Chiffrement des données

Exercices

Codage des données
Objectif(s) :
A la fin des exercices, l'élève doit être capable de :

- Chiffrer des données selon
  - Chiffrement de César
  - Chiffrement de Vigenère
- Utiliser un outil de chiffrement symétrique
  - Chiffrement AES-256.
- Créer des empreintes de
  - Mot de passe.
  - Fichier

Durée prévue : Selon UD

Exercice 1, Chiffrement de César

Chiffrement par substitution monoalphabétique.

1. Chiffrez une phrase de votre choix de 5 mots au minimum avec la clé de votre choix.
2. Donnez le message chiffré ainsi que la clé à votre voisin
3. Lui fera de même et chacun déchiffrera le message du voisin.

Message en clair :

Clé secrète :

Message chiffré :

Exercice 2, Chiffrement de Vigenère

Chiffrement par substitution polyalphabétique

Réalisez les points suivants :

1. Chiffrez une phrase de votre choix de 5 mots au minimum avec la clé « cryptographie ».
2. Donnez le message chiffré ainsi que la clé à votre voisin.
3. Lui fera de même et chacun déchiffrera le message du voisin.
4. Contrôlez si votre voisin a bien déchiffré le message.

Plier ici

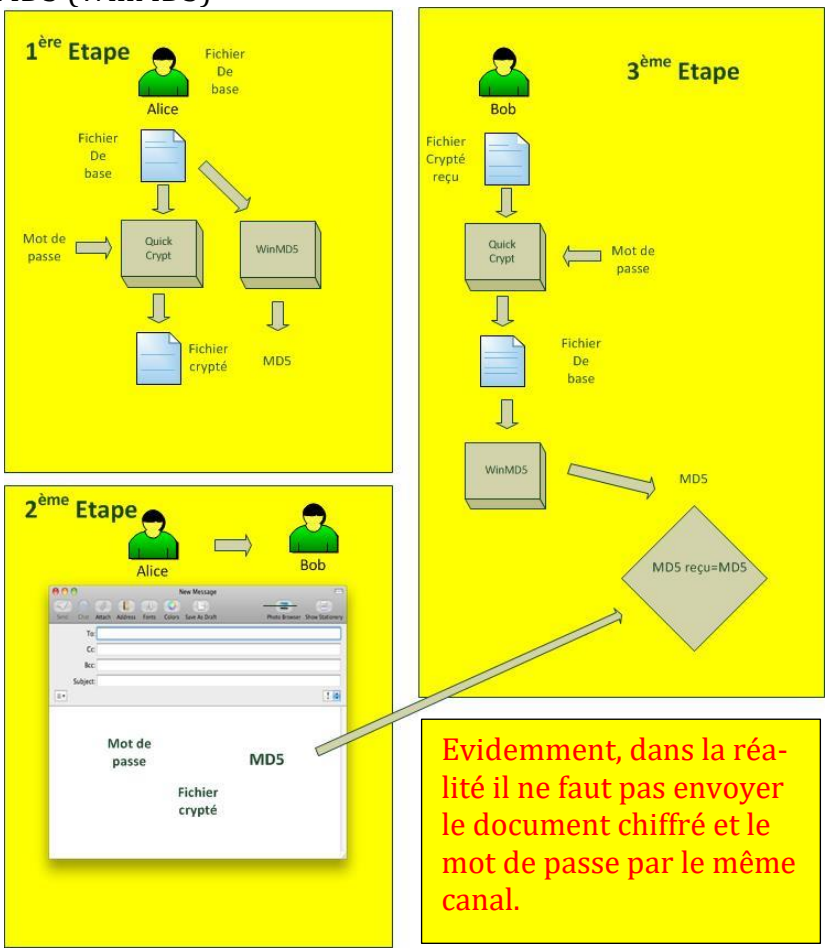
Lettre de la clé	Lettre en clair																								
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Lettres chiffrées (au croisement de la colonne *Lettre en clair* et de la ligne *Lettre de la clé*)																								
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	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

Exercice 3, Chiffrement AES-256

Chiffrement symétrique

Quick Crypt 1.1 est petit outil portable offrant le chiffrement AES-256 pour la protection des fichiers et documents sensibles. A l'aide de ce logiciel réalisez les points suivants :

- Vous êtes Alice, lancez Quick Crypt et avec l'aide du générateur de mot de passe sécurisé (menu Tools) générez une clef de chiffrement et chiffrez un fichier de votre choix.
- Trouver l'empreinte MD5 de votre ficher original.
- Transmettez le fichier chiffré, le mot de passe et l'empreinte à votre voisin (Bob) demandez-lui de le déchiffrer et de lire le contenu du fichier.
- Votre voisin (Bob) compare le résultat avec votre fichier original à l'aide d'une empreinte MD5 (WinMD5)



Evidemment, dans la réalité il ne faut pas envoyer le document chiffré et le mot de passe par le même canal.

- Recherchez quelles sont les autres possibilités de ce logiciel et mettez-les en pratique :

.....
.....
.....
.....

Exercice 4, Hachage d'un mot de passe

Hachage en ligne avec MD5

A l'aide du site : http://www.cryptage-md5.com vous pourriez chiffrer/hacher vos mots de passe pour ensuite les insérer, par exemple, dans votre base de données de votre programme. Bien entendu, dans la réalité, ce processus se fait automatiquement avec votre programme.

1. Hachez un mot de passe et avec le résultat, essayez de trouver un site qui décrypte ce code
2. Quelle conclusion en tirez-vous ?

.....

.....

.....

.....

.....

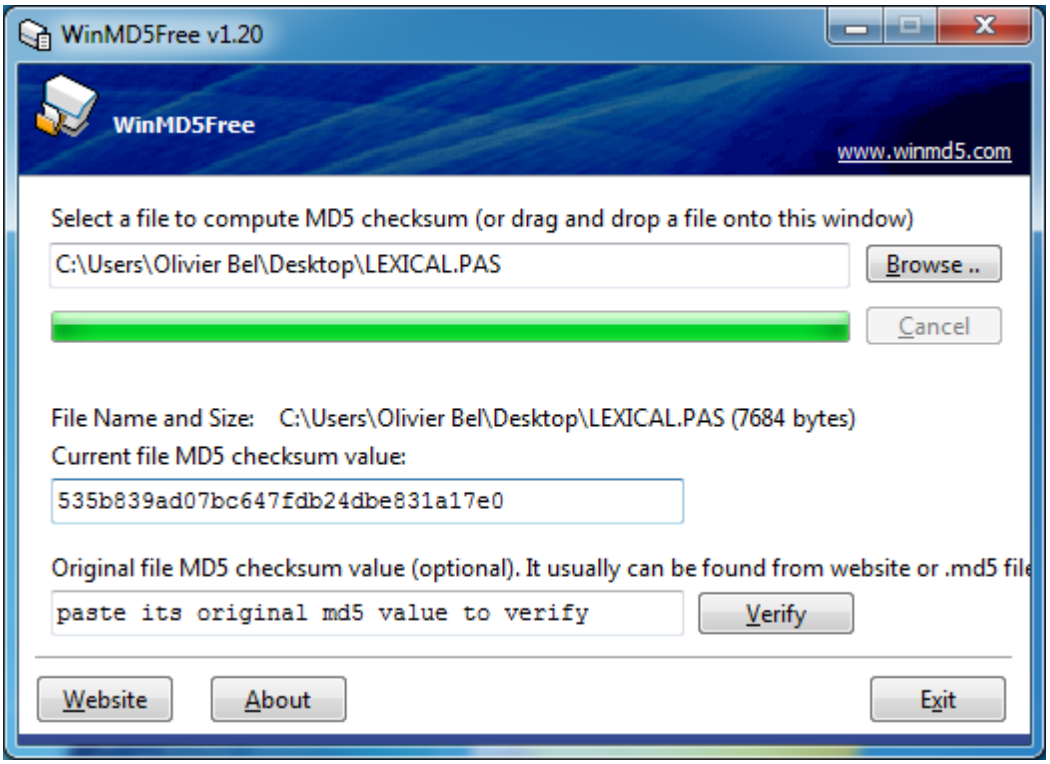
.....

Exercice 5, Création d'une empreinte de fichier

Hachage MD5

Pour avoir l'empreinte MD5 d'un fichier (que ce soit un document texte, une photo, ...), il vous suffit d'avoir une fonction ou un petit logiciel tel que WinMD5 qui le calcule.

1. Editez un document texte avec le bloc-notes et inscrivez quelques lignes de texte de-dans avant de l'enregistrer.
2. Créez, à l'aide de WinMD5, son empreinte numérique.
3. Dans mon cas j'obtiens l'empreinte suivante :
   `535b839ad07bc647fdb24dbe831a17e0`



4. Ouvrez à nouveau votre fichier texte, et modifiez son contenu, ne serait-ce qu'une lettre et vérifiez à nouveau son empreinte. Elle est devenue, dans mon cas : **`4b81c3d969433e3795d8be6b54a8dffb`**. Totalement différente de l'originale.