

**Classe :
terminale**

LYCÉE INTERNATIONAL COURS LUMIÈRE

séquence 3

Sécurisation des communications

Mr BANANKO K.

Objectifs :

Contenus	Capacités attendues	Commentaires
Sécurisation des communications.	Décrire les principes de chiffrement symétrique (clef partagée) et asymétrique (avec clef privée/clef publique). Décrire l'échange d'une clef symétrique en utilisant un protocole asymétrique pour sécuriser une communication HTTPS.	Les protocoles symétriques et asymétriques peuvent être illustrés en mode débranché, éventuellement avec description d'un chiffrement particulier. La négociation de la méthode chiffrement du protocole SSL (Secure Sockets Layer) n'est pas abordée.

Référence Manuels hachette Education : Page 196

Attention vocabulaire

- **Chiffrer** : il s'agit de rendre un document illisible avec une clef de chiffrement
- **Déchiffrer** : il s'agit de rendre lisible un document chiffré, en ayant connaissance de la clef de chiffrement
- **Crypter** : cela n'existe pas ; C'est un néologisme dérivé de "cryptographie" et est parfois employé pour exprimer l'action de rendre un document illisible
- **Décrypter** : il s'agit de rendre lisible un document chiffré, sans avoir connaissance de la clef de chiffrement
- **Cryptologie** : il s'agit de la science du secret

I- NOTION DE CHIFFREMENT

Soit 2 individus A et B qui cherchent à s'envoyer des messages par l'intermédiaire d'un réseau informatique. A et B désirent qu'une tierce personne (par exemple P) ne soit pas capable de lire les messages si par hasard ces derniers devaient être interceptés par P. Pour ce faire, A va chiffrer le message. Toute personne qui ne possédera pas le moyen de déchiffrer ce message chiffré se verra dans l'impossibilité de comprendre le contenu du message (si P intercepte le message chiffré et qu'il ne possède pas le moyen de déchiffrer ce message, l'interception aura été totalement inutile puisque P sera dans l'incapacité de comprendre le contenu du message). Il existe 2 grands types de chiffrement : **le chiffrement symétrique et le chiffrement asymétrique** que nous verrons après avoir donné quelques chiffrements de base

a- Le chiffrement de César

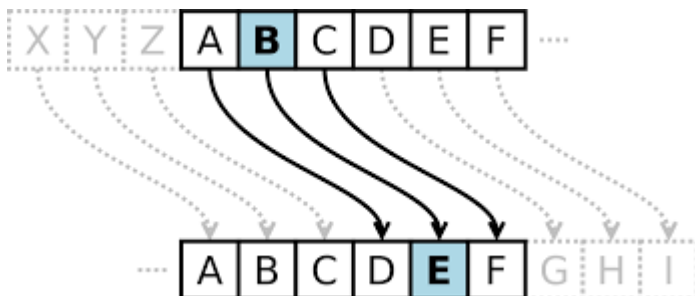
Le chiffrement César est basé sur un décalage de l'alphabet. Cependant pour chaque message les mots on le même déplacement.

Nous allons chiffrer HELLO WORD avec un décallage de 3

Lettre	Lettre décallée
A	D
B	E
C	F
...	...
X	A
Y	B
Z	C

HELLO WORD ce transforme en **KHOOR ZRUOG**

b- Chiffrement de Vigenère



Le chiffrement de Vigenère est une technique de chiffrement par substitution polyalphabétique, ce qui signifie qu'il utilise plusieurs alphabets pour chiffrer le texte. Il a été inventé par le cryptographe français Blaise de Vigenère au XVI^e(1501) siècle.

Voici comment fonctionne le chiffrement de Vigenère avec un exemple :

Supposons que nous voulons chiffrer le message "**SECURITE**" avec la clé "**CRYPTO**". La première étape est de répéter la clé suffisamment de fois pour qu'elle soit de la même longueur que le message à chiffrer :

- **Message: SECURITE**
- **Clé : CRYPTO**

Étape 1 : Répéter la clé La première étape consiste à répéter la clé suffisamment de fois pour qu'elle ait la même longueur que le message à chiffrer.

Message: S E C U R I T E Clé répétée: C R Y P T O C R Y

Étape 2 : Convertir les lettres en nombres Attribuer une valeur numérique à chaque lettre en utilisant l'alphabet standard, par exemple, en commençant par **A=0, B=1, ..., Z=25**.

Message: 18 4 2 20 17 8 19 4 Clé répétée: 2 17 24 15 19 14 2 17 24

Étape 3 : Additionner les valeurs correspondantes modulo 26 Additionner les valeurs correspondantes du message et de la clé, lettre par lettre, en utilisant l'arithmétique modulo 26.

Message chiffré: $(18+2)\%26$ $(4+17)\%26$ $(2+24)\%26$ $(20+15)\%26$ $(17+19)\%26$ $(8+14)\%26$ $(19+2)\%26$ $(4+17)\%26$ 20 21 0 9 10 22 21 21

Les résultats sont convertis de nouveau en lettres en utilisant l'alphabet standard (**A=0, B=1, ..., Z=25**).

Message chiffré: U V A J K W V V

Ainsi, le message "**SECURITE**" chiffré avec la clé "**CRYPTO**" donne "**UVAJKWVV**".

C'est ce texte chiffré que l'on enverrait si l'on utilisait le chiffrement de Vigenère avec cette clé spécifique. Pour déchiffrer, on utiliserait le processus inverse en soustrayant les valeurs de la clé au lieu de les additionner.

II- LE CHIFFREMENT SYMETRIQUE

Un **chiffrement symétrique** est un chiffrement où la clé de chiffrement est la même pour chiffrer et déchiffrer le message. Cette clé unique doit être connue de l'émetteur et du récepteur du message.



Pour chiffrer un message, A va utiliser une suite de caractères que l'on appelle "**clé de chiffrement**". Dans le cas du chiffrement symétrique, cette clé de chiffrement sera aussi utilisée par B pour déchiffrer le message envoyé par A. Dans ce cas, la clé de chiffrement est identique à la clé de déchiffrement.

Concrètement comment cela se passe-t-il ?

Avant d'entrer dans le vif du sujet, il faut savoir que l'idée de chiffrer des messages (de les rendre illisibles pour des personnes non autorisées) ne date pas du début de l'ère de l'informatique. En effet,

dès l'antiquité, on cherchait déjà à sécuriser les communications en chiffrant les messages sensibles (pour en savoir plus sur l'histoire du chiffrement, n'hésitez pas à consulter la page [Wikipédia](#) consacrée à ce sujet). Nous nous intéresserons ici uniquement aux communications ayant lieu par l'intermédiaire d'un réseau informatique. Comme nous avons déjà eu l'occasion de le voir en première, toute "donnée informatique" peut être vue comme une suite de zéro et de un. Nous chercherons donc à chiffrer une suite de zéro et de un :

Soit le message "**Hello World!**" ce qui nous donnera en binaire :

```
01001000011001010110110001101100011011110010000001010110110111101110010011011000
110010000100001
```

N.B. nous avons simplement utilisé le code ASCII de chaque caractère (par exemple, on peut vérifier que le H correspond bien à l'octet 01001000). Pour effectuer la "conversion" texte vers code binaire ASCII ou vis versa, vous pouvez utiliser le site <https://www.rapidtables.com/convert/number/ascii-to-binary.html>

Choisissons maintenant un mot (ou une phrase) qui nous servira de clé de chiffrement, prenons pour exemple le mot "**toto**". "**toto**" nous donne en binaire :

```
01110100011011110111010001101111
```

Pour chiffrer le message nous allons effectuer un **XOR** bit à bit. Pour rappel, vous trouverez la table de vérité du **XOR** ci-dessous :

Table de vérité "**XOR**" :

E1	E2	S
0	0	0
0	1	1
1	0	1
1	1	0

Comme la clé est plus courte que le message, il faut "**reproduire**" la clé vers la droite autant de fois que nécessaire (*si la taille du message n'est pas un multiple de la taille de la clé, on peut reproduire seulement quelques bits de la clé pour la fin du message*):

⊕ 01001000011001010110110001101100 01101111001000000101011101101111 01110010011011000110010000100001
 01110100011011110111010001101111 01110100011011110111010001101111 01110100011011110111010001101111
 00111100000010100001100000000011 00011011010011110010001100000000 00000110000000110001000001001110

Le signe + dans un cercle symbolise le **XOR**

Après ce XOR on obtient donc la suite de bits suivante :

```
00111100000010100001100000000011000110110100111100100011000000000000110000000110
001000001001110
```

Soit la chaîne de caractères suivante (*si on cherche à afficher le message chiffré avec un éditeur de texte*) :

```
???O# ???N
```

Maintenant ce message est prêt pour être envoyé à son destinataire B. Si P intercepte le message et cherche à le lire avec un éditeur de texte, il obtiendra la suite de caractère

```
???O# ???N
```

B a maintenant reçu le message chiffré, il possède la clé (**toto**), il va donc pouvoir déchiffrer le message en appliquant un **XOR** entre le message chiffré et la clé (*on applique exactement la même méthode que ci-dessus*).

⊕ 00111100000010100001100000000011 00011011010011110010001100000000 00000110000000110001000001001110
 01110100011011110111010001101111 01110100011011110111010001101111 01110100011011110111010001101111
 01001000011001010110110001101100 01101111001000000101011101101111 01110010011011000110010000100001

On trouve le code binaire suivant :

```
010010000110010101101100011011000110111100100000010101110110111101110010011011000
110010000100001
```

Vous pouvez remarquer que nous avons bien retrouvé le code binaire d'origine. Si vous ne voulez pas vous embêter à vérifier bit par bit, vous pouvez utiliser ce [site](#) qui vous permettra de repasser du code binaire **ASCII** au texte.

On retrouve bien le message d'origine : **Hello World!**, B a pu lire le message envoyé par A alors que pour P, malgré le fait qu'il a pu intercepter le message, il n'a pas pu prendre connaissance de son contenu sans la clé.

Activité 1

Soit 3 personnes A, B et P. A désire envoyer un message chiffré (chiffrement symétrique) à B. P est un pirate qui va essayer de déchiffrer un message qui ne lui est pas destiné.

Vous allez jouer le rôle de A.

Choisissez une ou un camarade dans la classe qui jouera le rôle de B.

Mettez-vous d'accord avec B sur une clé de **chiffrement/déchiffrement** (*choisissez un mot qui jouera le rôle de clé, ce mot doit rester secret*).

Choisissez un message à faire parvenir à B puis procédez au chiffrement de ce message, notez le résultat du chiffrement (*en binaire*) sur une feuille.

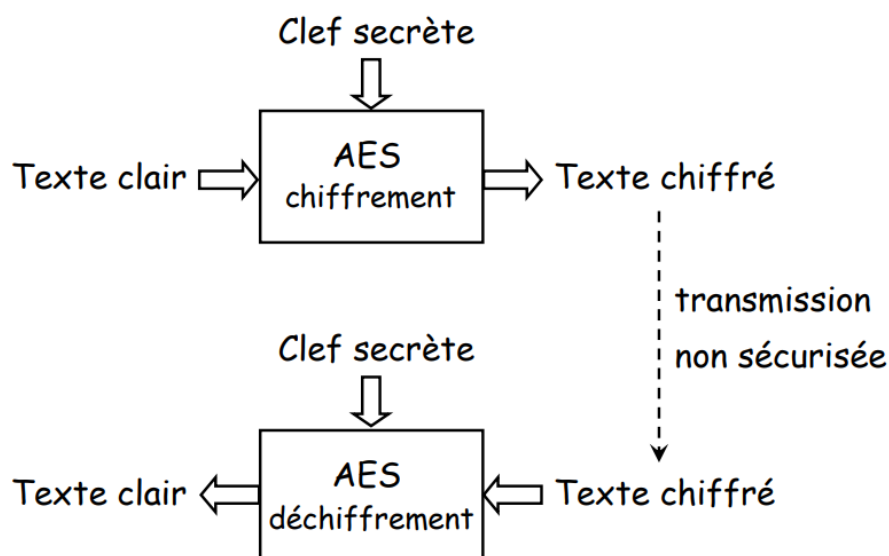
Donnez cette feuille à une ou un camarade tiers (*qui ne connaît pas la clé, ce camarade jouera donc le rôle de P*). P devra recopier le message avant de le transmettre à B. P devra essayer de trouver le message envoyé par A à B.

B devra déchiffrer le message à l'aide de la clé. Vous pourrez utiliser les sites cités plus haut afin d'assurer le passage **texte -> code ASCII binaire et code ASCII binaire-> texte**.

- <https://www.rapidtables.com/convert/number/ascii-to-binary.html>
- <https://www.rapidtables.com/convert/number/binary-to-ascii.html>

La méthode la plus utilisée en matière de chiffrement symétrique se nomme **AES (Advanced Encryption Standard)**. Cette méthode utilise une technique de chiffrement plus élaborée que ce qui a été vu ci-dessus, mais les grands principes restent identiques.

Le **chiffrement AES (Advanced Encryption Standard)** est un algorithme de chiffrement/déchiffrement symétrique. Il permet la transmission d'un message confidentiel par une liaison non sécurisée.



Une même clef secrète est utilisée pour les opérations de chiffrement et de déchiffrement (c'est un secret partagé entre l'expéditeur et le destinataire du message).

Le gros problème avec le chiffrement symétrique, c'est qu'il est nécessaire pour A et B de se mettre d'accord à l'avance sur la clé qui sera utilisée lors des échanges. Le chiffrement asymétrique permet d'éviter ce problème.

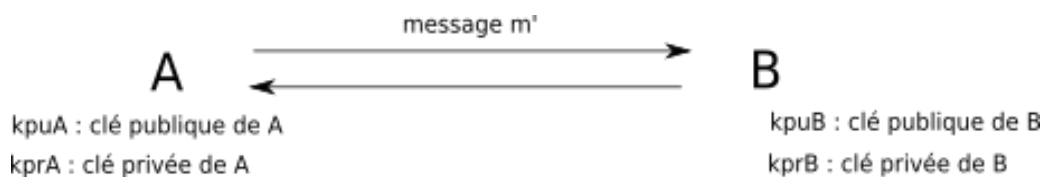
Activité

Résumez en quelques lignes le principe du chiffrement symétrique

III- Le chiffrement asymétrique

Dans le cas du chiffrement asymétrique A et B n'ont pas besoin de partager une "**clé secrète**" :

- A possède une "**clé privée**" que l'on notera k_{prA} et une "**clé publique**" que l'on notera k_{puA} . En aucun cas A ne devra divulguer sa clé privée à quiconque, elle devra rester strictement secrète. En revanche sa clé publique pourra être connue de tout le monde sans aucun problème.
- B possède une "**clé privée**" que l'on notera k_{prB} et une "**clé publique**" que l'on notera k_{puB} . En aucun cas B ne devra divulguer sa clé privée à quiconque, elle devra rester strictement secrète. En revanche sa clé publique pourra être connue de tout le monde sans aucun problème.



Si A désire envoyer un message m à B, il va utiliser **la clé publique** de B afin de réaliser le chiffrement (**m est chiffré en m'**).

Le message chiffré (m') va ensuite pouvoir transiter entre A et B. Une fois le message m' en sa possession, B va utiliser sa clé privée afin de pouvoir déchiffrer le message m' et ainsi obtenir le message m .

Le processus peut être résumé par le schéma suivant :

$$1) k_{puB}(m) \longrightarrow m'$$

$$2) A \xrightarrow[\text{réseau}]{m'} B$$

$$3) k_{prB}(m') \longrightarrow m$$

Si P intercepte le message m' , il sera incapable de déterminer m à partir de m' sans la clé privée de B.

Le chiffrement asymétrique repose sur des problèmes très difficiles à résoudre dans un sens et faciles à résoudre dans l'autre sens.

Prenons un exemple : l'algorithme de chiffrement asymétrique RSA (**du nom de ses 3 inventeurs : Rivest Shamir et Adleman**), est très couramment utilisé, notamment dans tout ce qui touche au commerce électronique.

RSA se base sur la factorisation des très grands nombres premiers.

Si vous prenez un nombre premier A (par exemple **A = 16813007**) et un nombre premier B (par exemple **B = 258027589**), il est facile de déterminer C le produit de A par B (ici on a **A x B = C** avec **C = 4338219660050123**).

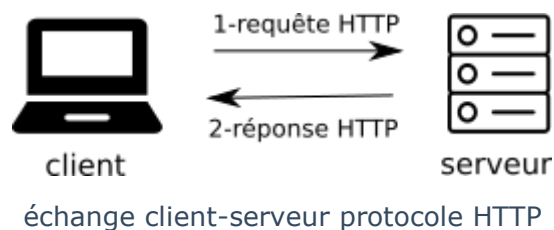
En revanche si je vous donne C (ici **4338219660050123**) il est très difficile de retrouver A et B. En tous les cas, à ce jour, aucun algorithme n'est capable de retrouver A et B connaissant C dans un temps "**raisonnable**".

Nous avons donc bien ici un problème relativement facile dans un sens (**trouver C à partir de A et B**) est extrêmement difficile dans l'autre sens (**trouver A et B à partir de C**). Les détails du fonctionnement de RSA sont relativement complexes (mathématiquement parlant) et ne seront pas abordés ici. Vous devez juste savoir qu'il existe un lien entre une clé publique et la clé privée correspondante, mais qu'il est quasiment impossible de trouver la clé privée de quelqu'un à partir de sa clé publique.

IV- LE PROTOCOLE HTTPS

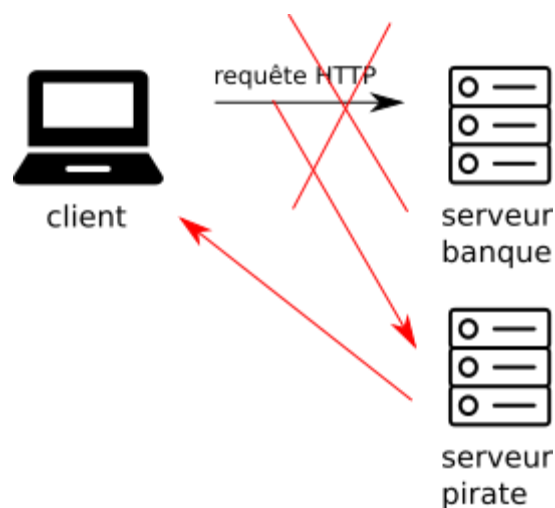
Nous allons maintenant voir une utilisation concrète de ces chiffrements symétriques et asymétriques : **le protocole HTTPS (Hypertext Transfer Protocol Secure)**.

Avant de parler du protocole HTTPS, petit retour sur le protocole HTTP : un client effectue une requête HTTP vers un serveur, le serveur va alors répondre à cette requête (*par exemple en envoyant une page HTML au client*). Si nécessaire n'hésitez pas à consulter ce qui a été fait en première pour plus de détails.



Le protocole HTTP pose 2 problèmes en termes de sécurité informatique :

- Un individu qui intercepterait les données transitant entre le client et le serveur pourrait les lire sans aucun problème (*ce qui serait problématique notamment avec un site de e-commerce au moment où le client envoie des données bancaires*)
- grâce à une technique qui ne sera pas détaillée ici (le [DNS¹ spoofing](#)), un serveur "**pirate**" peut se faire passer pour un site sur lequel vous avez l'habitude de vous rendre en toute confiance : imaginez-vous voulez consulter vos comptes bancaires en ligne, vous saisissez l'adresse web de votre banque dans la barre d'adresse de votre navigateur favori, vous arrivez sur la page d'accueil d'un site en tout point identique au site de votre banque, en toute confiance, vous saisissez votre identifiant et votre mot de passe. C'est terminé un "**pirate**" va pouvoir récupérer votre identifiant et votre mot de passe ! **Pourquoi ?** Vous avez saisi l'adresse web de votre banque comme d'habitude ! Oui, sauf que grâce à une attaque de type "**DNS spoofing**" vous avez été redirigé vers un site pirate, en tout point identique au site de votre banque. Dès vos identifiant et mot de passe saisis sur ce faux site, le pirate pourra les récupérer et se rendre avec sur le véritable site de votre banque. À noter qu'il existe d'autres techniques que le DNS spoofing qui permettent de substituer un serveur à un autre, mais elles ne seront pas évoquées ici.



Attaque DNS Spoofing

HTTPS est donc la version sécurisée de HTTP, le but de HTTPS est d'éviter les 2 problèmes évoqués ci-dessus. HTTPS s'appuie sur le protocole TLS (**Transport Layer Security**) anciennement connu sous le nom de SSL (**Secure Sockets Layer**)

Comment chiffrer les données circulant entre le client et le serveur ?

Les communications vont être chiffrées grâce à une clé symétrique.

Problème : **comment échanger cette clé entre le client et le serveur ?**

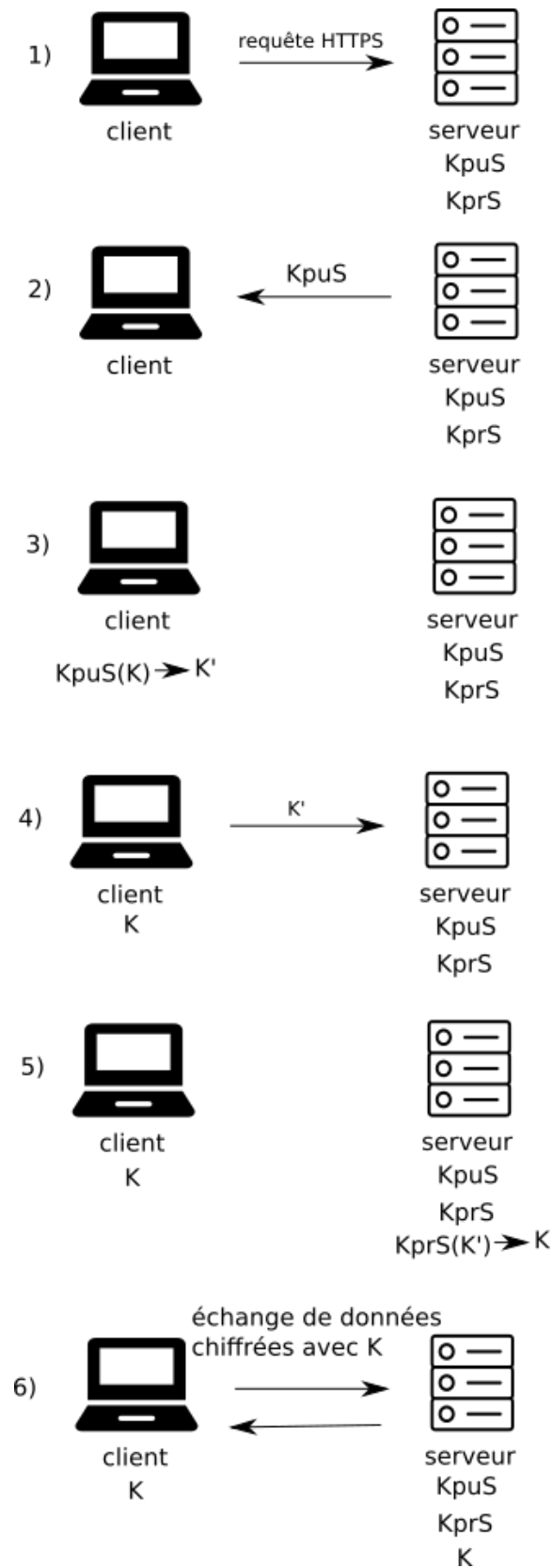
¹¹ Le **Domain Name System** (Service de nom de domaine) ou **DNS** est un service informatique distribué qui associe les noms de domaine Internet avec leurs adresses

Simplement en utilisant une paire **clé publique / clé privée** !

Voici le déroulement des opérations :

- le client effectue une requête HTTPS vers le serveur, en retour le serveur envoie sa clé publique (KpuS) au client
- le client "**fabrique**" une clé K (***qui sera utilisé pour chiffrer les futurs échanges***), chiffre cette clé K avec KpuS et envoie la version chiffrée de la clé K au serveur
- le serveur reçoit la version chiffrée de la clé K et la déchiffre en utilisant sa clé privée (KprS). À partir de ce moment-là, le client et le serveur sont en possession de la clé K
- le client et le serveur commencent à échanger des données en les chiffrant et en les déchiffrant à l'aide de la clé K (***chiffrement symétrique***).

On peut résumer ce processus avec le schéma suivant :



principe protocole TLS

Ce processus se répète à chaque fois qu'un nouveau client effectue une requête HTTPS vers le serveur.

Comment éviter les conséquences fâcheuses d'une attaque de type DNS Spoofing ?

Pour éviter tout problème, il faut que le serveur puisse justifier de son "**identité**" ("voici la preuve que je suis bien le site de la banque B et pas un site **"pirate"**"). Pour ce faire, chaque site désirant proposer des transactions HTTPS doit, périodiquement, demander (acheter dans la plupart des cas) un certificat d'authentification (sorte de carte d'identité pour un site internet) auprès d'une autorité habilitée à fournir ce genre de certificats (chaque navigateur web possède une liste des autorités dont il accepte les certificats). Comme dit plus haut, ce certificat permet au site de prouver son "**identité**" auprès des clients. Nous n'allons pas entrer dans les détails du fonctionnement de ces certificats, mais vous devez juste savoir que le serveur envoie ce certificat au client en même temps que sa clé publique (étape 2 du schéma ci-dessus). En cas d'absence de certificat (ou d'envoi de certificat non conforme), le client stoppe immédiatement les échanges avec le serveur. Il peut arriver de temps en temps que le responsable d'un site oublie de renouveler son certificat à temps (dépasse la date d'expiration), dans ce cas, le navigateur web côté client affichera une page de mise en garde avec un message du style **"ATTENTION le certificat d'authentification du site XXX a expiré, il serait prudent de ne pas poursuivre vos échanges avec le site XXXX"**.

Activité 2

La cryptologie est la science du secret. Cette science trouve ses origines dans la Grèce antique. Faites une frise chronologique qui reprend les principales dates de l'histoire de cette science. Entrez un peu plus dans les détails pour les éléments suivants :

- code de César
- chiffre de Vigenère
- Enigma

Activité 5

Résumez en quelques lignes le principe du protocole HTTPS.

Exercice 1

- 1- Après un chiffrement symétrique on obtient le message suivant : **ri**. Sachant que la clé de chiffrement est : 00001010 (la clé est directement donnée en binaire), déterminez le message d'origine.

On donne l'extrait de la table ASCII suivant :

lettre	code binaire	lettre	code binaire
a	01100001	t	01110100
b	01100010	v	01110110
c	01100011	w	01110111
d	01100100	x	01111000
e	01100101	y	01111001
f	01100110	z	01111010
i	01101001	(vertical bar)	01111100
r	01110010	{ (left opening brace)	01111101
s	01110011	~ (tilde)	01111110

2- Un utilisateur B souhaite échanger un message chiffré avec un utilisateur A en utilisant un chiffrement asymétrique. A possède une clé publique (AKpub) et une clé privée (AKpriv). B possède une clé publique (BKpub) et une clé privée (BKpriv). B souhaite chiffrer un message m afin de pouvoir l'envoyer à A :

- a- Quelle clé va être utilisée par B pour chiffrer le message m ?
- b- Quelle clé va être utilisée par A pour déchiffrer le message m ?

3- Expliquez en quelques lignes le principe du protocole HTTPS (*on s'intéressera uniquement à l'aspect Sécurité du protocole*)

Exercice 2

Exercice tiré du bac 2021

Pour chiffrer un message, une méthode, dite du masque jetable, consiste à le combiner avec une chaîne de caractères de longueur comparable. Une implémentation possible utilise l'opérateur **XOR** (ou exclusif).

Dans la suite, les nombres écrits en binaire seront précédés du préfixe 0b.

- 1- Pour chiffrer un message, on convertit chacun de ses caractères en binaire (à l'aide du format Unicode), et on réalise l'opération **XOR** bit à bit avec la clé.

Après conversion en binaire, et avant que l'opération **XOR** bit à bit avec la clé n'ait été effectuée, Alice obtient le message suivant :

m = 0b 0110 0011 0100 0110

- a- Le message **m** correspond à deux caractères codés chacun sur 8 bits : déterminer quels sont ces caractères. On fournit pour cela la table ci-dessous qui associe à l'écriture hexadécimale d'un octet le caractère correspondant (figure 2). Exemple de lecture : le caractère correspondant à l'octet codé 4A en hexadécimal est la lettre J.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	space	!	"	#	\$	%	&	'	()	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{		}	~	DEL

Figure 2

b- Pour chiffrer le message d'Alice, on réalise l'opération XOR bit à bit avec la clé suivante :

$k = 0b\ 1110\ 1110\ 1111\ 0000$

Donner l'écriture binaire du message obtenu.

2-

a- Dresser la table de vérité de l'expression booléenne suivante :

(a XOR b) XOR b

b- Bob connaît la chaîne de caractères utilisée par Alice pour chiffrer le message. Quelle opération doit-il réaliser pour déchiffrer son message ?