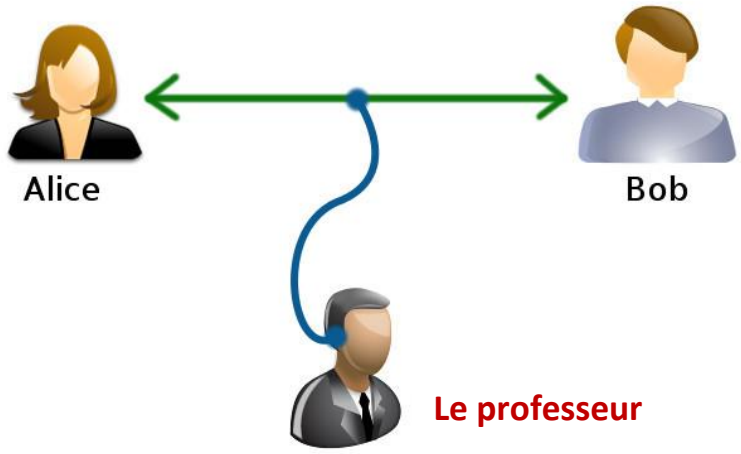
Sujet Collège – Codage et décodage de messages secrets

Bob est un jeune garçon qui souhaite recevoir des messages secrets de Alice. Il ne veut pas que leur professeur sache ce qu'Alice lui écrit.



Comment vont-t-ils faire ?

1ère méthode – La méthode par substitution *(utilisée durant l'antiquité)*

1/ Ecrivez/recopiez des textes en français et complétez pour chaque texte le tableau 1 donné en annexe.

2/ Rappelez les propriétés de la fréquence en pourcentage.

3/ Compléter le tableau 2. Quel est l'intérêt de ce second tableau ?

5/ Pour que le professeur ne puisse pas prendre connaissance de son message, Alice a remplacé chaque lettre par une autre lettre. Bien entendu, deux lettres distinctes ne peuvent être codées par la même lettre. Aidez Bob à décrypter le message d'Alice.

Alice : « Rd zgqmh fj'bjrqjgy'ujm, rd td kbmh xbh gdhidg b w'dzqwd. Xqjgfjqm ? Xbgzd fjd r'bm sbw b wb idid. Au tqt xwjiqi bj kdtigd. Di xjmh hjgiqji, r'bm w'msxgdhhmqt y'bkqmg yd wb amdkgd. Hm hdjwdsdti rd xqjkbmh bkqmg wb smegbmtd. Qj biigbxdg jt cqt egqh gujsd.

Sbhhjyb, z'dhi sqt kqmhmt yd zwbhhd. Jt rqjg, mw b ydhhmtd jtd wmetd hjg tqigd ibcwd di mw s'b amodd y'jt bmg sdzubti dt sd ymhbti : « Hm ij ydxbhhdh, ebgd b iqm ! ». Qjbty sdh smdiidh yd eqssd ydcqgydti yd hqt zqid, mw abmi igdscwdg sb zubmhd dt yqttbti yd egbtyh zqjxh yd xmdy ydybth. Di Sbhhjyb, zb wd abmi gmeqwdg.

Umdg, rjhid bkbti wb amt ydh zqjgh, qt h'dhi ymhxjidh. Sbhhjyb b zbhhd sqt zbydbj y'bttmkdghbmgd : jt rqwm zgbpqt fjm hdtibmi cqt wb agbmhd. R'dibmh hm igmhid fjd rd sd hjmh smhd b xwdjgdg !

Rd wjm bm rdid sb eqssd b wb amejgd… R'bm cmdt kj fj'mw td h'p biidtybmi xbh ! Bxgdh, mw t'b xbh bggdid yd sd gdebgydg y'jt qdmw tqmg.

Rd sd hjmh ydxdzudd yd gdtigdg sbmh rd hbmh fj'bjrqjgy'ujm, mw kb hd kdtedg.

Rd td kdjo xbh gdhidg b w'dzqwd. Rd kdjo gdtigdg b wb sbmhqt… Qu ! Rd t'dt gdkmdth xbh. Sbhhjyb kmdti yd sd yqttdg jtd xdimid ibxd dt cgdyqjmwwbti : « Wbgyqt ! ». »

http://www.cryptage.org/outil-crypto-substitution.html

Taille des blocs : 5 - Tableau de substitution :

CLAIR	A	B	C	D	E	F	G	H	I	J	K	L	M
CODE	b	c	z	y	d	a	e	u	m	r	v	w	s

CLAIR	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CODE	t	q	x	f	g	h	i	j	k	l	o	p	n

6/ A présent, Alice envoie un message en allemand à Bob. Pouvez-vous utiliser le tableau élaboré pour la langue française ? Comment allez-vous procéder ? Donnez un exemple.

Alice : « Dmtdh Sqgedth vbs dmt edlbwimedg Cbg kqs wmtvdt Jadg Ydh Awjhhdh Bja Ymd Cgjzvd nj.

Njg ewdmzudg Ndmi vbs dmt Gmdhd kqs gdzuidt Jadg. Cdmyd lqwwidt jcdg ymd wbted, hzusbwd Cgjzvd. Edtbj mt ydg Smiid igbadt ymd cdmydt bjadmtbtydg. Ydg Cbg gmzuidid hmzu uqzu bja. Dg hzujiidwid ydt Vqxa jty cgjssid nqgtme. Tdmt, dg ljgyd tmzui jsvdugdt, js yds Gmdhdt Xwbin nj sbzudt. Ydg Gmdhd hibty gjume yb. Tdmt, bjzu dg ljgyd tmzui jsvdugdt. Js btdmtbtydg kqgcdmnjedudt, lbg ymd Cgjzvd nj hzusbw.

« Lmg sjhhdt dmtd Lqhjte amtydt », hbeid ydg Gmdhd. Ydg Cbg tmzvid.

« Mzu ubch ! », gmda ydg Gmdhd xwqinwmzu. Dg sbzuid dmtdt Hzugmii bja ydt Cbgdt nj. « Mzu ubwid ymzu jty yj ubwihi smzu. Hq vbtt vdmtdg mt ymd Lmdad hijgndt. Jty ybtt ygdudt lmg jth. » « Dmtkdghibtydt », hbeid ydg Cbg. Dh hbu bjh bwh ljgyd ydg Cbg jty ydg Gmdhd smidmtbtydg ibtndt. Ebtn vwdmtd Hzugmiid sbzuidt hmd, jty smi rdyds Hzugmii cdldeidt hmd hmzu dmt Hijzv ldmidg. Edsdmthbs hzuldcidt hmd jcdg yds Bcegjty, jty dmtdg umdwi ydt btydgdt adhi. Dtywmzu hibty rdydg bja ydg Hdmid ydg Cgjzvd bja ydg dg hdmt lqwwid. « Mzu ybtvd ymg », hbeid ydg Gmdhd. « Jty mzu ybtvd ymg ! », hbeid ydg Cbg. Ymd cdmydt lmtvidt dmtbtydg agdjtywmzu nj, ybtt hdinid rdydg Hdmtdt Lde aqgi. »

7/ Pensez-vous que cette méthode de codage et décodage permet de décoder tous les messages secrets ? Pour quel type de messages est-elle la plus efficace ?

8/ Que pensez-vous de la fiabilité de la méthode en termes de confidentialité ?

ECRIVEZ LE TEXTE

	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	TOTAUX
Effectif																											
Fréquence (%)																											

Effectif : c'est le nombre d'apparition de la lettre dans le texte. Il vous suffit de compter la lettre dans votre texte.
Effectif total : c'est la somme des effectifs de chaque lettre de l'alphabet. Faites une addition !!!
Fréquence (%) : pour calculer la fréquence en pourcentage d'une lettre, on divise l'effectif de la lettre par l'effectif total, et on multiplie par 100. On arrondit à deux chiffres après la virgule.

Titre du texte	EFFECTIFS DES LETTRES																										
	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	TOTAUX
Totaux des effectifs																											
Fréquences (%)																											

Jules César envoyait souvent des messages secrets à l'aide de la méthode par décalage additif.
Mais, qui était Jules César ? Et dans quelle langue parlait-il ?

2ème méthode – La méthode par décalage additif *(utilisée par Jules César)*

Cette fois-ci, Alice note le rang dans l'alphabet de chaque lettre du message secret, puis ajoute à ce rang un même nombre entier qu'on appelle la clé secrète – personne ne connaît la clé secrète hormis Bob et Alice.

Par exemple, si Alice a une clé de 3 et s'il veut envoyer la lettre B à Bob, il notera que B est à la seconde place dans l'alphabet, calculera 2+3=5 et enverra finalement la lettre E (car E à la cinquième place).

1/ Que devient la lettre F si Alice choisit une clé secrète de 5 ? Que devient MATH EN JEANS avec une clé secrète de 4 ?

2/ Comment procède-t-on pour la lettre Z avec une clé secrète de trois ? Pour la lettre X avec une clé secrète de 8 ? Pour la lettre K avec une clé secrète de 120 ? Pour la lettre R avec une clé secrète de 4 589 ?

3/ Alice veut envoyer un message à Bob (en français ou en allemand). Il commence donc par choisir une clé. Inventez cette clé, imaginez le message de Alice (en français ou en allemand) puis codez ce message.

4/ Combien de clés existe-t-il ? Dressez un tableau à double entrée facilitant le décodage des messages secrets.

5/ Si un message est codé avec un clé secrète égale à +n, comment le décodera-t-on ?

6/ Alice a envoyé un second message à Bob. Malheureusement, son amie a oublié la clé secrète. Aidez-la à retrouver la clé et à décoder le message de Alice.

Alice : « Eglgjvm k'shhjguzw v'mfw bwmfw xaddw.

- Tgfbgmj, bw kmak dw hjafuw Eglgjvm.
- Wl ega, bw kmak ds hjafuwkkw Vwrwugddw wl bw kmak hjgxwkkwmjw vsfk mfw wugdw, jwhgfval d'smljw.
- Xgjl tawf, val dw hjafuw, wl imw vajawr-ngmk v'mfw hjgewfsvw vsfk uw hwlal hgak im'gf ngal ds-tsk ?
- Mf hwlal hgak ? k'wlgffw ds hjafuwkkw, esak gf fw kw hjgewfw hsk vsfk mf hwlal hgak ! U'wkl mf hwlal tgak im'gf ngal ds-tsk.
- Mf hwlal tgak ? Hsk vm lgml, jwhgfval dw hjafuw, dwk hwlalk tgak, gf dwk esfyw. B'wf kmak v'saddwmjk xjasfv wl ad e'sjjanw v'wf esfywj lsfl imw b'wf lgetw ksdsvw. B'slljshw sdgjk vw nadsafk egmlgfk ima ew vwesfywfl lgmlw ds fmal ! - S egf snak, ngmk kgmxxjwr vw eglk vw lwlw, k'wpudses ds hjafuwkkw Vwrwugddw wl bw nsak ngmk kgayfwj vsfk egf wugdw.

Sm tgml vw imwdimwk kwesafwk vw udskkw, Eglgjvm hsjnafl s hsjdwj fgjesdwewfl, esak kwk usesjsvwk dw ljgmnsawfl twsmugmh egafk vjgdw vwhmak im'ad fw lgjvsal hdmk dwk eglk ».

7/ Pensez-vous que cette méthode de codage de messages secrets est sûre et que Alice et Bob peuvent être rassurés ?

3ème méthode – La méthode par décalage multiplicatif

A présent, Alice note le rang dans l'alphabet de chaque lettre du message secret, puis multiplie ce rang par la clé secrète.

Par exemple, si la clé secrète est + 3 et s'il veut envoyer la lettre B à Bob, il fera le produit 2x3=6 car B est la seconde lettre de l'alphabet, et enverra à Bob la lettre placée au 6ème rang, c'est-à-dire la lettre F.

1/ Que devient la lettre F si Alice a utilisé une clé égale à 3 ? Que devient MATH EN JEANS avec une clé de 5 ?

2/ Comment procède-t-on pour envoyer lettre Z avec une clé de 639 ? Pour la lettre R avec une clé de 44 678 ?

3/ Alice veut envoyer un message (en français ou en allemand) en utilisant une clé de 9. Imaginez puis codez ce message.

4/ Dressez un tableau à double entrée facilitant le décodage des messages secrets. Combien de clés secrètes existe-t-il ?

5/ Si un message est codé avec une clé secrète égale à $\times$ n, peut-on toujours le décoder ? Si oui, dans quels cas ? et comment ?

6/ Pensez-vous que cette méthode de codage de messages secrets est sûre et que Alice et Bob peuvent être rassurés ?

Pensez-vous que Jules César utilisait aussi
la méthode par décalage multiplicatif ?

4ème méthode – La méthode de Viginère *(inventée à la fin du Moyen-Âge)*

Alice et Bob ont souhaité améliorer la fiabilité de leur système de codage. Ils ont donc décidé d'utiliser le procédé de Blaise de Vigenère. Mais qui est Blaise de Vigenère ?

Cette fois-ci la clé secrète est un mot ou un texte entier, auquel on associe une série de nombres en tenant compte de la place dans l'alphabet de chacun des lettres de la clé.

Par exemple, si la clé est MATH EN JEANS, alors on associe la série (13;1 ;20 ;8;5 ;14;10 ;5 ;1 ;14;19).

A présent, si Alice veut coder MESSAGE SECRET avec la clé MATH EN JEANS, il procèdera ainsi : il décalera la lettre M de 13 rangs, la lettre E de 1 rang, le premier S de 20 rangs, le second reste de 8 rangs, le A de 5

rangs, le G de 14 rangs, le second E de 10 rangs, le troisième S de 5 rangs, le troisième E d'un seul rang, le C de 14 rangs, le R de 19 rangs. A votre avis, de combien de rangs va-t-on décaler la lettre T ? Utilisez le tableau élaboré lors de l'étude de la méthode 2 pour coder MESSAGE SECRET.

1/ Alice veut envoyer un message à Bob. Il commence donc par choisir une clé. Inventez cette clé, imaginez le message d'Alice (en français ou en allemand) puis codez ce message.

2/ Alice a envoyé un second message à Bob. Malheureusement, son ami a oublié la clé secrète. Croyez-vous qu'il sera possible de retrouver la clé ?

Alice : « Vm ybfvu owv atrf vh kmvfh zld xxhscing b f'neqjaf. E'ov snuoavg oxlfof, ny fnjzo yxhkicwf ey kfisn uvgmze, tc kzzs zh'jf athscjzo yxhu fm yrnjb dvnb… n m'yvarsm. Mrix un som, qrt anen q'nijninron. Rcn fenjyvy cfoa uz qdv duz nyt hn jvajvfhb unt kd'zg xxhscing b f'neqjaf. « Iy, zjtblmvu hn picms ! Vm h'j gvx u'njl ktznimv », ynbnjyvy-vmm neown rvr. Tj picne i'jlbvning qub czx arnuzvhfm. Rc n'jw zpkcfvu. Jxlm qdv, tycq ppgykvnc fph zjif fn ggzb spo : ljifhri xmjzqcws qf jjkdsb n sicqrunnj. Dq b'ronzfvourk otdf mya obvlb, gvyrabhb, unucwriy ng qubnabhc vihxef. Kcjyronj njvnjhmx cmob kvwm, nvr kmnnjrfisjgt xc rboxn uz ujgjha f epouvoynf, my kmvfh yrmyrpjji f gpocvn qnf dicwffm. Jl bwjae ybtaoyvviy mh qojqvd yc uzx bcplbnst, cu izrybsni qrt yyizzert xm avuybjz, gjguuvy n qfjkz hxhuozj yfm jlownf dbircjiwj. Kjafphvj a'bpjzo jwpplm wrbfrjz zwr uytqr qyawjwvnowm. Jg divdz xr pfn mccmirk ij ur tonkvturk kfb, y'fnzfahy lydjw efgxteuu nenzrgf fmx rqlnlqjb q'fhlzebhlv. Dq br qugf zfgn cz hdypn lj tbawvm qnf divhbvlb uz xjhum l'totnjtgjb. P'fning jhlijdjomy, ntencmrwqn ! Qfm iizjljkzzaf qizyrsywk gj lujyv xhs fj ggzb ubobj zbllyz id cpxqzz. Ph uld rrg fhazvuy dez jwbsgm rreurcgj jhuicw qv wxl, ntdf mya fcqfjlynbffgmsgt x'dez kxhmy ms qffriz. Vdrm mchpfm ! Uv xmrro ybfvu udo vsprt. « W'mxg fhlfmj vvfof vhf xjen rxa sydj », cfhbr-o-nu.»

4/ Pensez-vous que cette méthode de codage de messages secrets est sûre et que Alice et Bob peuvent être rassurés ?