LP IOTIA

Module « Échanges sécurisés de données sur réseaux »

Travaux Dirigés

Il vous est demandé d'indiquer vos réponses dans un fichier Word.
Des impressions d'écrans peuvent être intégrées au document lorsque des lignes de commande sont demandées.
Ce fichier est à envoyer à la fin des Travaux Dirigés à l'adresse : lionel.clot@cstb.fr

A. Des exemples de chiffrement

A.1 Le décalage de césar

Décrypter ce texte sans connaître la clé utilisée pour décaler.
Indiquer le texte déchiffré dans le document à remettre.

GIXE MXPE TPIM RIPY RI

A.2 La table de Vigenère

Explications

Le chiffre de Vigenère est un système de chiffrement, élaboré par Blaise de Vigenère (1523-1596), diplomate français du XVIe siècle.

C'est un système de substitution poly-alphabétique. Cela signifie qu'il permet de remplacer une lettre par une autre qui n'est pas toujours la même, contrairement au chiffre de César qui se contente d'utiliser le même chiffre de substitution (mono-alphabétique).
Il s'agit donc un système beaucoup plus robuste.

Ce chiffrement introduit la notion de clé. Une clé se présente généralement sous la forme d'un mot ou d'une phrase. Pour pouvoir chiffrer un texte, à chaque caractère il faut utiliser une lettre de la clé pour effectuer la substitution. Plus la clé sera longue et variée et mieux le texte sera sécurisé.

L'outil indispensable du chiffrement de Vigenère est : « La table de Vigenère » :

		Lettre en clair																										
		A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	
Clé Utilisée	**A**	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	**Lettre Chiffrée**
	B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	
	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	
	D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	
	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	
	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	
	G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	
	H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	
	I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	
	J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	
	K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	
	L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	
	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	
	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	
	O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
	Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
	S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
	T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
	U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
	V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	
	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	
	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	
	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	

Pour chaque lettre en clair, on sélectionne la colonne correspondante et pour une lettre de la clé on sélectionne la ligne adéquate, puis au croisement de la ligne et de la colonne on trouve la lettre chiffrée. La lettre de la clé est à prendre dans l'ordre dans laquelle elle se présente et on répète la clé en boucle autant que nécessaire.

clé : MUSIQUE
texte : j'adore écouter la radio toute la journée
Texte en clair : JADOREECOUTERLARADIOTOUTELAJOURNEE
Clé répétée : MUSIQUEMUSIQUEMUSIQUEMUSIQUEMUSIQU

Par exemple :
Colonne O, ligne I: on obtient la lettre W.
Colonne D, ligne S: on obtient la lettre V.
Colonne A, ligne U: on obtient la lettre U.
Colonne J, ligne M: on obtient la lettre V.

Le texte chiffré est alors : VUVWHYIOIMBULPMLSLYIXAOLMBUNAOJVUY.

Si on veut déchiffrer ce texte, on regarde pour chaque lettre de la clé répétée la ligne correspondante, et on y cherche la lettre chiffrée. La première lettre de la colonne que l'on trouve ainsi est la lettre déchiffrée.

Texte chiffré	V	U	V	W	H	Y	I	O	I	M	B	U	L	P	M	L	…
Clé répétée	M	U	S	I	Q	U	E	M	U	S	I	Q	U	E	M	U	…

Par exemple :
Ligne I, on cherche W: on trouve la colonne O.
Ligne S, on cherche V: on trouve la colonne D.
Ligne U, on cherche U: on trouve la colonne A.
Ligne M, on cherche V: on trouve la colonne J.

Exercice

Déchiffrer le texte suivant :

BCGW VIRT NKIQ GGCG RXRT

Avec la clé : LICENCE

Et répondre à la question posée.

Indiquer le texte déchiffré et la réponse à la question dans le document à remettre.

B. L'outil OpenSSL

B.1 Présentation

OpenSSL est une suite logicielle gratuite de cryptographie essentiellement destinée aux développeurs. Elle est devenue la référence en la matière. De très nombreux produits de cryptographie gratuits ou commerciaux sont basés sur cette suite logicielle. OpenSSL fait partie de la plupart des distributions Linux. Il est également intégré dans PHP (depuis la version 5). OpenSSL se présente sous la forme d'un ensemble de bibliothèques de programmation en C et propose une commande en ligne sous DOS. C'est cette console que nous allons utiliser.
De nombreux sites Internet existent sur l'utilisation d'OpenSSL. Le principal étant http://www.openssl.org. Vous pouvez vous y référencer pour obtenir de l'aide sur les différentes commandes et options de la ligne de commande.

B.2 Installation d'OpenSSL

Pour installer OpenSSL, suivre les instructions suivantes :

1. Créer un répertoire « TD_OPENSSL ».
2. Créer un sous-répertoire « OpenSSL ».
3. Dans ce dernier répertoire, copier les trois fichiers récupérés sur : http://www.lpsil-eds.eu/OPENSSL/openssl.zip :
    a. openssl.exe (ligne de commande) ;
    b. libeay32.dll (bibliothèque) ;
    c. ssleay32.dll (bibliothèque).
4. Double-Cliquer sur « openssl.exe » pour lancer la ligne de commande (ouverture d'une fenêtre DOS).

B.3 Fonctionnement de la ligne de commande d'OpenSSL

OpenSSL dispose d'un ensemble de commandes correspondant à des fonctions cryptographiques. Pour visualiser l'ensemble des commandes, saisir la commande « help » ou « ? ». Les noms des commandes sont décrites dans la partie « Standards Commands ».

La plupart des commandes possèdent des options/paramètres (par exemple fichiers d'entrée, fichiers de sortie, algorithme à utiliser, etc…). Pour visualiser l'ensemble des options d'une commande, il suffit de saisir le nom d'une commande et un caractère quelconque. Par exemple, pour connaître la liste des options de la commande « ca », saisir « ca / ».

Pour visualiser un fichier généré par OPENSSL, il est conseillé d'utiliser Notepad++ car ceux-ci interprètent la mise en page des fichiers (pem) contrairement à notepad.

Les fichiers d'entrée ou de sortie des commandes OPENSSL doivent être dans le même répertoire que l'exécutable openssl.exe, sinon, il est nécessaire d'indiquer le chemin complet des fichiers.

C. Chiffrement/Déchiffrement symétrique

La commande « **enc** » permet de chiffrer et de déchiffrer symétriquement un document. Les principales options de cette commande sont :

-algo : spécification de l'algorithme à utiliser pour le chiffrement (par exemple –des : chiffrement avec l'algorithme DES)

-in *nomfichier* : fichier à chiffrer (ou à déchiffrer)

-out *nomfichier* : fichier chiffré (ou déchiffré)

-e : chiffre (valeur par défaut)

-d : déchiffre

-k : mot de passe : génère une clé à partir d'un mot de passe

-kfile *nomfichier* : fichier contenant un mot de passe

-p : affiche la clé sous forme hexadécimale

Exercice n° C.1

1. Copier un fichier vous appartenant (un fichier Word ou PDF par exemple) dans le répertoire OpenSSL.
2. Chiffrer ce fichier avec l'algorithme DES en utilisant un mot de passe que vous définissez. *Indiquer la commande OpenSSL dans le document à remettre.*
3. Les tailles du fichier non chiffré et du fichier chiffré sont-elles identiques ? Pourquoi ?
4. Ouvrir le fichier chiffré.

Exercice n° C.2

1. Renommer le fichier d'origine vous appartenant.
2. Déchiffrer le fichier chiffré avec le même mot de passe. *Indiquer la commande OpenSSL dans le document à remettre.*
3. Ouvrir le fichier déchiffré.
4. Essayer de déchiffrer le fichier chiffré avec un mot de passe différent.

Exercice n° C.3

1. Chiffrer de nouveau votre fichier avec un mot de passe, mais en affichant cette fois-ci la clé sous forme hexadécimale. *Indiquer la commande OpenSSL dans le document à remettre.*

Exercice n° C.4

1. Récupérer les fichiers exo4.txt et MotPasseC.bin à partir de l'adresse : http://www.lpsil-eds.eu/TD/EXO_C4.zip
2. Le fichier exo_C4.txt a été chiffré symétriquement avec l'algorithme Blowfish (option : - bf). La clé a été obtenue par mot de passe.
3. Le mode de passe chiffré symétriquement avec l'algorithme base 64 (option : -base64) est contenu dans le fichier MotPasseC.bin. À l'aide la commande appropriée, déchiffrer le mot de passe.
4. Déchiffrer ensuite le fichier exo_C4.txt.
   Indiquer toutes les commandes OpenSSL dans le document à remettre.

D. Génération de clés asymétriques

IMPORTANT : Gardez les clés générées dans les exercices D, celles-ci seront utilisées dans les exercices suivants !

Exercice n° D.1
La commande « **genrsa** » permet de générer une clé privée. Les options principales sont :

-out *nomfichier* : fichier de sortie qui contiendra la clé privée
nombrebits : longueur de la clé

1. Générer une clé privée en 512 bits. *Indiquer la commande OpenSSL dans le document.*
2. Ouvrir le fichier contenant cette clé privée : le fichier obtenu est un fichier au format PEM codé en base64.
3. Générer une clé privée en 1 024 bits, 2 048 bits, 4 096 bits.

Exercice n° D.2
Pour des raisons évidentes de sécurité, il est déconseillé de laisser une clé privée en clair.
La commande « genrsa » propose, lors de la création d'une paire de clés, de chiffrer le fichier de sortie de façon symétrique (par exemple suivant l'algorithme DES avec l'option **-des**). Pour cela, il faut indiquer le nom de l'algorithme en option de la commande genrsa. Un mot de passe permettant à OpenSSL de générer la clé de chiffrement symétrique sera demandé.

1. Générer votre clé privée en 1024 bits en la protégeant par un mot de passe. Le fichier de sortie contenant la clé privée devra contenir votre nom (ou à défaut devra s'appeler maClePrivee.txt). *Indiquer la commande OpenSSL dans le document à remettre.*
2. Ouvrir le fichier contenant votre clé privée.

Exercice n° D.3
La commande « **rsa** » permet de gérer les clés (privées ou publiques) RSA. Les options principales sont :

-in nomFichier : fichier d'entrée
-out nomFichier : fichier de sortie
-pubin : spécifie que le fichier d'entrée est une clé publique
-pubout : spécifie que le fichier de sortie sera une clé publique

Important :
Si l'option –pubin n'est pas spécifiée, le fichier d'entrée doit être une clé privée.
Si l'option –pubout n'est pas spécifiée, le fichier de sortie sera une clé privée.

1. A partir de votre clé privée générée dans l'exercice D.2, générer votre clé publique. Le fichier de sortie contenant la clé publique devra contenir votre nom (ou à défaut devra s'appeler maClePublique.txt). *Indiquer la commande OpenSSL dans le document à remettre.*

Exercice n° D.4
Faut-il conserver la clé publique en clair ou faut-il la chiffrer ? *Indiquer votre réponse et la justification dans le document à remettre.*

E. Chiffrement/Déchiffrement asymétrique

Exercice n° E.1
La commande « **rsautl** » permet de chiffrer et déchiffrer asymétriquement. Les principales options de cette commande sont :

-in *nomfichier* : fichier à chiffrer (ou à déchiffrer)
-out *nomfichier* : fichier à chiffré (ou déchiffré)
-inkey *nomfichier* : (une clé)
-pubin : le fichier spécifiée après l'option -inkey est une clé publique
-encrypt : permet de chiffrer
-decrypt : permet de déchiffrer
Important :
Si l'option –pubin n'est pas spécifiée, la clé spécifiée après l'option –inkey doit être une clé privée.

1. Chiffrer asymétriquement un de vos documents (de taille moyenne ou importante) avec votre clé publique. *Indiquer la commande OpenSSL dans le document à remettre.*
2. Chiffrer asymétriquement un document de petite taille avec votre clé publique.
3. Déchiffrer le document chiffré avec votre clé privée. *Indiquer la commande OpenSSL dans le document à remettre.*
4. Déchiffrer le document avec votre clé publique. *Indiquer la commande OpenSSL dans le document à remettre.*
5. Déchiffrer le document avec une autre clé privée que vous aurez préalablement générée rapidement avec la commande genrsa (genrsa –out test.txt 1024).

F. Chiffrement hybride

Exercice n° F.1
Récupérer à partir de l'adresse suivante http://www.lpsil-eds.eu/TD/EXO_F1.zip les quatre fichiers suivants :

- Exo_F1.txt
- Cle.txt
- MotdePasse.rsa
- MotdePasse.base64

Le but de l'exercice est de déchiffrer le fichier exo_F1.txt en sachant que :

1. Le fichier exo_F1.txt a été obtenu en chiffrant symétriquement un texte avec la commande « enc ». L'algorithme de chiffrement symétrique utilisé est BlowFish en mode CBC (option –bf-cbc).
2. La clé secrète utilisée pour chiffrer symétriquement le fichier a été dérivée à partir d'un mot de passe. La version chiffrée asymétriquement de ce mot de passe est contenue dans le fichier MotdePasse.rsa.
3. Le fichier Cle.txt contient la clé privée RSA qui sert à déchiffrer asymétriquement le mot de passe.
4. Le fichier MotdePasse.base64 contient le mot de passe protégeant la clé privée RSA. Ce fichier est codé en base 64.

Indiquer toutes les commandes OpenSSL dans le document à remettre.

G. Hachage

Exercice n° G.1
La commande « **dgst** » permet de calculer le hash d'un document.
La syntaxe est :

dgst -*hachage* -out *empreinte fichier_entree*

hachage est une fonction de hachage parmi :

- MD5 (option md5), qui calcule des empreintes de 128 bits,
- SHA1 (option sha1), qui calcule des empreintes de 160 bits,
- SHA256 (option sha256), qui calcule des empreintes de 256 bits.

1. Calculer le hash d'un de vos documents avec l'algorithme SHA256. *Indiquer la commande OpenSSL dans le document à remettre.*
2. Ouvrer le hash et vérifier sa taille.
3. Modifier votre document d'origine et recalculer le hash.
4. Comparer visuellement les deux hash.
5. Calculer le hash du premier fichier l'algorithme MD5 et comparer le avec le SHA256.

H. Signature électronique

Rappel : signer un document signifie chiffrer le hash du document avec une clé privée.

Exercice n° H.1
La commande « dgst » permet de signer directement un document.
La syntaxe est :

dgst -out *signature* -sign cleprivee *fichier_entree*

Les options sont les suivantes :
-out *nomfichier* : résultat de la signature (hash chiffré avec une clé privée)
-sign *cleprivee* : calcul le hash et le signe avec la clé privée contenue dans cleprivee
fichier_entree : le fichier à signer

1. Signer un document avec votre clé privée. *Indiquer la commande OpenSSL dans le document à remettre.*

Exercice n° H.2
La commande « dgst » permet de vérifier la signature d'un document. Les options sont les suivantes :
La syntaxe est : **dgst -verify *clePublique* -signature *signature fichier_entree***
-verify *clePublique* : clePublique permettant de vérifier une signature
-signature : *signature* (hash chiffré avec une clé privée) à vérifier
fichier_entree: le document d'origine

1. Vérifier le document signé précédemment. *Indiquer la commande OpenSSL dans le document à remettre.*
2. Modifier le hash signé. Vérifier de nouveau le document signé.

Exercice n° H.3

La commande « rsautl » permet de signer directement un hash avec une clé privée (en utilisant l'option (-sign). Elle permet également de vérifier directement un hash signé (option – verify). Dans ce cas, l'option –in doit être suivie de la signature à vérifier et l'option –inkey de la clé publique permettant de vérifier la signature (ne pas oublier l'option –pubin).

1. Récupérer les trois fichiers contenus dans l'archive à l'adresse : http://www.lpsil-eds.eu/TD/EXO_H3.zip
2. Lequel des deux fichiers signature1.txt et signature2.txt a bien été signé par le possesseur de la clé privée correspondante à la clé publique contenue dans le fichier ClePubEXO_H3.txt ? *Indiquer les commandes OpenSSL dans le document à remettre et le résultat.*

I. Certificat électronique

Exercice n° I.1 : création d'une requête de demande de certificat.

La commande « **req** » permet de créer une demande de certificat. Ces principales options sont :

-new : cette option génère une nouvelle demande de certificats. Il sera demandé à l'utilisateur de fournir les valeurs de champs nécessaires. Ces champs ainsi que les valeurs maximales et minimales sont spécifiées dans le fichier de configuration.

-config *fichierconfiguration* : fichier de configuration contenant les valeurs par défaut et les valeurs maximales et minimales des données de la requête.

-out *nomfichier* : fichier qui contiendra la requête.

-key *nomfichier* : clé privée du demandeur de la requête.

1. Récupérer le fichier de configuration config.txt à l'adresse http://www.lpsil-eds.eu/TD/EXO_I1.zip.
2. Ouvrir le fichier de configuration pour le visualiser.
3. Générer votre requête pour votre certificat. *Indiquer la commande OpenSSL dans le document à remettre.*
4. Ouvrir avec Notepad++ le fichier de requête généré.

Exercice n° I.2 : une autorité de certification

Une fois que vous avez établi une requête de certificat, vous devez contacter une autorité de certification qui vous délivrera un certificat signé (après avoir procédé à des vérifications vous concernant).

Vous allez jouer le rôle d'une autorité de certification. Pour cela, vous devez avoir un certificat d'une autorité de certificat ainsi que sa clé privée (paire de clés).

1. Récupérer les fichiers CertificatUNSA.cer et ClePriveeUNSA.txt à l'adresse http://www.lpsil-eds.eu/TD/EXO_I2.zip.
2. Double-cliquer sur le fichier CertificatUNSA.cer.
3. Cherchez quelle est la date d'expiration du certificat et la taille de la clé publique. *Indiquer les réponses dans le document à remettre.*

Exercice n° I.3 : création et signature du certificat par l'autorité de certification
La commande « x509 » permet de créer un certificat et de le signer par une autorité de certification.

Les principales options de la commande sont :
-days : durée de validité en nombre de jours du certificat
-CA *certificat* : certificat de l'autorité de certificat
-CAkey *cleprivee* : clé privée de l'autorité de certification
-in *fichier* : la requête
-out *fichier* : fichier qui contiendra le certificat
-CAserial *fichier* : fichier contenant le numéro de série du prochain certificat à signer. Ce fichier est un fichier texte (à créer) contenant une ligne avec un nombre hexadécimal sur deux digits (par exemple : 01, 0F,…)
-req : spécifie que l'argument de l'option –in est une requête.

1. Créer votre certificat et signer le par l'autorité de certification. *Indiquer la commande OpenSSL dans le document à remettre.*

Exercice n° I.4 : vérification de la validité d'un certificat.
La commande « **verify** » permet de vérifier la validité d'un certificat. La syntaxe est la suivante :
verify –CAfile *CertificatAutorité MonCertificat*

1. Vérifier le certificat généré dans l'exercice précédent. *Indiquer la commande OpenSSL dans le document à remettre.*

Exercice n° I.5 : utilisation du magasin de certificats d'un navigateur Internet
1. Citer deux autorités de confiance installées par défaut dans votre magasin de certificats de votre navigateur Internet. *Indiquer votre réponse dans le document à remettre.*
2. Installer votre certificat dans le magasin de certificats d'Internet Explorer.
3. Visualiser le certificat dans le magasin.
4. Installer le certificat de l'Autorité de Certificat dans le magasin de certificats.
5. Visualiser de nouveau votre certificat dans le magasin.

Exercice n° I.6 : création du certificat avec la clé privée.
La commande « pkcs12 » permet de créer un certificat contenant la clé privée (et bien sûr la clé publique). Les principales options sont :
-export : option obligatoire
-inkey *clé* : clé privée
-in *certificat* : le certificat contenant déjà la clé publique
-out *fichier>* : fichier qui contiendra le certificat avec la clé privée (donner à ce fichier l'extension .p12).

1. Générer votre certificat incluant votre clé privée. Le fichier contenant le certificat doit avoir pour extension .p12. *Indiquer la commande OpenSSL dans le document à remettre.*
2. Installer ce certificat dans le magasin d'Internet Explorer. Visualiser le certificat dans le magasin pour vérifier que ce certificat contient bien votre clé privée.

J. Chaîne de certification

Exercice n° J.1 : génération de certificats racine.

L'objet de l'exercice est de créer une chaîne de certification contenant :

- une racine principale nommée « IUT » ;
- sous cette racine, une racine représentant les professeurs, et une racine représentant les étudiants (nommées « Professeurs » et « Étudiants ») ;
- sous la racine représentant les étudiants, votre propre certificat incluant votre clé privée.

Important - Cas particulier : le certificat de la racine principale (IUT), ne peut être signé que par lui-même. On parle d'un certificat autosigné. Pour créer un certificat autosigné, vous devez utiliser uniquement la commande req avec l'option –x509. Cette option spécifie à OpenSSL de créer directement un certificat autosigné et non une requête. Il est alors inutile d'utiliser la commande x509.

Pour chaque racine, vous devez :

1. Créer une clé privée spécifique (commande « genrsa » utilisée avec l'option –des pour chiffrer la clé).
2. A partir de cette clé privée, générer une requête (commande req). Pour générer les requêtes, récupérer le fichier de configuration à l'adresse : http://www.lpsil-eds.eu/TD/EXO_J1.zip
3. A partir de cette requête, créer le certificat signé par l'autorité de certification supérieure (commande x509).

Indiquer toutes les commandes OpenSSL dans le document à remettre.

Les clés privées des racines doivent être de longueur 1024.
Pour toutes les racines, les durées de validités des certificats doivent être de 5 ans.

Exercice n° J.2
Installer l'ensemble des certificats créés dans l'exercice J.1 dans votre magasin de certificats puis visualiser l'arborescence complète.

K. Bonus

Exercice n° K.1
Vous venez de perdre votre clé privée mais vous avez encore la clé publique correspondante.

1. Pouvez-vous encore envoyer des documents confidentiels ?
2. Pouvez-vous encore lire des documents confidentiels ?
3. Pouvez-vous encore signer les documents que vous envoyez ?
4. Pouvez-vous encore vérifier les documents signés que vous recevez ?

Indiquer les réponses et les justifications dans le document à remettre.

Exercice n° K.2
Vous venez de perdre votre clé publique mais vous avez encore la clé privée correspondante.

1. Pouvez-vous encore envoyer des documents confidentiels chiffrés ?
2. Pouvez-vous encore lire des documents confidentiels que vous recevez ?
3. Pouvez-vous encore signer les documents que vous envoyez ?
4. Pouvez-vous encore vérifier les documents signés que vous recevez ?

Indiquer les réponses et les justifications dans le document à remettre.