Journée du lundi 13 mars 2017

Carré de Polybe – document de l'enseignant

Démarche

Objectifs

Se repérer dans un tableau en utilisant ou en élaborant des représentations pour résoudre des problèmes.

Principes

Les exercices sont basés sur le carré de Polybe. Ils sont de difficulté croissante : les niveaux 1 à 5 correspondent globalement aux 5 niveaux de classe de l'école élémentaire.

Déroulement :

- Des documents introducteurs à projeter, à lire ou faire lire permettent de situer le contexte.
- Le codage du même mot –exemple « ECOLE » est donné pour chaque niveau.
- Une activité de décodage collective est proposée au départ en phase d'entraînement.
- L'activité de décodage et l'activité de codage peuvent ensuite être menées individuellement ou en groupes.

Remarque

Les réponses attendues par les élèves sont grisées.

Carré de Polybe

Polybe

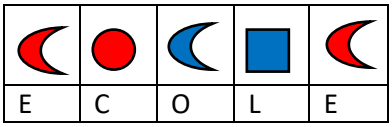
Le carré de Polybe consiste à remplacer chaque lettre par les coordonnées de sa position dans une grille, souvent carrée.
Ce système de codage, appelé aussi système de chiffrement peut être rendu encore plus compliqué en lui ajoutant un mot de passe qui permet de remplir la grille avec un alphabet désordonné.
On suppose que cette manière de coder été inventée par *Polybe*, historien grec, qui a vécu au deuxième siècle avant Jésus Christ.

Pour indiquer une lettre, on doit indiquer dans quelle colonne elle se trouve, puis dans quelle ligne. On obtient un couple de points qui indique la case dans laquelle la lettre est rangée.

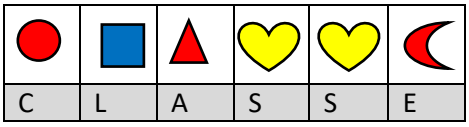
Niveau 1 – Enoncés avec les couleurs

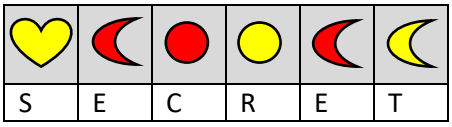
	△	□	○	♡	☾
	A	B	C	D	E
	F	G	H	I	J
	K	L	M	N	O
	P	Q	R	S	T
	U	V	X	Y	Z

Exemple :

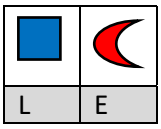


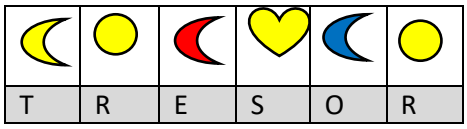
Entraine-toi :

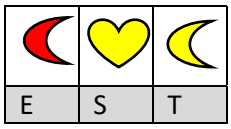


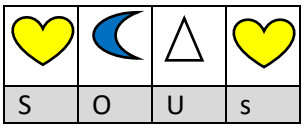


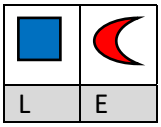
Décode le message secret et réponds à la question : Où est le trésor ?

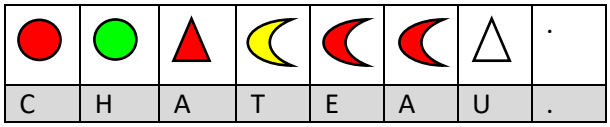




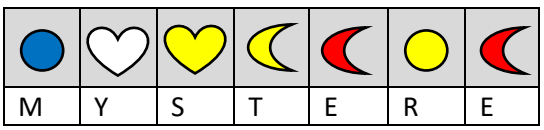








Ecris le message secret :



Niveau 1 – Enoncés avec le nom des couleurs (pour impression ou photocopie noir et blanc)

					
rouge	A	B	C	D	E
vert	F	G	H	I	J
bleu	K	L	M	N	O
jaune	P	Q	R	S	T
blanc	U	V	X	Y	Z

Exemple :

 rouge	 rouge	 bleu	 bleu	 rouge
E	C	O	L	E

Entraine-toi :

 rouge	 bleu	 rouge	 jaune	 jaune	 rouge
C	L	A	S	S	E

 jaune	 rouge	 rouge	 jaune	 rouge	 jaune
S	E	C	R	E	T

Décode le message secret et réponds à la question : Où est le trésor ?

 bleu	 rouge
L	E

 jaune	 jaune	 rouge	 jaune	 bleu	 jaune
T	R	E	S	O	R

 rouge	 jaune	 jaune
E	S	T

 jaune	 bleu		 jaune
S	O	U	S

 bleu	 rouge
L	E

 rouge	 vert	rouge	jaune	rouge	rouge	blanc	
C	H	A	T	E	A	U	.

Ecris le message secret :

bleu	blanc	jaune	jaune	rouge	jaune	rouge
M	Y	S	T	E	R	E

Niveau 2 – Enoncé

	△	□	○	♡	☾
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	X	Y	Z

Exemple :

☾ 1	○ 1	☾ 3	□ 3	☾ 1
E	C	O	L	E

Entraine-toi :

□ 1	☾ 3	♡ 3	☾ 2	☾ 3	△ 5	○ 4
B	O	N	J	O	U	R

♡ 4	☾ 1	○ 3	△ 1	♡ 2	♡ 3	☾ 1
S	E	M	A	I	N	E

Décode le message secret et réponds à la question : Où est le trésor ?

□3	☾1
L	E

☾4	○4	☾1	♡4	☾	○ 4
T	R	E	S	O	R

☾ 1	♡ 4	☾ 4
E	S	T

♡1	△ 1	♡3	♡4
D	A	N	S

□ 3	☾1
L	E

○ 1	△ 5	□ 1	☾ 1	
C	U	B	E	.

Ecris le message secret :

○ 1	☾ 3	♡ 1	☾ 1
C	O	D	E

♡ 4	☾ 1	○ 1	○ 4	☾ 1	☾ 4
S	E	C	R	E	T

Niveau 3 – Enoncé

1. Documents introducteurs

a. Les chiffres romains

D'après http://www.mathematiquesfaciles.com/nombres-chiffres-romains_2_37194.htm

- Avant l'introduction des chiffres arabes, qui remonte à la fin du Xème siècle, les Romains employaient les sept lettres suivantes, dites 'chiffres romains'.

I	V	X	L	C	D	M
1	5	10	50	100	500	1000

- On a conservé l'usage des chiffres romains pour marquer les heures sur les cadrans d'horloge, pour numéroter les chapitres des livres, les siècles (XXème siècle = 20ème siècle).
  On les utilise obligatoirement pour les rois de France et les empereurs : Louis XVI, Napoléon III ...

- La numérotation romaine est soumise aux règles suivantes :

1. Les lettres, placées à la droite d'une autre, ajoutent leur valeur à celle de cette lettre si les valeurs sont égales.
   II = 1 + 1 = 2 - XXX = 10 + 10 + 10 = 30

2. Toute lettre, placée à la droite d'une autre plus forte, ajoute sa valeur à celle de cette lettre.
   VI = 5 + 1 = 6 - XV = 10 + 5 = 15

3. Toute lettre, placée à la gauche d'une autre plus forte, retranche sa valeur de cette lettre.
   IV = 5 - 1 = 4 - IX = 10 - 1 = 9

b. Veni, vidi, vici

D'après https://fr.wikipedia.org/wiki/Veni,_vidi,_vici

Veni, vidi, vici est une expression latine.
Le latin est une langue, parlée autrefois par les Romains.
Le latin a donné naissance aux langues suivantes : français, italien, espagnol, portugais, roumain

Cette expression a été employée par Jules César en 47 av. J-C à la suite d'une rapide victoire militaire. Elle peut être traduite en français par « je suis venu, j'ai vu, j'ai vaincu »1. Cette expression très courte est devenue célèbre. On l'utilise pour parler d'un succès très rapide.

c. Vercingétorix et Jules César

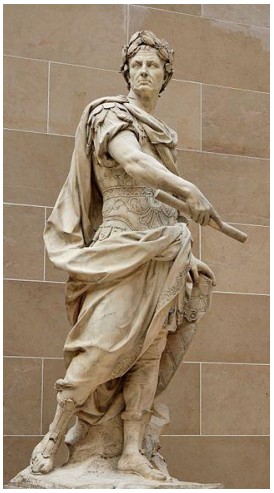
Vercingétorix

D'après https://fr.vikidia.org/wiki/Vercing%C3%A9torix

Vercingétorix est le plus connu des chefs gaulois. Il est né en 72 av. J.-C. en Auvergne et mort en 46 av. J.-C. à Rome. Il est un des chefs de la résistance des Gaulois contre la conquête de la Gaule par **Jules César**.

Vercingétorix bat César à Gergovie en 52 av. J.-C., mais il est ensuite battu et fait prisonnier à Alésia la même année. Il est devenu connu car en se rendant, il a sauvé des vies de son peuple.

Cependant, on sait très peu de chose sur lui, parce que les seuls textes qui en parlent sont écrits par des Romains.
Jules César a fait le portrait de son adversaire dans son récit de l'invasion des Gaules, appelé Commentaires sur la Guerre des Gaules



Jules César

Enoncé

	1	2	3	4	5
I	A	B	C	D	E
II	F	G	H	I	J
III	K	L	M	N	O
IV	P	Q	R	S	T
V	U	V	X	Y	Z

Exemple :

5I	3I	5III	2III	5I
E	C	O	L	E

Entraine-toi :

3IV	5III	3III	1I	4II	4III
R	O	M	A	I	N

2II	1I	1V	2III	5III	4II	4IV
G	A	U	L	O	I	S

Décode le message secret et réponds à la question : Qui a prononcé ces paroles ?

3I	5I	4IV	1I	3IV
C	E	S	A	R

1I
A

4I	4II	5IV	:
D	I	T	:

2V	5I	4III	4II
V	E	N	I

2V	4II	4 I	4II
V	I	D	I

2V	4II	3 I	4II
V	I	C	I

Ecris le message :

2V	5I	3IV	3I	4II	4III	2II	5I	5IV	5III	3IV	4II	3V
V	E	R	C	I	N	G	E	T	O	R	I	X

Niveau 4 – Enoncé

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	X	Y	Z

Exemple :

51	31	53	29	51
E	C	O	L	E

Entraine-toi :

33	51	44	44	11	22	51
M	E	S	S	A	G	E

12	15	42	54	51
F	U	I	T	E

Décode le message secret et réponds à la question : Où l'espion a-t-il trouvé refuge ?

29		51	44	14	42	53	43		44	51		31	11	31	32	51
L	'	E	S	P	I	O	N		S	E		C	A	C	H	E

11	15		14	53	34	54		41	15		11	11	25	34	51
A	U		P	O	R	T		D	U		H	A	V	R	E

Exercice 2 : codage

41	51	31	32	42	12	12	34	11	22	51
D	E	C	H	I	F	F	R	A	G	E

Niveau 5 – Enoncé

Textes introducteurs

Enigma

« Enigma » est une machine électromécanique portable d'origine allemande, ressemblant à une machine à écrire, destinée au chiffrement, souvent appelé "cryptage", et au déchiffrement des messages secrets commerciaux, diplomatiques ou militaires, en usage de 1920 à 1945.

Machine de chiffrement **« Enigma » à quatre rotors**. On distingue : le clavier, les lampes qui donnent le résultat du message crypté ou décrypté, et les rotors.

Historique

La machine Enigma a été commercialisée en Europe et dans le reste du monde dès le début des années 1920. Puis elle a été adaptée et complexifiée pour les besoins militaires et diplomatiques.

Son utilisation la plus célèbre a été celle de l'Allemagne nazie, pendant la Seconde Guerre mondiale.

Carré de Polybe avec clé de cryptage

On choisit une clé, on écrit toutes les lettres de cette clef qui ne sont pas en double dans le « mot-clé »choisi, puis on écrit, le reste de l'alphabet dans l'ordre. On fait bien attention à ne pas écrire les lettres qui sont dans le « mot-clé ». On ne place pas la lettre « W », qui n'est pas très utilisée en français.
L'alphabet est ainsi désordonné et cela rend encore plus difficile le décodage pour une personne qui intercepte le message.

	1	2	3	4	5
1	M	A	T	H	E
2	I	Q	U	S	B
3	C	D	F	G	J
4	K	L	N	O	P
5	R	V	X	Y	Z

La clé choisie ici est
« MATHEMATIQUES »

Construis la table de cryptage avec la clé « MESSAGE »

	1	2	3	4	5
1	M	E	S	A	G
2	B	C	D	F	H
3	I	J	L	L	N
4	O	P	Q	R	T
5	U	V	X	Y	Z

Trouve le bon code du mot « ENIGME »

21	53	13	15	11	21

21	53	13	51	11	21

12	35	31	15	11	12

Décode le message secret et réponds à la question : Qui a permis de déchiffrer les messages nazis pendant la deuxième guerre mondiale ?

51	44	41	22	21
G	R	A	C	E

41
A

41	33	41	13	53
A	L	A	I	N

54	15	44	13	53	51
T	U	R	I	N	G

33	21	31
L	E	S

41	33	33	13	21	31
A	L	L	I	E	S

14	53	54
O	N	T

44	21	15	31	31	13
R	E	U	S	S	I

41
A

32	21	22	52	13	42	42	44	21	44
D	E	C	H	I	F	F	R	E	R

33	21
L	E

22	14	32	21
C	O	D	E

53	41	55	13	
N	A	Z	I	.

Exercice 4 : coder le message « cryptographie »

22	44	45	24	54	14	51	44	41	24	52	13	21
C	R	Y	P	T	O	G	R	A	P	H	I	E

Annexes

- Annexe 1 : Carré de Polybe (tous niveaux)
- Annexe 2 : « Veni vidi vici » / la guerre des Gaules (niveau 3)
- Annexe 3 : La machine Enigma (niveau 5)

Annexe 1 : le carré de Polybe

Carré de Polybe

Polybe

Le carré de Polybe consiste à remplacer chaque lettre par les coordonnées de sa position dans une grille, souvent carrée.
Ce système de codage, appelé aussi système de chiffrement peut être rendu encore plus compliqué en lui ajoutant un mot de passe qui permet de remplir la grille avec un alphabet désordonné.
On suppose que cette manière de coder été inventée par *Polybe*, historien grec, qui a vécu au deuxième siècle avant Jésus Christ.

Pour indiquer une lettre, on doit indiquer dans quelle colonne elle se trouve, puis dans quelle ligne. On obtient un couple de points qui indique la case dans laquelle la lettre est rangée.

Annexe 2 : Niveau 3 – « veni vidi vici » / Guerre des Gaules

Les chiffres romains

D'après http://www.mathematiquesfaciles.com/nombres-chiffres-romains_2_37194.htm

- Avant l'introduction des chiffres arabes, qui remonte à la fin du Xème siècle, les Romains employaient les sept lettres suivantes, dites 'chiffres romains'.

I	V	X	L	C	D	M
1	5	10	50	100	500	1000

- On a conservé l'usage des chiffres romains pour marquer les heures sur les cadrans d'horloge, pour numéroter les chapitres des livres, les siècles (XXème siècle = 20ème siècle).
  On les utilise obligatoirement pour les rois de France et les empereurs : Louis XVI, Napoléon III ...

- La numérotation romaine est soumise aux règles suivantes :

1. Les lettres, placées à la droite d'une autre, ajoutent leur valeur à celle de cette lettre si les valeurs sont égales. II = 1 + 1 = 2 - XXX = 10 + 10 + 10 = 30

2. Toute lettre, placée à la droite d'une autre plus forte, ajoute sa valeur à celle de cette lettre.
   VI = 5 + 1 = 6 - XV = 10 + 5 = 15

1. Toute lettre, placée à la gauche d'une autre plus forte, retranche sa valeur de cette lettre.
   IV = 5 - 1 = 4 - IX = 10 - 1 = 9

Veni, vidi, vici

D'après https://fr.wikipedia.org/wiki/Veni,_vidi,_vici

Veni, vidi, vici est une expression latine.
Le latin est une langue, parlée autrefois par les Romains.
Le latin a donné naissance aux langues suivantes : français, italien, espagnol, portugais, roumain

Cette expression a été employée par Jules César en 47 av. J-C à la suite d'une rapide victoire militaire. Elle peut être traduite en français par « je suis venu, j'ai vu, j'ai vaincu »1. Cette expression très courte est devenue célèbre. On l'utilise pour parler d'un succès très rapide.

Vercingétorix et Jules César

Vercingétorix

D'après https://fr.vikidia.org/wiki/Vercing%C3%A9torix

Vercingétorix est le plus connu des chefs gaulois. Il est né en 72 av. J.-C. en Auvergne et mort en 46 av. J.-C. à Rome. Il est un des chefs de la résistance des Gaulois contre la conquête de la Gaule par **Jules César**.

Vercingétorix bat César à Gergovie en 52 av. J.-C., mais il est ensuite battu et fait prisonnier à Alésia la même année. Il est devenu connu car en se rendant, il a sauvé des vies de son peuple.

Cependant, on sait très peu de chose sur lui, parce que les seuls textes qui en parlent sont écrits par des Romains.
Jules César a fait le portrait de son adversaire dans son récit de l'invasion des Gaules, appelé Commentaires sur la Guerre des Gaules

Jules César

Annexe 3 : machine Enigma

Enigma

« Enigma » est une machine électromécanique portable d'origine allemande, ressemblant à une machine à écrire, destinée au chiffrement, souvent appelé "cryptage", et au déchiffrement des messages secrets commerciaux, diplomatiques ou militaires, en usage de 1920 à 1945.

Machine de chiffrement **« Enigma » à quatre rotors**. On distingue : le clavier, les lampes qui donnent le résultat du message crypté ou décrypté, et les rotors.

Historique

La machine Enigma a été commercialisée en Europe et dans le reste du monde dès le début des années 1920. Puis elle a été adaptée et complexifiée pour les besoins militaires et diplomatiques.

Son utilisation la plus célèbre a été celle de l'Allemagne nazie, pendant la Seconde Guerre mondiale.