

# OMNIA PER OMNIA

N'importe quoi peut signifier n'importe quoi



Courtesy of the George C. Marshall Foundation, Lexington, Virginia.

## Au sujet du code bilitère de Bacon et du rôle indirect de Shakespeare dans l'histoire de la cryptographie.

La photo de groupe en accroche de cet article est en réalité un message codé. Regardez mieux les personnages : certains regardent devant eux et d'autres de côté.

Pour le comprendre, attendons un peu... et intéressons-nous d'abord à Sir Francis Bacon, philosophe, homme politique et homme de science de l'époque élisabéthaine, qui créa une méthode **stéganographique** révolutionnaire pour l'époque.

Il décida de coder chaque lettre de l'alphabet, 24 lettres à l'époque ( I et J étant confondus, de même que U et V) avec une suite de 5 lettres, soit *a* soit *b*. Ce qui donne :

A = aaaaa	I/J = abaaa	R = baaaa
B = aaaab	K = abaab	S = baaab
C = aaaba	L = ababa	T = baaba
D = aaabb	M = ababb	U/V = baabb
E = aabaa	N = abbaa	W = babaa
F = aabab	O = abbab	X = babab
G = aabba	P = abbba	Y = babba
H = aabbb	Q = abbbb	Z = babbb

Il appela sa méthode "alphabet bilitère". Aujourd'hui on dirait "binaire" (remplacez a et b par 0 et 1 et vous verrez !).

Cette méthode a un intérêt majeur, qui est la manière dont on peut l'utiliser. En effet, les *a* et les *b* ne sont pas écrits "en l'état" mais peuvent être représentés par à peu près n'importe quoi (d'où le titre de cet article).

Je m'explique : pour aller vite, prenons un mot très court, par exemple "va".

La méthode bilitère "brute" donne : baabb aaaa (donc un message qui "sent son code" à plein nez).

Mais si maintenant on camoufle ce code dans n'importe quelle phrase (de la bonne longueur de préférence, soit ici 10 caractères), dont les *a* sont (par exemple) des minuscules, et les *b* des capitales, cela donnera :

J'aiME le riz ou bien BonJOur, toi !

On peut, de même, décider que les *a* et les *b* seront représentés par deux polices de caractères différentes, ce qui pourrait donner, avec les mêmes phrases :

*J'aime le riz* ou bien **Bonjour**, toi !

Mais pourquoi se limiter à des lettres ? Le système permet en effet toutes les déclinaisons, puisque *a* et *b* peuvent prendre n'importe quelle forme : des traits courts ou longs, des carrés de deux couleurs distinctes, des cercles et des triangles, des pommes et des poires, ou -pour revenir à notre photo - des personnages regardant soit devant eux soit de côté !

Bref, du moment qu'on choisit deux types de représentations, une pour *a* et une pour *b*, on peut exprimer ce qu'on veut avec n'importe quoi !

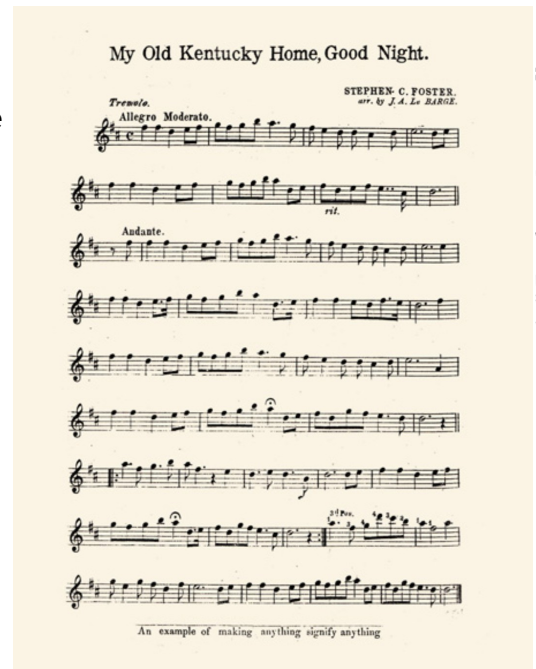
C'est en tout cas la théorie développée par Bacon (qu'il exprime dans la phrase "*Omnia per omnia*", reprise en exergue de cet article), puis étudiée et enrichie par William et Elizebeth Sherman au XX<sup>e</sup> siècle.

Les illustrations de cette page sont extraites des publications de William Shermann.

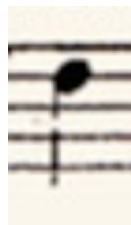
### Exemple 1.

Si on remarque les petites coupures sur les hampes de certaines notes (voir gros plan), on voit qu'avec une vraie partition on peut faire passer un message.

Pour les curieux, le texte (facilement mais longuement) décodé est "*Enemy advancing right / We march at daybreak.*"



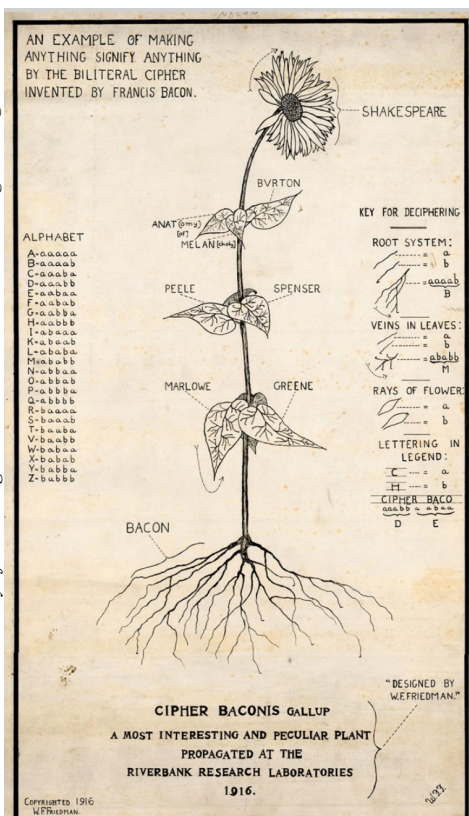
Courtesy of the George C. Marshall Foundation, Lexington, Virginia.



### Exemple 2.

Par contre, le déchiffrement de cette planche (présentée par Friedman comme un exemple des possibles), est nettement plus coriace, même avec les explications à côté !

Mais l'auteur travaillait pour la sécurité de son pays, donc le niveau de difficulté attendu n'avait rien à voir avec ce que nous recherchons pour nos élèves.



Courtesy of the George C. Marshall Foundation, Lexington, Virginia.



William et Elizebeth Friedman furent de célèbres cryptographes, de la première guerre mondiale aux années 60 (et même toute leur vie durant). Leur histoire avec la cryptographie commença de manière assez inattendue.

Elizebeth (avec un e), spécialiste de l'œuvre de Shakespeare, fut embauchée dans le laboratoire de recherche privé de Riverbank, financé par un milliardaire excentrique. Celui-ci voulait trouver la preuve que Francis Bacon était le véritable auteur des pièces de Shakespeare, en y découvrant les hypothétiques messages secrets que le véritable auteur y aurait caché (cette rumeur court d'ailleurs toujours). Voilà pourquoi le code de Bacon est également appelé "le code shakespearien".

À cause du travail qu'elle devait accomplir, Elizebeth s'éloigna de plus en plus de la littérature pour devenir une spécialiste des codes secrets et consacrer sa vie à cette discipline.

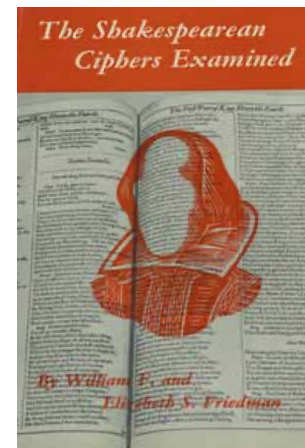
Quant à William, il fut embauché après ses études de biologie pour prendre en charge le département de génétique de Riverbank. Mais une fois sur place il s'intéressa davantage à Elizebeth - qui l'initia à la cryptographie - qu'à la biologie. Il abandonna donc rapidement son poste pour rejoindre sa future épouse dans le même département, où ils dirigèrent à partir de 1917 la première formation de cryptographes aux USA.



Courtesy of the George C. Marshall Foundation, Lexington, Virginia.

Ils furent ensuite tous deux à l'origine de nombreuses avancées en matière de cryptanalyse (un mot inventé par William Friedman) : leurs travaux permettront, entre autres, de démanteler de nombreux réseaux d'espionnage nazis et de casser un important code japonais.

Ils savaient aussi faire preuve d'humour : lorsqu'ils publièrent en 1957 la conclusion de leurs recherches sur le sujet qui les avait réunis trente ans plus tôt, ils y cachèrent malicieusement une phrase chiffrée en alphabet bilitère (évidemment!), qui disait : *I did not write the plays. F.Bacon* (traduction : *Je n'ai pas écrit les pièces. F.Bacon*).



Courtesy of the George C. Marshall Foundation, Lexington, Virginia.

Leur travail était aussi leur passion. Par exemple ils adoraient chiffrer les messages destinés à leurs proches, comme on peut le voir sur cette carte de vœux - déchiffrable grâce à la grille de Cardan fournie sur la gauche.





Leur dernier clin d'oeil fut réalisé par Elizebeth : devenue veuve, elle fit graver sur leur pierre tombale "Knowledge is power" (tirée d'un ouvrage de Bacon, et qu'on pourrait traduire par "la connaissance, c'est le pouvoir") avec deux polices différentes (oui, c'est subtil, je vous l'accorde).



**W**

**F**

**F**

Deux polices sont utilisées :

Une sans serif (comme la police Arial):

**KNOWLEDGE IS POWER** → les a

Une avec serif (= empattements) comme la police Times :

**KNOWLEDGE IS POWER** → les b

Elle a donc, grâce au code bilitère, caché dans leur phrase fétiche les initiales de son époux et collègue de toute une vie. Joli, non ?

"Et notre photo de groupe ?" direz-vous. Eh bien, une fois décodée, elle donne justement : KNOWLEDGE IS POWE (le R final est manquant, faute d'un nombre suffisant de personnages !). Vous y remarquerez William et Elizebeth, assis au premier rang, sur la gauche, au milieu de la promotion 1918 des jeunes officiers cryptanalyses formés par leurs soins. Le décodage de la photo est visible en annexe 2.

### Sources :

#### Sur Francis Bacon et le code bilitère :

<https://www.apprendre-en-ligne.net/crypto/stegano/bilitere.html>

[https://en.wikipedia.org/wiki/Bacon%27s\\_cipher](https://en.wikipedia.org/wiki/Bacon%27s_cipher)

[https://fr.wikipedia.org/wiki/Francis\\_Bacon\\_\(philosophe\)](https://fr.wikipedia.org/wiki/Francis_Bacon_(philosophe))

#### Sur les époux Friedman et leur rapport avec le code bilitère de Bacon :

<http://www.cabinetmagazine.org/issues/40/sherman.php> (excellent article qui m'a donné envie d'en savoir plus)

<https://youtu.be/9iqXOf8L72g> (conférence d'Elonka Dunin)

#### Sur William Friedman, document NSA des années 1970 (1)

[https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-spectrum/legendary\\_william\\_friedman.pdf](https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-spectrum/legendary_william_friedman.pdf)

#### Sur Elizebeth Friedman, articles de 2017 et 2018 (2)

<https://www.brainpickings.org/2018/09/06/the-woman-who-smashed-codes-elizabeth-friedman/>

<https://www.wired.com/story/world-war-2-codebreakers-elizabeth-smith-friedman/>

<https://dailygeekshow.com/elizabeth-friedman-espionnage-enigma-decryptage-nazis/>

(1) où on voit qu'Elizebeth est à peine mentionnée, tout juste comme une collaboratrice.

(2) où inversement le mari est quasiment passé sous silence.

## Concrètement, comment l'utiliser aujourd'hui ?

Après cette (longue) partie historique, venons-en à un aspect plus pratique : en quoi cette méthode peut être utilisée dans le cadre d'un escape game pédagogique ?

Il faut prendre déjà en compte l'inconvénient important de cette méthode, qui est sa longueur. Chaque lettre étant représentée par 5 signes, le texte codé sera 5 fois plus long que l'original, et les chiffrage/déchiffrage assez ingrats (et donc sujets à erreurs) s'ils s'éternisent trop. Il est donc raisonnable de l'utiliser pour le chiffrage d'un seul mot.

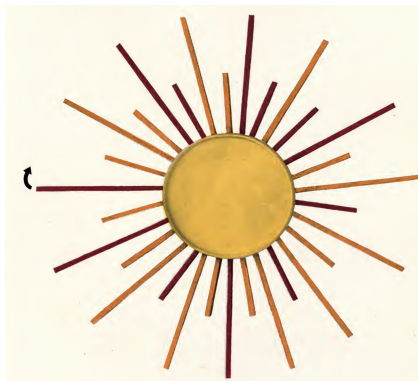
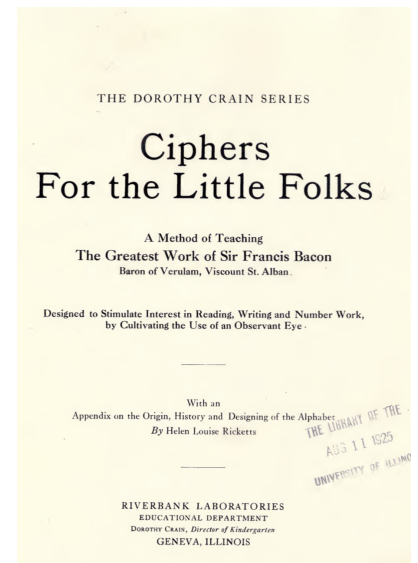
Mais elle a par contre un atout majeur : comme n'importe quoi peut signifier n'importe quoi, elle permet des codages qui dépassent le cadre de la phrase - aussi sibylline soit-elle.

J'ai trouvé une méthode complète, datant de 1916, pour apprendre aux enfants à manier ce langage.

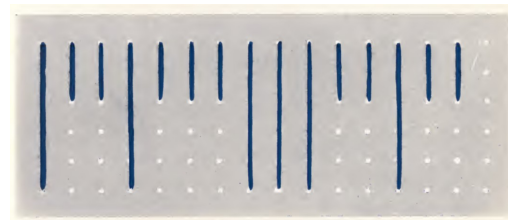
Je ne sais pas quelle en était la finalité ni si beaucoup d'élèves ont sué sur cette méthode (!), mais elle peut nous être précieuse aujourd'hui, et pas seulement comme objet de curiosité.

Dans ses exercices, elle propose en effet plusieurs motifs que nous pourrions réutiliser dans certains escape games.

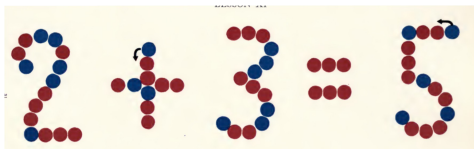
Je vous en livre quelques exemples ici.



A. Ici on lira les couleurs des rayons (jaune/ rouge) en suivant le sens indiqué par la flèche.



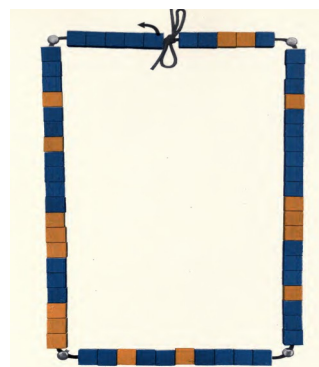
B. Avec du laçage (court/long), ça fonctionne aussi.



C. L'opération n'a évidemment ici aucune importance : seuls comptent les points rouges et bleus, et les flèches permettant de connaître le sens de lecture.



D. Même principe que précédemment.



E. Un collier avec des perles de deux couleurs.

Si on veut réaliser pareil objet, il faudra penser à y intégrer un élément indiquant le sens de lecture ainsi que le début du texte.

Cette méthode permet donc d'apporter une dimension nouvelle dans nos jeux en échappant au côté habituellement scriptural d'un code, puisqu'un mot peut être caché dans un dessin, une photo, une partition, ou même l'organisation d'objets réels.

On utilisera soit deux types d'objets (exemples 1 et 3), soit deux couleurs différentes (exemple 2), soit des objets à la nature identique mais présentés de façon différente (exemple 4) - ce qui nous ramène à nos soldats de la page 1.

Il faudra éviter de possibles confusions en choisissant soigneusement ses objets (ne pas mélanger formes et couleurs qui empêcheraient de comprendre clairement les codes a et b).

La clé de décryptage pourra être donnée sous forme de liste (telle qu'on la trouve le plus souvent) ou de tableau à double entrée (comme proposé page suivante), ce qui apporte un petit travail supplémentaire tout en clarifiant considérablement la mécanique.

Les aides naturelles :

1. Compter les objets permet de savoir combien de lettres comporte le mot (nombre d'objets /5).
2. Les a sont (la plupart du temps) plus nombreux que les b, ce qui aide à savoir "quoi est quoi".

La difficulté sera d'amener les élèves/joueurs à comprendre que ces images/objets ont un sens caché (ce codage ne me semble donc pas utilisable avant le niveau collège). On peut les aider avec un symbole commun sur le message codé et sur la clé de décryptage, qui permettra de faire le lien. Ou même proposer si nécessaire un "coup de pouce" de type "a=couché / b=debout" ou "a=pomme / b=poire".

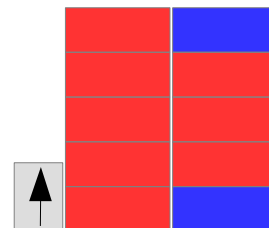
Voici quelques propositions de transpositions dans le "réel". À déchiffrer si vous le souhaitez !

En annexe 1 : des outils de codage/décodage.

En annexe 2 : les solutions.



Ex 1 : deux types d'objets (balles, cubes...) fixés dans un contenant.  
Attention: on n'est pas obligé de les aligner parfaitement mais leur position doit induire le sens de lecture sans confusion possible.



Ex 2 : couleurs. Avec des briques type Lego™ (il faudra indiquer le sens de lecture). Les piles de 5 caractères rendent le décodage plus simple (une pile par lettre).



Ex.3: avec deux types de pinces à linge sur un fil, ou tous objets pouvant être accrochés.



(Sinon, pour les perfectionnistes, ces petits oiseaux imprimables en 3D sont à télécharger sur [Cults](#) et à installer sur un tourillon de 15 mm de diamètre)



Ex.4: avec de vrais livres dans une bibliothèque (interdiction d'y toucher pour ne pas modifier le code!)

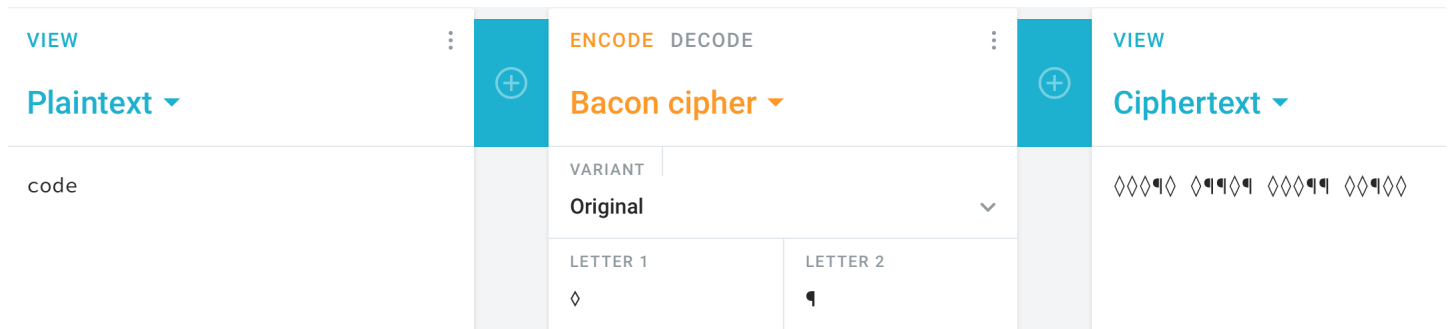
# ANNEXE 1 : CODEURS / DECODEURS

## 1. Pour coder/décoder automatiquement en ligne :

On peut trouver de nombreux codeurs/décodeurs en ligne du code de Bacon.

Mais je vous conseille ce site : <https://cryptii.com/pipes/bacon-cipher>. Son intérêt, par rapport aux autres, est qu'on peut remplacer les a et les b par deux caractères de son choix, du moment qu'ils sont accessibles avec le clavier (testez les combinaisons *Alt + lettre*, qui créent souvent des caractères assez originaux) et simplifie donc considérablement le codage puisqu'on n'a pas besoin de passer ensuite par une phase de transformation.

Exemple ici, où le mot "CODE" a été codé avec des  $\diamond$  (*alt+V*) et des ¶ (*alt+6*) :



Note : le codage installe par défaut une coupure entre les groupes de 5 caractères représentant chaque lettre, ce qui rend la lecture plus aisée. Vous pourrez bien sûr supprimer ces espaces par la suite, si vous souhaitez davantage de difficulté.

**2. Pour coder/décoder manuellement** (parce qu'on peut avoir envie de comprendre comment se font les choses), je vous ai préparé une table à double entrée, pour une meilleure compréhension de la mécanique du code. J'ai pu expérimenter, en créant les exemples pour cet article, combien cette table permettait de s'habituer au codage/décodage et devenir rapidement à l'aise avec.

En rouge : les 3 premières lettres. En bleu : les 2 dernières.

	aa	ab	ba	bb
aaa	A	B	C	D
aab	E	F	G	H
aba	I ou J	K	L	M
abb	N	O	P	Q
baa	R	S	T	U ou V
bab	W	X	Y	Z

Exemple avec une lettre : S = baaab

Exemple avec un mot : CHIC = aaaba aabbb abaaa aaaba



# ANNEXE 2 : SOLUTIONS

## Photo de groupe de la page 1:



Cette photo n'a jamais quitté W. Friedman : si vous regardez attentivement la photo de la page 3, vous verrez qu'elle est présente sous le verre de son bureau.

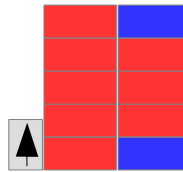
## Exercices de la page 5:

A (le soleil) : Sunset // B (le laçage): The // C (l'addition): United States  
 C (le chien) : Barking // E (le collier) : A cypher chain

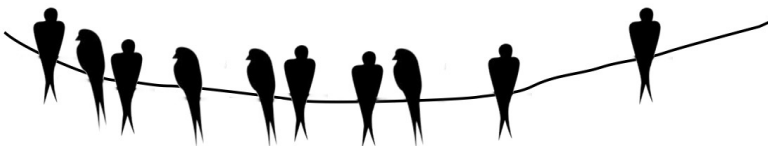
## Exemples de la page 6 :



Ex 1 : (pomme=a / orange=b)  
 aaaba                  aaaaa                  abbba  
**C**                                  **A**                                  **P**



Ex 2 : (Rouge=a / bleu=b)  
 aaaa                          baaab  
**A**                                  **S**



Ex 3 : ( =a / =b)  
 ababb                          aabaa  
**M**                                  **E**

Ex 4 : (livre vertical=a / livre couché=b)  
 aaaba    abbab                  aaabb                  aabaa  
**C**                  **O**                                  **D**                                  **E**



## Exemple proposé sur l'article de présentation :



(violet=a / rose=b)  
 ababb                          abaaa  
**M**                                  **I**



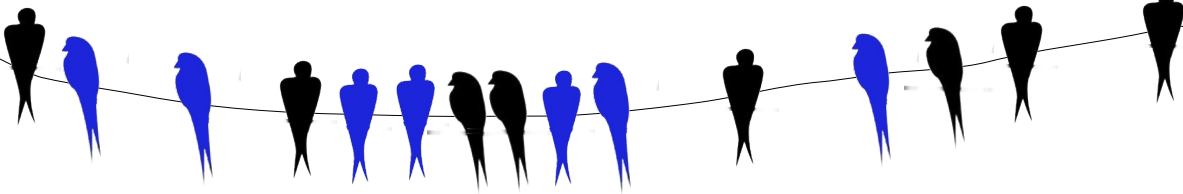
# ANNEXE 3 : PROLONGEMENTS

## 1. Vous avez un groupe de joueurs aguerris, toujours à la recherche de nouveaux défis ?

—► Essayez l'imbrication de deux mots au sein d'un même message.

Pour cela, rien de bien compliqué : il suffit de combiner deux modes de codage différents. Par exemple : forme pour le premier mot et couleur pour le deuxième.



*Besoin d'un petit visuel?*



## 2. Malgré la passion que l'auteure a mise dans cet article, vous restez allergique à l'alphabet bilitère de Francis Bacon?

—► Utilisez les mêmes méthodes stéganographiques, mais avec le code Morse.

*Les deux mots imbriqués : solution*

(  =a /  =b )		
abbaa	abbab	abbaa
<b>N</b>	<b>O</b>	<b>N</b>

( ● =a / ● =b )		
abbab	baabb	abaa
<b>O</b>	<b>U</b>	<b>I</b>