signature
Vérification de la signature

Une formation
Alphorm.com



Pourquoi il faut une signature

La signature électronique permet
d'authentifier de manière fiable l'auteur du
fichier et de s'assurer que le contenu de
celui-ci n'a pas été altéré ou modifié

Du coup si on a un fichier signé alors il est
authentique depuis le point de départ vers
le point d'arrivée

Une formation
Alphorm.com



Génération de la signature

Une formation
Alphorm.com



Vérification de la signature

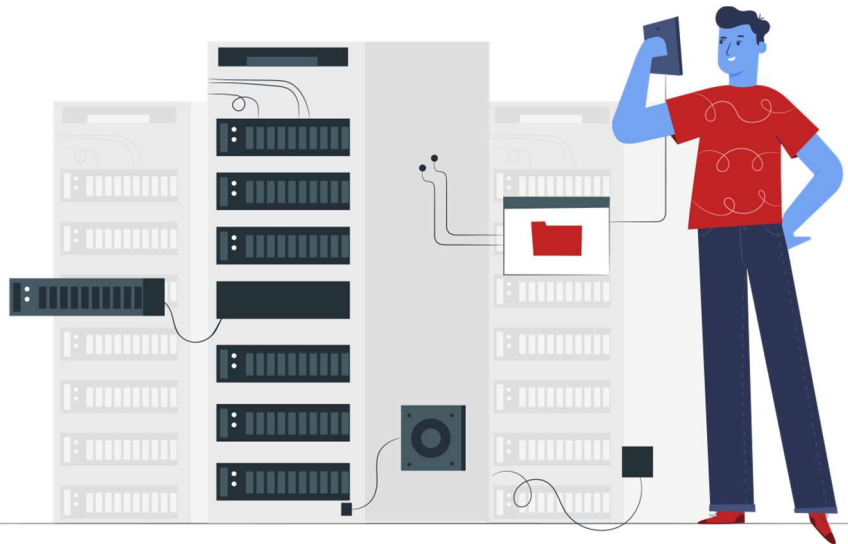
Une formation
Alphorm.com

OpenSSL

Cryptography and SSL/TLS tools

Cryptage des données

Démo



Une formation
Alphorm.com

OpenSSL

Cryptography and SSL/TLS tools

Cryptage des données

Le hashing



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Principe du hachage Fonction du hachage

Une formation
Alphorm.com



Principe du hachage

La fonction du hachage permet d'extraire
une empreinte qui caractérise les données
Calcul facile et rapide , il est plus rapide que
le cryptage symétrique

Une formation
Alphorm.com

OpenSSL

Cryptography and SSL/TLS tools

Cryptage des données

Fonction du hachage

MD5: Génère une empreinte de taille 128 bits en traitant les données d'entrée par blocs

SHA-1: Génère une empreinte de taille 160 bits, et il est plus fort que le MD5

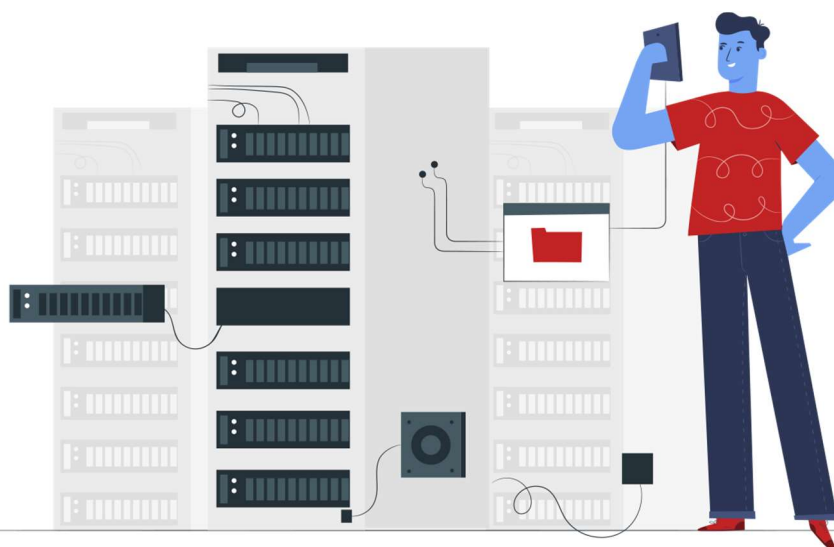
Une formation
Alphorm.com

OpenSSL

Cryptography and SSL/TLS tools

Cryptage des données

Démo



Une formation
Alphorm.com



Une formation
Alphorm.com

Tester les protocoles



Mohamed Anass EDDIK



Une formation
Alphorm.com

Block Cipher modes



Mohamed Anass EDDIK



Plan

Algorithmes du block cipher Comment l'utiliser ?

Une formation
Alphorm.com



Algorithmes du block cipher

Electronic Codebook Mode (ECB)

Le même bloc de texte ordinaire produit toujours le même bloc de chiffrement (pour la même clé) ce qui le rend vulnérable à une « attaque de dictionnaire »

Une formation
Alphorm.com



Algorithmes du block cipher

Cipher Block Chaining Mode (CBC)

L'opération d'enchaînement rend les blocs de chiffrement dépendants du courant et de tous les blocs de texte clair précédents et donc les blocs ne peuvent pas être réarrangés

L'utilisation de différentes variables de départ empêche la même gravure en texte clair au même texte de chiffrement

Une formation
Alphorm.com



Algorithmes du block cipher

Cipher Feedback Mode (CFB)

L'opération d'enchaînement rend les variables de texte de chiffrement dépendantes des variables actuelles et toutes les variables précédentes et donc les variables sont enchaînées et ne peuvent pas être réarrangées

Une formation
Alphorm.com

OpenSSL

Cryptography and SSL/TLS tools

Cryptage des données

Comment l'utiliser?

\$ openssl enc -ciphertype

L'utilisation de base est de spécifier un nom de chiffrement et diverses options décrivant la tâche réelle

\$ openssl list-cipher-algorithms

On peut utiliser cette commande pour lister les différents cipher disponibles sur cette version de mon openssl

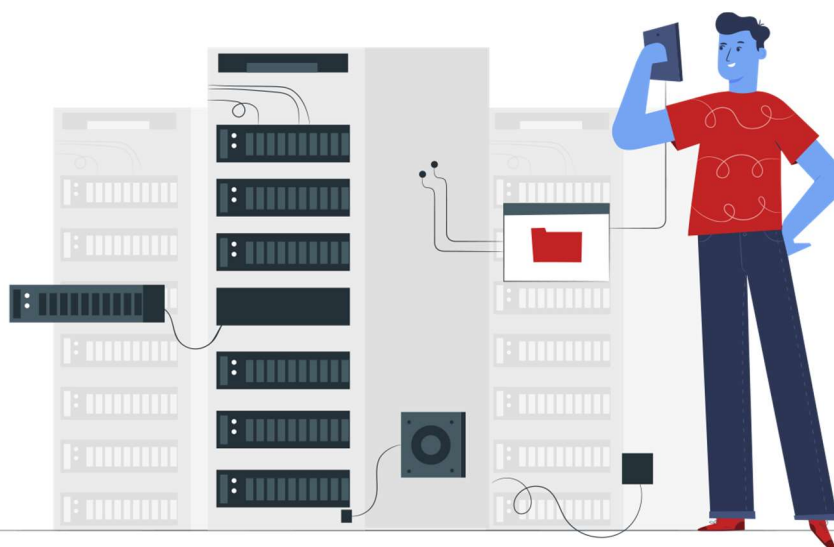
Une formation
Alphorm.com

OpenSSL

Cryptography and SSL/TLS tools

Cryptage des données

Démo



Une formation
Alphorm.com



Une formation
Alphorm.com

Conclusion



Mohamed Anass EDDIK



Une formation
Alphorm.com

Bilan

Introduction au OpenSSL
Crypter et décrypter avec OpenSSL
Gérer les certificats
Signer un message
Tester avec Openssl

