

Correction du TD N° 1

Exercice 1 : Le code de César est considéré comme le plus ancien algorithme de chiffrement par substitution. La technique est élémentaire : il suffit de remplacer chaque lettre du texte à chiffrer par la lettre qui se situe 3 places plus loin dans l'alphabet (on remplacera A par D, B par E, C par F..., X par A, Y par B et Z par C).

Exemple : SMIA PREMIERE ANNEE donne VPLD SUHPLHUH DQQHH

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
code	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

1. Chiffré le message : BONJOUR A TOUS

Correction :

B → E, O → R, ..., S → V : BONJOUR A TOUS → ERQMRXU D WRXV

2. Déchiffré le message suivant : DLG PRXEDUHN VDLG

Correction :

D → A, L → I, ..., G → R : DLG PRXEDUHN VDLG → AID MOUBAREK SAID

Exercice 2 : J'ai crypté avec le code de César, le texte donné ci-dessous. Mais j'ai oublié la clé pour le décoder. Avec le diagramme en bâtons, aider moi à décoder le texte suivant (expliquer la méthode) :

KV USXNS ZELVSO VO ZBOWSOB YEFBKQO NO MBIZDKXKVICO, (WKXECMBSD CEB VO NOMRSPPBOWOXD NOC WOCKKQOC MBIZDYQBKZRSAEOC) BODBYEFO OX 1987 NKXC VOC KBMRSFOC YDDYWKXOC K SCDKXLEV, MOD YEFBKQO ZBOCOXDO VK DOMRXSAEO N'KXKVICO PBOAEOXDSOVVO NOC VOEDBOC NE DOHDO MRSPPBO

Correction :

La méthode d'Alkindi est de compter l'occurrence de chaque lettre dans le texte et trouver la lettre la plus réputer dans le texte K → 14, V → 11, U → 1, S → 11, X → 11, ..., O → 39 Dans la langue française la lettre la plus réputer est le E donc ici dans le texte le O provient du E : donc décalage de 10, on décale toutes les lettres de 10 on obtient :

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
code	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

Pour décoder le message on remplace : K → A, V → L, U → K, S → I, X → N, N → D, S → I, ... le résultat est :

AL KINDI PUBLIE LE PREMIER OUVRAGE DE CRYPTANALYSE MANUSCRIT SUR LE DECHIFFREMENT DES MESSAGES CRYPTOGRAPHIQUES RETROUVEES DANS LES ARCHIVES OTTOMANES A ISTANBUL CET OUVRAGE PRESENTE LA TECHNIQUE D ANALYSE FREQUENTIELLE DES LETTRES DU TEXTE CHIFFRE