Sécurisation des communications

1. Introduction

La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou clés. Elle se distingue de la stéganographie qui fait passer inaperçu un message dans un autre message alors que la cryptographie rend un message supposément inintelligible à une autre personne que celle autorisée.

Elle est utilisée depuis l'Antiquité, mais certaines de ses méthodes les plus modernes, comme la cryptographie asymétrique, datent de la fin du XXe siècle.

Regarder la vidéo d'introduction de « L'informateur » sur YT.

Rappel : Le code de César a été vu en 1ere NSI ainsi que le chiffre de Vigenère. Un historique des différents codes à travers les âges est consultable sur Wikipédia.

A partir de la vidéo précédente définir les 3 mots suivants :

Confidentialité	**Seule la personne autorisée peut avoir accès au message qui lui est destiné. Même si le message est intercepté le pirate ne pourra pas lire le message.**
Authenticité	**Lors de la réception d'un message, le destinataire doit être sûr que celui**-ci provient de la bonne personne. Le message est alors authentique.
Intégrité	**Lors du trajet, le message ne peut pas être transformé. Le message est bien intègre.**

2.Le cahier des charges d'un crypto système

- Le cryptage doit être simple mais l'opération réciproque difficile, voire impossible, en l'absence d'une information (la clef).

- Le concept de clef : c'est un paramètre de l'algorithme de chiffrement. Il peut donc être changé sans modifier l'algorithme. Un même algorithme peut alors être employé par plusieurs personnes qui utilisent des clés différentes. Le principe de Kerckhoffs s'énonce ainsi : « La sécurité d'un crypto système doit résider dans le secret de la clé. Les algorithmes utilisés doivent pouvoir être rendus publics »

- L'efficacité d'un crypto système dépend donc aussi de la facilité à construire et distribuer des clefs. Si la clef est secrète et est nécessaire au décryptage, il faudra prévoir un canal de communication séparé.

- Lorsque la clef permet à la fois de crypter et décrypter on parle de chiffrement symétrique.

- On peut mettre en place un chiffrement asymétrique : dans ce nouveau système, si une personne connait la clef de chiffrement (la clef publique), il peut crypter le message mais pas le décrypter. Il a besoin pour cela d'une autre clef (la clef privée qui reste secrète).

3.Chiffrement symétrique

3.1 Introduction

Regarder la vidéo de « L'informateur » sur YT.

A partir de la vidéo précédente définir les 3 mots suivants :

Chiffrement par bloc (block cipher)	
DES	Data Encryption Standard
AES	Advanced Encryption Standard

Quelle est la longueur de la clé d'un cryptage DES ?

56 bits

Quelles sont les différentes longueurs des clés du cryptage AES ?

128, 192 et 256 bits

Quelle est la limite pratique d'un chiffrement symétrique ?

L'expéditeur et le destinataire doivent se mettre d'accord sur le contenu de la clé de cryptage.

3.2 Le chiffrement à masque jetable de type « ou exclusif »

A l'aide du fichier **`cryptageMaquetteExcelAnalyse.xlsx`** , crypter le mot « SPECIALITE » en utilisant la clef « CRYPTAGE ».

Essayer de crypter votre prénom avec une autre clé.

Table de vérité du ou exclusif (XOR)

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

Fonctions du tableur :

- Transformer un caractère en son code Ascii : = CODE (caractère)
- Transformer un code Ascii en son caractère : = CAR(entier)
- Convertir un décimal en binaire : =DECBIN(decimal)
- Convertir un binaire en décimal =
- Effectue le « ou exclusif » bit à bit entre deux entiers : BITOUEXCLUSIF (entier1; entier2)
- (ou BITXOR(entier1;entier2) en version anglaise)

Message à Crypter en caractère	S	P	E	C	I	L	I	T	E	N	S	I
Message numérisé en Ascii	83	80	69	67	73	76	73	84	69	78	83	73
Message numérisé en Binaire	1010011	1010000	1000101	1000011	1001001	1001100	1001001	1010100	1000101	1001110	1010011	1001001
Clef Cryptage en caractère	C	R	Y	P	T	A	G	E	C	R	Y	P
Clef cryptage en ascii	67	82	89	80	84	65	71	69	67	82	89	80
Clef de cryptage binaire	1000011	1010010	1011001	1010000	1010100	1000001	1000111	1000101	1000011	1010010	1011001	1010000
Cryptogramme par masque xor en binaire	10000	10	11100	10011	11101	1101	1110	10001	110	11100	1010	11001
Cryptogramme en décimal	16	2	28	19	29	13	14	17	6	28	10	25
Cryptogramme en caractère	†	┐		‼			♬	◄	–			├
Vérification décryptage ascii	83	80	69	67	73	76	73	84	69	78	83	73
Décryptage caractères.	S	P	E	C	I	L	I	T	E	N	S	I

3.3 Mise en pratique du chiffrement à masque jetable en python

On se propose de coder une fonction en Python qui va réaliser le cryptage (et le décryptage puisque l'opération est symétrique).

Si le message est de taille supérieure à la clef, on réalise sur celle-ci une rotation : on revient au début de la clef, comme dans l'exemple du tableur.

Dans l'idéal, il faudrait utiliser une clef générée aléatoirement et de longueur égale au message, ce qui rendrait le décryptage incassable (pourvu que cette génération soit réellement aléatoire !).

Algorithme de cryptage symétrique :

Résultat ← chaine vide
Pour chaque caractère du message
    Numériser ce caractère (le transformer en valeur décimale).
    Extraire de la clef le caractère correspondant, puis le numériser.
    Appliquer l'opération « ou exclusif ».
    Transformer ce dernier résultat en un caractère.
    Concaténer ce caractère obtenu dans le résultat.
Fin Pour

Rappel de fonctions usuelles vues en 1ere NSI :

Instructions	Résultat affiché dans la console

`A = 'SPECIALITE'`
`print(A[0])`
`print(A[2])`
`print(ord(A[2]))`
`print(chr(83))`
	S
	E
	69
	S

`a=13`
`b=5`
`print(a//b)`
`print(a%b)`
	2
	3

`a=83`
`b=67`
`c=a^b`
`print(c)`
	16

Compléter la fonction cryptage du script python suivant :

Script Python

```
def cryptage(message, clef):
    longueur=len(clef)
    cryptogramme=''
    # A completer



    return(cryptogramme)

crypto1=cryptage("Il fait super beau aujourd'hui", 'Test')

fichier = open("cryptage.txt", "w", encoding='utf8') # ouverture en mode write
fichier.write(crypto1)
fichier.close()

fichier = open("cryptage.txt", "r", encoding='utf8') # ouverture en mode read
cryptogramme=fichier.read()
fichier.close()

messageDecrypte=cryptage(cryptogramme, 'Test') # On décrypte !

fichier = open("decryptage.txt", "w", encoding='utf8')
fichier.write(messageDecrypte)
fichier.close()
```

4.La sécurité du chiffrement à masque jetable

4.1 Attaque par force brute

L'attaque par force brute est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles. Reprenons notre exemple (message : SPECIALITENSI, clef = CRYPTAGE) et tentons de casser le code, c'est à dire de trouver le message initial sans connaitre la clef.

On dispose des renseignements suivants :

- On connait l'algorithme utilisé (Le principe de Kerckhoffs) : on sait donc que la clef est constituée de caractères codés sur un octet.
- Pour 1 caractère combien de combinaisons doit-on tester ? **256**
- Pour 2 caractères ? **256^2 ou 2^{16}**
- Pour n caractères ? **256^n**

La complexité en temps d'un algorithme utilisant cette stratégie serait de 256^n (n : taille message). La durée pour casser le code n'est pas acceptable, sauf si l'on connait la langue utilisée.

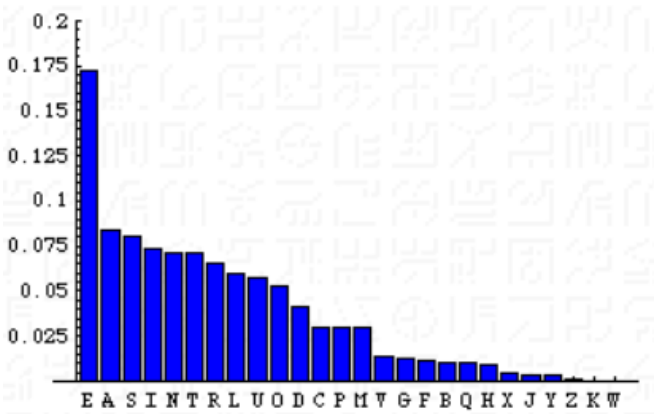
4.2 Notion d''analyse fréquentielle.

En français la fréquence d'apparition des lettres dans un texte est très variable selon la lettre.

Analyse des fréquences en français

Fréquences d'apparition des lettres

Lettre	Fréquence	Lettre	Fréquence
A	8.15 %	N	7.12 %
B	0.97%	O	5.28 %
C	3.15 %	P	2.80 %
D	3.73 %	Q	1.21 %
E	17.39 %	R	6.64 %
F	1.12 %	S	8.14 %
G	0.97 %	T	7.22 %
H	0.85 %	U	6.38 %
I	7.31 %	V	1.64 %
J	0.45 %	W	0.03 %
K	0.02 %	X	0.41 %
L	5.69 %	Y	0.28 %
M	2.87 %	Z	0.15 %



Quelle lettre est la plus fréquente ? **E**

Quelle lettre est la moins fréquente ? **K**

Pour éviter l'analyse fréquentielle, il faut que le message crypté soit plat, c'est-à-dire que les fréquences d'apparition des lettres soient sensiblement identiques.

5.Chiffrement asymétrique

5.1 Introduction

Regarder la vidéo de « L'informateur » sur YT. (Ne pas hésiter à faire des retours en arrière)

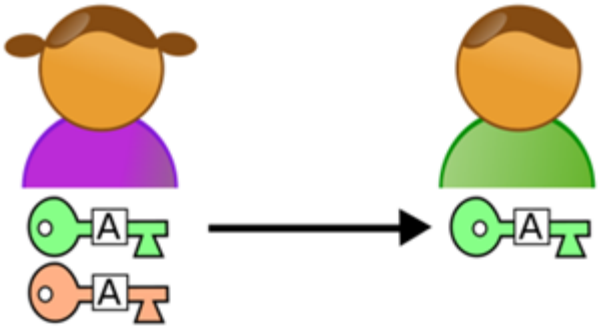
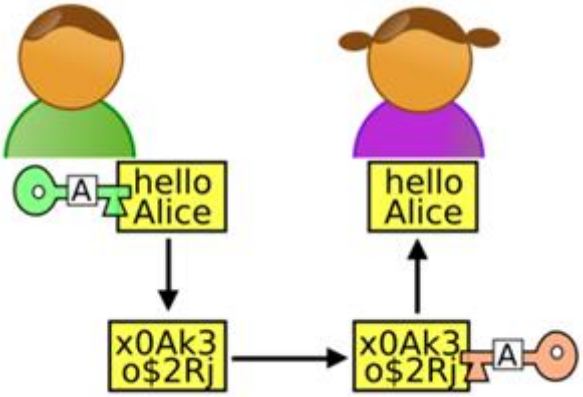
Que signifie l'acronyme du chiffrement RSA ?

Le chiffrement RSA asymétrique vient du nom de ses inventeurs (Rivest, Shamir et Adleman).

Quels sont les deux outils mathématiques indispensables du chiffrement RSA ?

Modulo et factorisation.

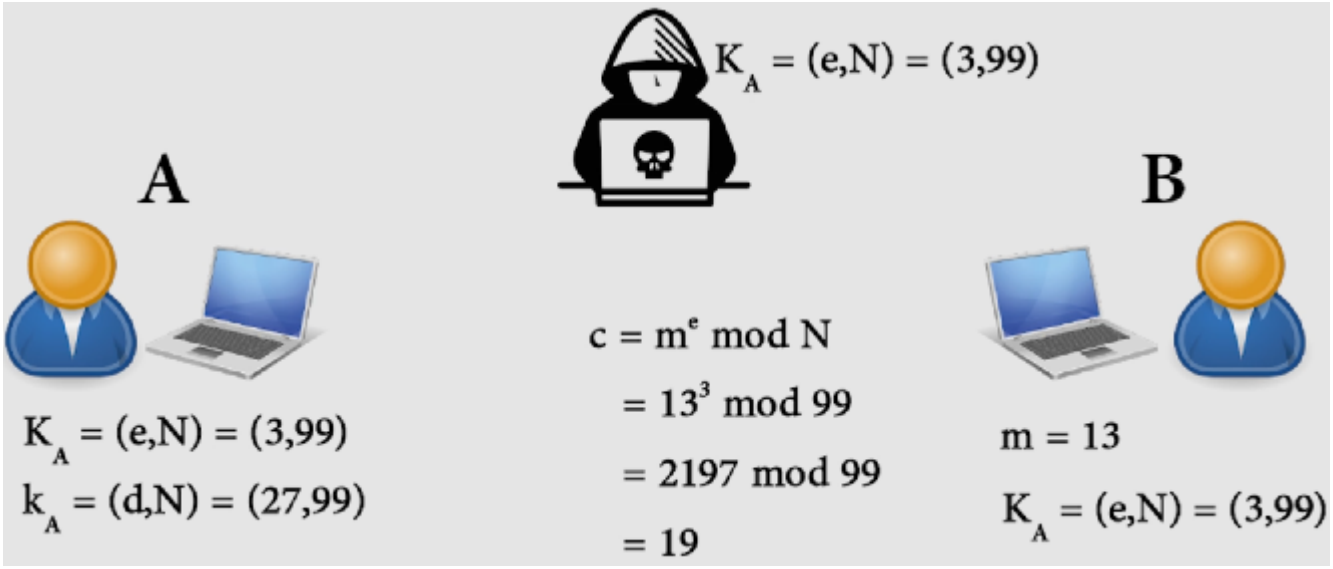
5.2 Principe du chiffrage asymétrique

	**1ere étape : Alice génère deux clés.** La clé publique (verte) qu'elle envoie à Bernard et la clé privée (rouge) qu'elle conserve précieusement sans la divulguer à quiconque.
	**Deuxième et troisième étapes :** Bernard chiffre le message avec la clé publique d'Alice et envoie le texte chiffré. Alice déchiffre le message grâce à sa clé privée.

5.3 Principe Mathématique

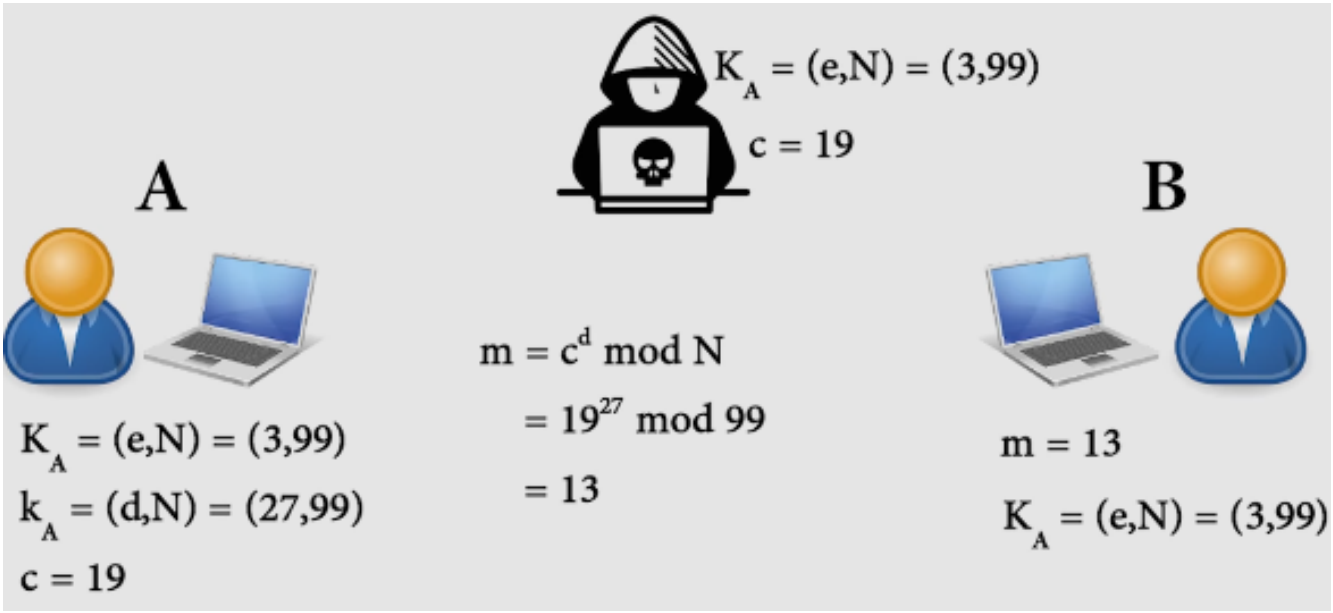
1ere étape :

- A envoie à B sa clé publique K_A
- B chiffre le message 13 avec la clé publique de A. Cela donne 19



2ème étape :

- A déchiffre le message c avec sa clé privée k_A. Cela donne bien le message d'origine (13)



5.4 Le protocole TLS

Regarder la vidéo d'introduction de « L'informateur » sur YT.

Que signifie l'acronyme TLS?

TLS signifie Transport Layer Security. C'est la sécurité de la couche de transport.

Rappeler à nouveau les 3 propriétés de sécurité.

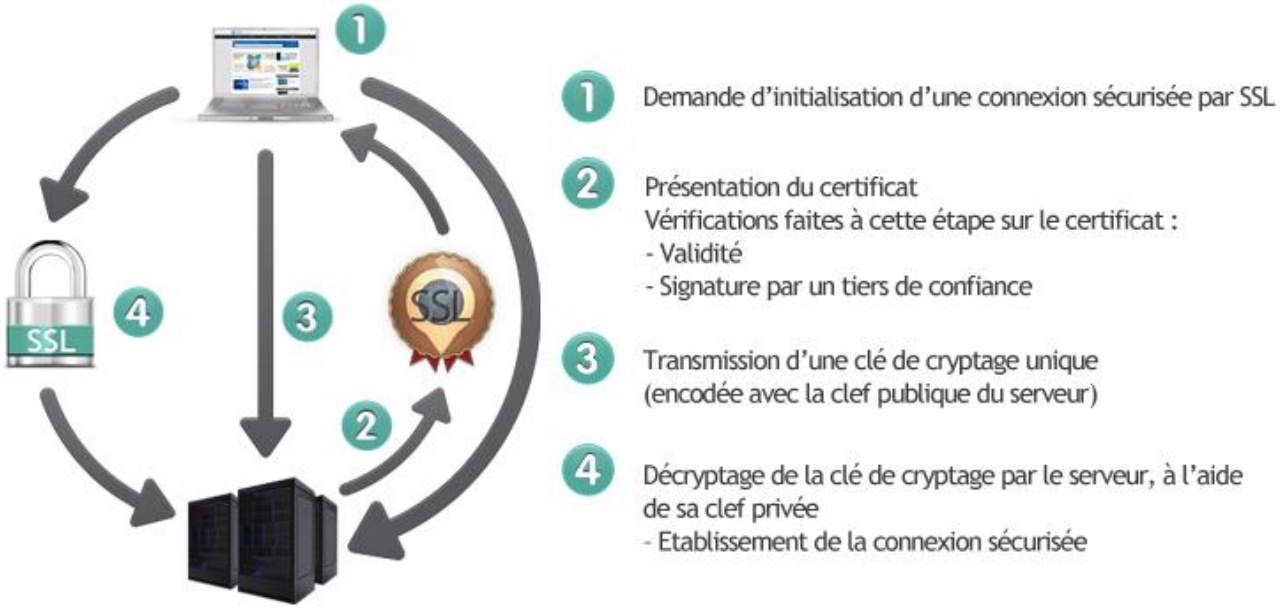
Confidentialité, authenticité et intégrité.

Quel est le numéro du port sécurisé de HTTPS pour le protocole TCP ?

443

Résumé :

- HTTPS utilise un chiffrement asymétrique pour établir une connexion et échanger une clé symétrique
- Ensuite les échanges utilisent un chiffrement symétrique. L'intérêt de ce système est que le chiffrement symétrique est beaucoup moins gourmand en ressources. Une fois la connexion établie, l'HTTPS consomme des ressources CPU assez raisonnables.



A voir : La cryptographie quantique