SOLUTION DE L'EXERCICE NUMERO 5

Observons les premier, deuxième et troisième messages :

I - Un message N° 17 « de 1ère division à Q.G. » le 4 décembre à 16.00.
II - Un message N° 114 « de Q. G. à 1ère division » le 4 décembre à 16.45.
III - Un message N° 17 « de 1ère division à Q.G. » le 4 décembre à 17.10.

Ceci est un cas type qui fait le bonheur des décrypteurs : on remarque que les premier et troisième messages ont même origine, même numéro et même longueur. Le deuxième message est très court et adressé à l'expéditeur du premier message. On peut en déduire que, très probablement, il informe son correspondant que son message est indéchiffrable.

Examinons le deuxième message :

N° 17 – 16.45
ZVII4 AEFGF EITIB LODRN HMSEA ECRVE S

S'agissant d'une transposition, ce cryptogramme est l'anagramme du texte clair. On peut écarter le premier groupe ZVII4, qui est manifestement un groupe-clé. La présence de deux F et d'un B confirme l'hypothèse du mot « indéchiffrable ». Si on retire ces lettres du cryptogramme, il reste : G, T, O, M, S, E, A, E, R, V, E, S. Dans ces lettres, il me paraît aisé d'isoler le mot « message ». Il ne reste plus alors que les lettres T, O, R, V, E., qui donne le mot « votre ». Le texte clair est donc « votre message indéchiffrable ».

Juxtaposons maintenant une suite numérique ordonnée, le cryptogramme et le texte clair :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	E	F	G	F	E	I	T	I	B	L	O	D	R	N	H	M	S	E	A	E	C	R	V	E	S
v	o	t	r	e	m	e	s	s	a	g	e	i	n	d	e	c	h	i	f	f	r	a	b	l	e

Texte clair du deuxième message: « votre message indéchiffrable ».

Rappelons qu'au chiffrement les lettres du clair sont relevées dans l'ordre fourni par la clé. Donc le « v » clair se trouvait, au chiffrement, sous le nombre-clé 24. Le premier nombre de la clé est donc 24. Ce raisonnement est possible parce qu'il n'y a qu'un seul « v » dans le texte clair. Par contre, chacun des deux « f » du clair peut correspondre soit au nombre 3, soit au nombre 5. Compte tenu de ces observations, voyons si nous pouvons rétablir la clé au moins partiellement :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	E	F	G	F	E	I	T	I	B	L	O	D	R	N	H	M	S	E	A	E	C	R	V	E	S
v	o	t	r	e	m	e	s	s	a	g	e	i	n	d	e	c	h	i	f	f	r	a	b	l	e
24	12	8	14 23		17		18 26	18 26	1 20	4		7 9	15	13		22	16	7 9	3 5	3 5	14 23	1 20	10	11	

On voit que, pour un certain nombre de lettres, on a deux nombres clés possibles. Pour les « e », on en aurait cinq, c'est pourquoi je ne les ai pas marqués.

Intéressons -nous maintenant aux quatrième et cinquième messages. On observe qu'ils ont le même groupe clé que le deuxième message (ZVII4) et comme ils ont la même grandeur, toutes les données déjà acquises pour leur clé commune sont valables pour eux. Voyons d'abord le quatrième message.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
F	T	E	N	R	M	T	M	T	O	R	E	M	A	A	N	D	S	O	I	S	E	N	D	N	N
24	12	8	14 23		17		18 26	18 26	1 20	4		7 9	15	13		22	16	7 9	3 5	3 5	14 23	1 20	10	11	
d	e	m	a n		d		s n	s n	f i	n		t	a	m		e	n	t	e r	e r	a n	f i	o	r	

Dans la colonne de rang 4, le « a » s'impose (demand...), ce qui ne laisse plus que le « n » dans la colonne de rang 22, et, grâce à ce n, on peut lire (colonnes de rangs 21 à 25 : « enfor », ce qui suggère évidemment le mot « renfort », ce qui permet de préciser la clé pour les colonnes de rang 20 à 23, par voie de conséquence, pour la colonne de rang 10 (par élimination du « f ».

Faisons le point :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
F	T	E	N	R	M	T	M	T	O	R	E	M	A	A	N	D	S	O	I	S	E	N	D	N	N
24	12	8	14	16 25	17				20	4		7 9	15	13		22	12 5	7 9	5	3	23	1	10	11	2
d	e	m	a	n	d		s n	s n	i	n		t	a	m		e	n	t	r	e	n	f	o	r	t

Nous allons maintenant utiliser cette clé fortement améliorée pour attaquer le cinquième cryptogramme :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
U	E	E	D	E	E	U	O	S	I	S	T	R	C	P	Q	G	N	R	A	E	S	P	S	K	E
24	12	8	14	16 25	17		18 26	18 26	20	4		7 9	15	13		22	16 25	7 9	5	3	23	1	10	11	2
s	t	o	c	q k	g		n e	n e	a	d		u s	p	r		s	q k	u s	e	e	p	u	i	s	e

Il est aisé de deviner le texte complet du **cinquième message** : « stock grenades presque épuisé ».Nous allons maintenant pouvoir reconstituer la clé numérique complète :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
U	E	E	D	E	E	U	O	S	I	S	T	R	C	P	Q	G	N	R	A	E	S	P	S	K	E
s	t	o	c	k	g	r	e	n	a	d	e	s	p	r	e	s	q	u	e	e	p	u	i	s	e
24	12	8	14	25	17	19	26	18	20	4	6 21	9	15	13	6 21	22	16	7	5	3	23	1	10	11	2

Il nous reste une ambiguïté pour les deux colonnes de rangs 12 et 16, mais nous pouvons la lever en nous reportant au quatrième message ci-dessus, où on peut voir que le 21 doit aller au rang 12 et, donc, le 6 au rang 16.

La clé étant complètement rétablie, nous terminons le déchiffrement du quatriéme message.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
F	T	E	N	R	M	T	M	T	O	R	E	M	A	A	N	D	S	O	I	S	E	N	D	N	N
24	12	8	14	25	17	19	26	18	20	4	21	9	15	13	6	22	16	7	5	3	23	1	10	11	2
d	e	m	a	n	d	o	n	s	i	n	s	t	a	m	m	e	n	t	r	e	n	f	o	r	t

Texte clair du quatrième message : « Demandons instamment renfort ».

RECHERCHE DE LA CLE LITTERALE

Nous allons rechercher maintenant la clé littérale. Le processus a déjà été expliqué. Indiquons cependant que pour ne pas nous perdre dans des colonnes trop longues, nous utiliserons **surtout** les lettres fréquentes, sans toutefois perdre de vue qu'une clé littérale comporte d'autres lettres que les lettres fréquentes.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
24	12	8	14	25	17	19	26	18	20	4	21	9	15	13	6	22	16	7	5	3	23	1	10	11	2
T	N	L	O	T	R	S	T	R	S	E	S	L	O	N	I	S	O	I	E	B	S	A	L	L	A
U	O	N	R	U	S	T	U	S	T	F	T	N	R	O	L	T	R	L	F	C	T		N	N	
																				D					

Ici, on entre pleinement dans le domaine des hypothèses (quand une hypothèse mène à une impasse, on l'abandonne et on en prend une autre !).

Je vais retenir :

- pour les colonnes de rang 1 et 2 : UN
- pour les colonnes de rang 10, 11 et 12 : SES
- pour les colonnes de rang 23, 24, 25, et 26 : ALLA

En appliquant ces hypothèses, je vais pouvoir affiner le tableau :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
24	12	8	14	25	17	19	26	18	20	4	21	9	15	13	6	22	16	7	5	3	23	1	10	11	2
U	N	L	O	U	R	S	U	R	S	E	S	L	O	N	I	S	O	I	E	B	S	A	L	L	A
		N		V			V							O	L	T	R	L	F	C	T				
																				D					

On peut deviner « sur ses longs », ce qui devrait rappeler des souvenirs à tous ceux à qui on a fait ânonner les fables de La Fontaine en C.M. 2. On peut deviner ainsi la clé complète « Un jour sur ses longs pieds alla... ».

Reste maintenant à trouver quel rapport il y a entre cette clé et le groupe -clé « ZVII4 ».

Pour en savoir plus, on se reporte au site internet « Toutes les fables de Jean de La Fontaine » et on cherche le titre « Le héron ». On apprend ainsi que « Le héron » est la fable « **4** » du livre « **VII** ».

La clé est donc composée du numéro du livre (en chiffres romains) suivi du numéro de la fable (en chiffres arabes), le tout précédé d'un ou plusieurs « Z » pour compléter le groupe à cinq caractères.

Avec ces indications on devrait pouvoir déchiffrer (et non pas décrypter) le troisième message (rappelons que le premier message est indéchiffrable).

En consultant le même site internet, le groupe clé « (ZZZI2)I, nous indique que la fable est la fable numéro 2 du livre I (Le corbeau et le renard).

DECHIFFREMENT DU MESSAGE NUMERO III.

Le message comporte 79 lettres.

					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
					M	A	I	T	R	E	C	O	R	B	E	A	U	S	U	R	U	N	A	R	B	R	E
					42	1	36	71	57	19	13	51	58	10	20	2	75	69	76	59	77	45	3	60	11	61	21
Z	Z	Z	I	2	E	B	O	I	D	P	U	R	L	M	A	T	S	E	O	E	M	N	I	E	C	U	E
					l	e	t	r	o	i	s	i	e	m	e	b	a	t	a	i	l	l	o	n	a	o	c

24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
P	E	R	C	H	E	T	E	N	A	I	T	E	N	S	O	N	B	E	C	U	N	F	R	O	M	A	G
55	22	62	14	34	23	72	24	46	4	37	73	25	47	70	52	48	12	26	15	78	49	32	63	53	43	5	33
A	A	R	U	E	D	Z	S	C	E	C	S	T	N	E	S	E	S	L	T	X	L	T	C	E	S	E	I
c	u	p	e	c	e	m	a	t	i	n	l	a	c	o	t	e	t	r	o	i	s	c	e	n	t	d	e

52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
E	M	A	I	T	R	E	R	E	N	A	R	D	P	A	R	L	O	D	E	U	R	A	L	L	E	C	H
27	44	6	38	74	64	28	65	29	50	7	66	17	56	8	67	39	54	18	30	79	68	9	40	41	31	16	35
T	N	O	C	O	O	E	I	N	O	P	E	T	S	X	T	B	T	O	R	M	L	R	A	A	L	I	E
u	x	p	e	r	t	e	s	d	e	u	x	m	o	r	t	s	o	n	z	e	b	l	e	s	s	e	s

Texte clair du troisième message : « Le troisième bataillon a occupé ce matin la cote 302. Pertes : 2 morts, 11 blessés ».

.