Cryptographie et Sécurité
Série 1 : Cryptographie Classique

18 Septembre 2019

A rendre exclusivement sur papier, au plus tard au début de la séance du **25 Septembre 2019 et avant 17h15**.

Toutes vos réponses doivent être justifiées.

Exercice 1: César

Le décalage de César consiste à décaler tous les caractères du message d'un même nombre de places. Ce nombre est la clé. Par exemple, une clé de 3 remplace le A par le D, le B par le E, etc... La permutation est circulaire, lorsqu'on atteint la fin de l'alphabet, on reprend au début (avec la clé 3, X devient A, Y devient B, Z devient C).

- Codez le message "BONJOUR" avec la clé 4.
- En considérant l'alphabet comme uniquement les lettres de A à Z, combien de clés différentes existe-il ? Et en considérant les caractères de l'ASCII 8 bits ?
- Est-il difficile de casser ce codage ?

Exercice 2 : Substitution Monoalphabétique

La substitution monoalphabétique consiste à assigner à chaque caractère un autre caractère. Par exemple, la clé MONALPHBETIQUCDFGJKRSVWXYZ remplace chaque A par un M, chaque B par un O, chaque C par un N, ...
Pour simplifier, on prend souvent une phrase ou un texte comme clé : on prend alors les lettres dans l'ordre ou elles apparaissent dans le texte pour construire la clé, en enlevant les lettres déjà apparues plus tôt. On ajoute alors les éventuelles lettres restantes de l'alphabet pour terminer la clé.
On observe facilement que la clé donnée ci-dessus est créée ainsi à partir du mot "MONOALPHABETIQUE".

- Le message "BGYDKCNGSDMAIBHSJJAFRI" à été encodé à l'aide de la phrase "substitutionmonoalphabétique". Donnez la clé complète, puis indiquez quel est le message original.
- Est-il difficile de casser ce codage ?

Exercice 3 : Algorithme de Vigenère

On s'attarde maintenant sur les substitutions polyalphabétiques, avec le codage de Vigenère. On donne une valeur à chaque caractère : le A vaut 0, le B vaut 1, et ainsi de suite jusqu'au Z qui vaut 25. La substitution est faite en sommant la valeur du caractère du message à la valeur du caractère à la même position de la clé, modulo 26. On obtient alors la valeur du nouveau caractère (et si l'on dépasse 25, le modulo nous fait repartir à A=0). La clé est une chaine de caractère, que l'on répète autant de fois que nécessaire pour atteindre la même longueur que le message.
Par exemple, le message BONJOUR encodé avec la clé BAC donne le message COPKOWS ($B + B = C$, $O + A = O$, $N + C = P$, puis on recommence au début de la clé, $J + B = K$, et ainsi de suite).

La figure 1 montre la table de Vigenère pour sommer ces caractères.

- Encodez le message "JESUISUNPOKEMON" avec la clé "ABRA".
- Décodez le message "JFJUITLNDSVSSFLR", sachant que la clé est de nouveau "ABRA".
- Sachant que la clé est beaucoup plus courte que le message, est-il difficile de casser ce codage ?
- Et qu'en est-il si la clé est de la même longueur que le message ?

	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
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

Figure 1: Table de Vigenère