LE CHIFFREMENT MANUEL

REVISITÉ

Ph. ALLARD

AMD-crypto@orange.fr

2015

Le chiffrement manuel revisité

Avant-propos

Ce document rassemble plusieurs articles tous consacrés au chiffrement manuel. Ce sujet peut sembler désuet à l'ère des ordinateurs et des puissantes méthodes de chiffrement numérique. La situation est comparable à celle du problème de la localisation à la surface de la terre, le système GPS l'a résolu à l'échelle de la planète et avec une précision inégalée mais aucun explorateur ou randonneur confirmé ne partirait sans boussole et carte. De même toute personne impliquée dans une communication secrète doit prévoir une solution de secours et un procédé de dépannage simple et efficace ne nécessitant qu'un papier et un crayon avec le minimum d'effort intellectuel. C'est dans cet esprit et sous l'impulsion de notre participation au challenge allemand, mais à vocation internationale, MTC3[1] que nous avons abordé le passionnant sujet des méthodes classiques de chiffrement en s'efforçant d'y porter un regard nouveau et fécond. Les articles rassemblés traitent successivement d'un chiffre par substitution, d'une méthode de parcours d'un tableau, de deux chiffres par transposition, de l'algorithme de permutation utilisé dans ces chiffres, du problème général et pratique de fourniture des clés secrètes et enfin de conventions accessoires pour l'usage d'un alphabet limité :

Spirale : il s'agit plus précisément d'un chiffre à masque jetable qui est la forme reconnue la plus forte pour un chiffre par substitution. Sa conception est basée sur des notions très classiques comme la table de Vigenère et la suite de Fibonacci mais celles-ci sont renouvelées en profondeur par généralisation et aboutissent à une table de correspondance et une récurrence pseudo-linéaire qui donne à ce crypto-système une richesse combinatoire au moins égale à celle d'un chiffre à 128 bits. De plus il permet de traiter n'importe alphabet, aussi bien un mélange de lettres, chiffres et ponctuations qu'une langue étrangère et son sens d'écriture. Un programme associé a été développé et est disponible librement.

[1] https://www.mysterytwisterc3.org/en/

Parcours de relèvement d'un tableau : le problème du parcours ordonné d'un tableau, pour en relever le contenu, se rencontre dans la transposition de celui-ci. Nous proposons dans cet article une méthode systématique pour construire les éléments d'un vaste sous-ensemble de celui, immense, des permutations du tableau.

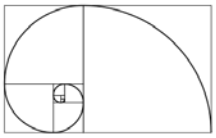
Diagonales : il s'agit ici de l'application à un chiffre par transposition des idées développées dans l'article précédent. Moins ambitieux et performant que Spirale, il est voulu surtout plus simple et rapide à mettre en œuvre tout en étant plus puissant que le classique chiffre par transposition simple des lignes et colonnes.

Carrousel : ce chiffre par transposition, conceptuellement très simple, repose exclusivement sur l'algorithme tournant de permutation au cœur de Spirale et Diagonales. Il fonctionne avec n'importe quel alphabet et des textes de n'importe quelle taille. Un programme associé a été développé et est disponible librement.

Algorithme de permutation : nous étudions dans ce bref article les propriétés de l'algorithme de permutation utilisé dans les chiffres précédents.

Création de clés : nous exposons ici un ensemble d'idées pour substituer au problème de la distribution des clés aux utilisateurs d'un crypto-système symétrique celui de la création des clés par les utilisateurs eux-mêmes. Les solutions proposées à ce problème s'appuient sur plusieurs procédés et outil informatique que nous suggérons ici.

Conventions accessoires pour alphabet limité : l'usage d'un alphabet limité à 26 lettres limite l'intelligibilité des messages et empêche de nombreux chiffres manuels de traiter des messages à caractère scientifique ou technique. Cette brève note propose plusieurs conventions pour palier à ce handicap.



SPIRALE

Un chiffre à masque jetable

Plan[1]

1. Introduction

Malgré notre époque de haute technologie et la puissance des ordinateurs personnels permettant l'implémentation de systèmes de chiffrement numérique sophistiqués, à clé privée ou publique, il y a encore un effort de quelques-uns pour créer un chiffre manuel moderne. Le chiffre bien connu Solitaire de B. Schneier [2] et Handycipher de B. Kallick [1] en sont les cas les plus récents.

Solitaire est du type chiffre à Masque Jetable, la version moderne du chiffre de Vigenère, caractérisé par une clé aléatoire de même longueur que le texte clair. La suprématie démontrée de cette approche repose sur une très longue clé ou masque formé d'une suite totalement aléatoire de caractères ainsi que sur un usage unique de celle-ci. La première condition n'est atteinte qu'en faisant appel à un phénomène physique naturellement aléatoire, comme la désintégration nucléaire, et la seconde par la transmission du lot de masques à travers un canal absolument sûr, en pratique de la main à la main, aux différents correspondants. Avec en corollaire le problème de l'archivage sécurisé de ces masques par les correspondants. Ces conditions ne sont qu'exceptionnellement réalisées et la mise en

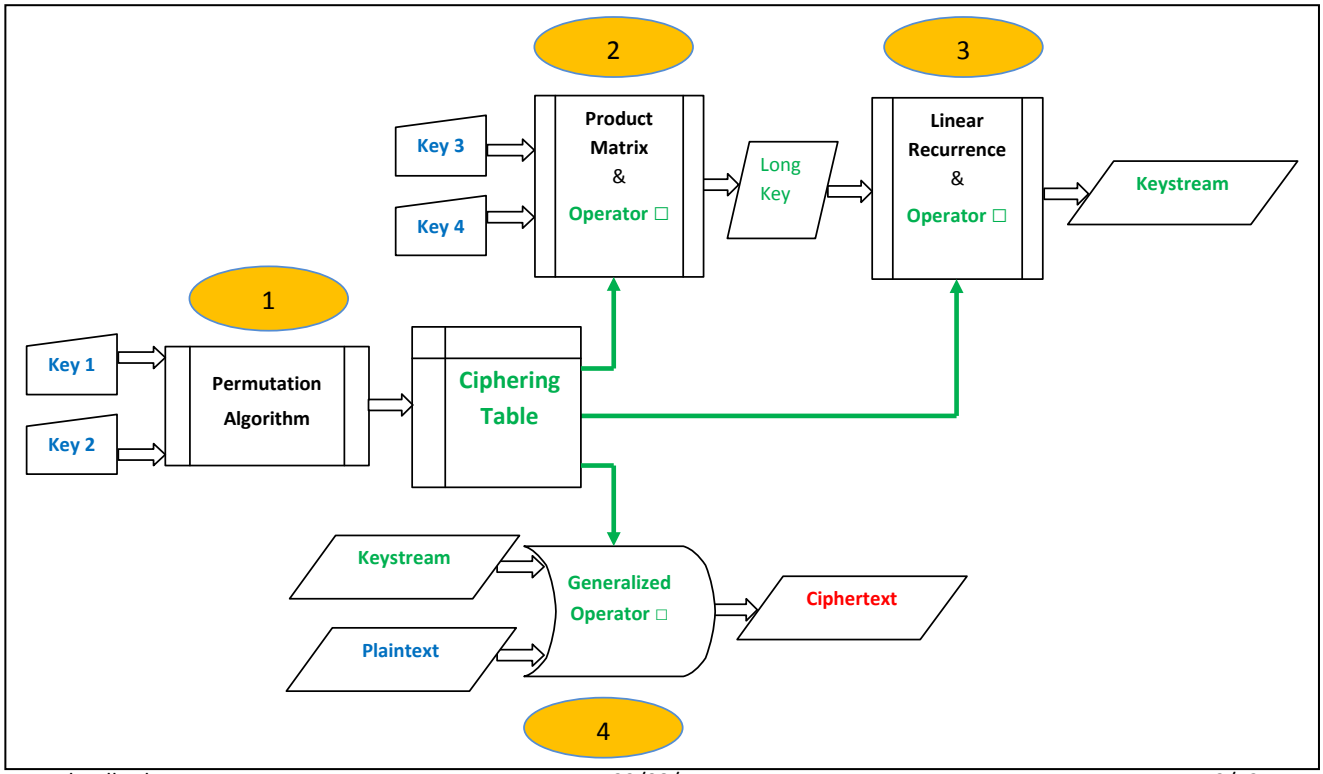
[1] Ce document est la traduction de l'article originel en anglais pour le challenge MTC3 (https://www.mysterytwisterc3.org/en/).

œuvre pratique, et finalement dégradée, de ces concepts consiste à calculer pour chaque message un masque, et donc une suite seulement pseudo-aléatoire, à partir d'un nombre élevé de clés conservées et partagées par les correspondants. Solitaire est original par l'usage qu'il fait d'un jeu de cartes pour réaliser manuellement le processus de calcul de la suite de lettres. Il a été bien étudié et son efficacité est établie.

Mais il est maintenant si célèbre que, dans un contexte de communications secrètes, posséder un jeu de cartes est aussi compromettant qu'un ordinateur contenant des programmes de cryptage. De plus tout le monde n'a pas une pratique ou aisance suffisante avec le jeu de Bridge base de la méthode. Aussi B. Callick a-t-il proposé Handycipher comme une solution alternative ne nécessitant que papier et stylo. C'est un chiffre à substitution homophonique non déterministe dans lequel chaque lettre du texte clair est remplacée de manière pseudo-aléatoire par un groupe de 1 à 5 caractères. Aussi le texte chiffré est-il beaucoup plus long que le texte clair et dans un rapport généralement supérieur à 4. Cet inconvénient pratique ajouté au processus plutôt laborieux de chiffrement ne fait pas de cet algorithme une alternative satisfaisante.

Nous proposons donc ici une autre solution. C'est aussi un chiffre à masque jetable, conçu pour une mise en œuvre manuelle simple avec un haut niveau de variabilité combinatoire équivalent à un système de cryptage à 128 bits. Pour générer le masque pseudo-aléatoire nous nous appuyons sur des concepts classiques comme la suite de Fibonacci et la congruence mais en les généralisant pour atteindre la richesse combinatoire souhaitée contre la cryptanalyse. L'algorithme final ne demande presque pas de calculs mentaux et se limite à des entrées répétitives dans une table spéciale. Ce processus est résilient aux erreurs commises par l'utilisateur car elles n'ont qu'un effet local et laissent le texte chiffré globalement intelligible.

Le chiffre Spirale se déroule en plusieurs étapes selon le schéma suivant (*Figure.1*):



avec les données d'entrée en bleu, les algorithmes fixes en noir, les résultats et opérateur intermédiaires en vert et le résultat final en rouge.

2. Généralisation de la suite de Fibonacci[2]

Pour un premier exposé des idées nous travaillons avec l'alphabet simple A, B, C … X, Y, Z et nous associons à chaque lettre son rang comme valeur: 1 pour A, 2 pour B, … 26 pour Z. Spirale étant un chiffre à masque jetable notre but et idée sont ici de créer un long masque à partir d'une chaîne de lettres de longueur k faisant fonction d'amorce. Travaillons maintenant sur les valeurs entières, cela signifie créer une suite de nombres (plus bas en vert) à partir d'une suite donnée de longueur k (plus bas en bleu). Le problème est de générer par un calcul déterministe une longue suite de lettres aussi pseudo-aléatoire que possible. En travaillant maintenant sur leurs valeurs, le problème devient arithmétique et pour rester toujours dans l'intervalle [1, 26] les calculs doivent être exécutés modulo 26.

La solution classique pour générer une suite est d'utiliser une relation de récurrence. Gardant à l'esprit l'objectif d'un chiffre manuel facile à calculer, la forme la plus simple à exploiter est la récurrence linéaire dont l'exemple emblématique est la suite de Fibonacci :

$$X_n = (X_{n-1} + X_{n-2}) \bmod 26$$

Des résultats comme **16, 19**, 9, 2, 11, 13, 24, 11, 9, 20, 3, 23, 26, 23, 23, 20, 17, 11, 2… (avec k = 2) semblent aléatoires mais avec cette formule chaque élément est fortement corrélé aux deux précédents. Une idée pour éviter cette caractéristique structurelle pourrait être d'augmenter l'ordre de la récurrence en prenant en compte plus de terme mais cela augmenterait aussi la charge de calcul. Un compromis est d'éloigner les deux termes de la récurrence, par exemple le second en le prenant à l'autre bout de la suite initiale de longueur k :

$$X_n = (X_{n-1} + X_{n-k}) \bmod 26$$

avec k = 4 termes initiaux les résultats sont **16, 19, 9, 2**, 18, 11, 20, 22, 14, 25, 19, 15, 3, 2, 21, 10, 13, 15, 10, 20, 7, 22, 6, 26, 6, 2, 8, 8, 14, 16… Il reste que, comme X_n dépend de X_{n-1}, deux termes consécutifs sont encore corrélés et une erreur dans le calcul de X_{n-1} se propage à X_n et à tous les termes suivants comme ici les six derniers termes.

Pour éviter ces derniers défauts l'idée est aussi de repousser le premier terme, par exemple à l'autre bout lui aussi :

$$X_n = (X_{n-k+1} + X_{n-k}) \bmod 26$$

Ou quelque part à une profondeur d proche du milieu de la suite initiale, pour répartir spatialement avec uniformité l'influence locale des éléments de l'amorce sur ceux du masque :

$$X_n = (X_{n-d} + X_{n-k}) \bmod 26$$

[2] Utilisée dans l'étape 3 du chiffre.

La figure 2 explique notre idée : le nombre X_n est dépendant seulement de X_{n-k} et X_{n-d}, si d est proche de k (d=k-1) l'influence de proche en proche sur les nombres suivants du masque induira sur celui-ci une structure pseudo-aléatoire proche de celle de la séquence amorce ; en espaçant n-d de n-k nous augmentons le caractère pseudo-aléatoire du masque. Nous préférons aussi cette dernière solution car ainsi, deux éléments consécutifs sont corrélés à deux paires d'éléments précédents complètement différentes et de plus une erreur se propagera uniquement par sauts de d et k éléments. Mais un cas est à éviter :

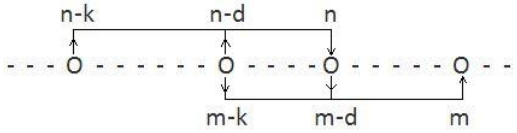


Figure.2

Quand un élément m est créé à partir de deux éléments déjà impliqués dans la récurrence. Une telle situation amène à générer non pas une unique et longue suite récurrente mais plutôt une petite série de suites de Fibonacci classiques imbriquées entre elles. Les conditions pour cette situation sont :

$$n\text{-}d = m\text{-}k \qquad \text{and} \qquad n = m\text{-}d$$

d'où $$k = 2d \qquad (1)$$

3. Génération de la séquence amorce[3]

Comme nous venons de le voir, pour diminuer la corrélation entre éléments consécutifs du masque, il est bénéfique que la séquence amorce soit longue. Pour créer une telle longue chaîne qui joue le rôle de clé dans le processus de chiffrement classique de Vigenère, nous utilisons deux clés courtes Key 1 et Key 2 et nous disposons ces données et leur résultat dans une matrice via la formule :

$$Y_{p,q} = (X_p + X_q) \bmod 26$$

Par exemple, avec les clés Key 1 = {19, 15, 12, 9} et Key 2 = {20, 1, 9, 18, 5}, nous engendrons une matrice de 4x5 = 20 cellules:

Key 1						
	19	13	20	2	11	24
	15	9	16	24	7	20
	12	6	13	21	4	17
	9	3	10	18	1	14
		20	1	9	18	5
		Key 2				

Figure.3

[3] Utilisée dans l'étape 2 du chiffre.

Ensuite nous pourrions lire cette matrice horizontalement ou verticalement. Mais s'il y a dans une des clés un nombre répété cela produira la répétition d'une ligne ou d'une colonne. Pour éviter cela une première solution est de convenir de ne pas mettre deux fois le même nombre dans une clé. Une autre solution, non exclusive de la première, est de lire différemment la matrice. Nous optons finalement pour une lecture en diagonale ascendante depuis le coin supérieur gauche. C'est un des procédés classiques utilisés dans le chiffrement par transposition pour bousculer l'ordre des éléments d'un message. Mais tout autre cheminement facile et efficace pourrait convenir. Ainsi la longue clé finale de 20 éléments est donc :

{13, 9, 20, 6, 16, 2, 3, 13, 24, 11, 10, 21, 7, 24, 18, 4, 20, 1, 17, 14}

Et elle pourrait être utilisée comme séquence amorce de la récurrence linéaire :

$$X_n = (X_{n-9} + X_{n-20}) \bmod 26$$

Avec n-9 pour éviter la condition (1). Les premiers éléments générés seraient alors :

$$13,21 \rightarrow 7 \qquad 9,7 \rightarrow 16 \qquad 20,24 \rightarrow 18 \qquad 6,18 \rightarrow 24 \qquad \ldots$$

Pour ce déplacer le long de la suite générée et identifier facilement les éléments à utiliser dans la formule, il est commode de se servir d'une bande de papier avec trois marques, espacées respectivement ici de 11 et 9 cases :

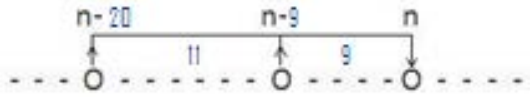


Figure.4

4. Généralisation de l'addition congruente[4]

Pour un exposé simplifié des idées mise en jeu ici nous nous limiterons aux entiers compris entre 0 et 9. La classique congruence modulo 10 composée avec l'addition définit une application de [0,9]x[0,9] sur [0,9] et une loi de composition interne sur l'intervalle [0,9] exprimée par un opérateur que nous noterons ⊕ :

$$X \oplus Y = (X+Y) \bmod 10$$

Cet opérateur peut aussi être décrit par sa table :

[4] Utilisée dans les étapes 2 à 4 du chiffre.

⊕	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Table.1

Il jouit de propriétés particulières:

- Symétrie X⊕Y = YX⊕X
- Surjectivité 3= 1⊕2= 5⊕8= 6⊕7 5= 2⊕3= 9⊕6= 7⊕8 …
- Surjectivité uniforme : chaque valeur (0,…,9) du résultat X⊕Y apparait autant de fois dans la table et pour chacune d'elles il y a un nombre égal de couples (X,Y) donnant cette valeur.

Cette dernière propriété est utile en cryptographie car elle permet de construire des fonctions difficiles à inverser ou à découvrir, du fait de la multiplicité des solutions possibles. En effet, si on rencontre un 3 dans un texte chiffré comment savoir de quel couple il provient : (1,2) ou (5,8) ou (6,7) ?

Que se passe-t-il si nous permutons les valeurs résultat dans la table ? La symétrie disparaitra probablement, ce qui est un avantage finalement, mais pas la propriété principale : nombre égale de pré-images pour chaque valeur. Nous aurions alors une autre fonction utile pour le chiffrement. Comme il y a 10x10=100 éléments dans la matrice cela ferait 100 ! = $9{,}3.10^{157}$ combinaisons possibles.

Ce nombre monstrueux est bien au-delà de nos besoins et nous pouvons aisément définir un nombre suffisant de fonctions utiles, maintenant notées par l'opérateur □, en permutant simplement les valeurs d'entrées (indexes des lignes et colonnes). L'usage des symboles ⊕ et □ est fondamental pour montrer la différence entre la classique addition congruente et l'opérateur généralisé obtenu par permutation des indexes de la table. Voici un exemple d'une telle table permutée :

□	6	9	2	1	8	5	0	4	3	7
3	0	1	2	3	4	5	6	7	8	9
2	1	2	3	4	5	6	7	8	9	0
9	2	3	4	5	6	7	8	9	0	1
6	3	4	5	6	7	8	9	0	1	2
1	4	5	6	7	8	9	0	1	2	3
8	5	6	7	8	9	0	1	2	3	4
7	6	7	8	9	0	1	2	3	4	5
5	7	8	9	0	1	2	3	4	5	6
0	8	9	0	1	2	3	4	5	6	7
4	9	0	1	2	3	4	5	6	7	8

Table.2

Nous pouvons voir qu'avec cette nouvelle fonction :

$3 \square 6 = 0$ et $6 \square 3 = 1$ $\quad$ $1 \square 7 = 3$ et $7 \square 1 = 6$ $\quad$ …

$2 = 3 \square 2 = 2 \square 9 = 9 \square 6 = 1 \square 3 = 8 \square 4 = 7 \square 0 = 5 \square 5$

Pour entrer facilement dans cette nouvelle table il serait utile de réordonner les entrées en permutant lignes et colonnes comme dans les classiques chiffres par transposition. Nous verrons plus tard que nous pouvons éviter cette étape. Permuter indépendamment les entrées produira 10 !x10 ! combinaisons, soit plus de $1{,}3.10^{13}$ combinaisons.

Maintenant, que nous savons comment construire de nombreuses fonctions de chiffrement, nous pouvons revenir aux lettres, alphabet et congruence modulo 26. Avec les lettres, la traditionnelle addition modulo 26 est décrite par la classique table de Vigenère [annexe A]. En permutant chaque alphabet d'entrée nous pouvons créer une *table de chiffrement* complètement différente à chaque fois. Un exemple en est donné dans l'annexe B. Pour faciliter les entrées dans la table il n'est pas nécessaire de réordonner lignes et colonnes mais simplement d'ajouter une ligne et une colonne remplies avec les rangs des lettres dans chaque alphabet permuté.

Avec le même exemple de table de chiffrement, cryptons le mot SPIRALE par le masque SGKKFPW :

lettre claire	S	P	I	R	A	L	E
ligne correspondante	15	16	11	21	13	19	17
masque	S	G	K	K	F	P	W
colonne correspondante	11	12	2	2	3	19	5
lettre chiffrée à l'intersection	Y	A	L	V	O	K	U

Nous observons que le processus de chiffrement ne demande aucun calcul mental mais seulement une succession d'entrées dans la table de chiffrement, il est donc facile et permet une grande vitesse de chiffrement. La construction de la table de chiffrement est la deuxième étape du processus complet de chiffrement, après la permutation des alphabets. Cette table ne sert qu'une seule fois et doit être détruite après usage, dans un véritable contexte de communications secrètes.

Le processus de déchiffrement est inverse : entrée par une colonne, lecture dans celle-ci de la lettre chiffrée et sortie par la même ligne donnant la lettre claire :

masque	S	G	K	K	F	P	W
colonne correspondante	11	12	2	2	3	19	5
lettre chiffrée	Y	A	L	V	O	K	U
ligne correspondante	15	16	11	21	13	19	17
lettre claire	S	P	I	R	A	L	E

A partir de maintenant, c'est une table de chiffrement analogue jouant le rôle de *table de correspondance* à usage unique, et l'opérateur associé □, qui sera utilisée pour générer la séquence amorce (la matrice de la Figure 3 fonctionne alors comme une « matrice produit » des clés générant la séquence amorce), le masque ainsi que le texte chiffré et non plus la simple addition congruente ⊕ introduite dans l'exposé préliminaire du paragraphe 4. Cette table de correspondance provisoire est ainsi au cœur du système de chiffrement. Ce que nous avons exprimé, entre autre, dans la figure 1.

5. Algorithme de permutation[5]

Nous avons donc besoin de permuter l'alphabet deux fois par message à envoyer. Pour cela nous appliquons l'algorithme suivant :

- À partir d'une courte chaîne de lettres jouant le rôle de clé ;
- Nous formons une *liste de permutation*, formée d'entiers, avec les rangs dans l'alphabet de chacune des lettres ;
- Puis la permutation est menée en tournant autour de l'alphabet, en commençant par l'extrémité droite et en sélectionnant les lettres espacées conformément à la liste de permutation. Quand une lettre a déjà été sélectionnée elle est sautée aux tours suivants. La liste de permutation est lue cycliquement jusqu'à épuisement de l'alphabet original. Au fur et à mesure de leur sélection, les lettres sont portées dans l'alphabet permuté qui se constitue ainsi progressivement;

L'annexe C décrit en détails un exemple avec la clé BHMAY et donc la liste de permutation [2, 8, 13, 1, 25]. Examinons le processus de permutation des premières lettres de l'alphabet original : 2 → Y, 8 → Q, 13 → D, 1 → C, 25 → Z en tournant autour de l'alphabet pour revenir à l'origine, puis nouvelle lecture de la liste de permutation, 2 → W en sautant Y déjà sélectionnée et barrée, 8 → N en sautant Q, 13 → V en sautant D et C, 1 → U , 25 → K en sautant Q-N-D-C-Z-Y-W-V-U, … l'alphabet permuté commence donc par YQDCZWNVUK. Parallèlement, la quatrième ligne du tableau est remplie avec le nouveau rang des lettres qui sera utilisé dans la table de chiffrement.

Dans cette étape, encore, il n'y a pas vraiment de calculs mais seulement une opération simple et répétitive.

6. Le chiffre Spirale

Nous avons maintenant tous les concepts et outils nécessaires pour construire notre chiffre. Il utilise finalement 4 clés :

- Clé 1 pour permuter les lignes de la table de chiffrement;
- Clé 2 pour permuter les colonnes de la table de chiffrement;
- Clé 3 pour créer les lignes de la matrice de la séquence amorce;
- Clé 4 pour créer les colonnes de la matrice de la séquence amorce;

[5] Utilisé dans l'étape 1 du chiffre.

Une clé formée de p lettres offre $C=26^p$ combinaisons possibles. Les effets de ces clés sont indépendants, combinés et entrelacés dans le processus complet de chiffrement. Le nombre total de combinaisons est donc $C_1xC_2xC_3xC_4 = 26^{p_1+p_2+p_3+p_4}$. Ainsi le nombre total de combinaisons dépend-il finalement de la taille cumulée *n* de ces clés formées de suite de lettres choisies parmi 26. Le but est de donner à Spirale un niveau de sécurité combinatoire, contre les attaques par force brute, équivalent à un chiffre à 128 bits, or

$$2^{128} = 26^n \qquad \text{implique} \qquad n \approx 27.2$$

Cela signifie qu'avec une clé globale de 28 lettres l'objectif est largement atteint, en supposant que nous ayons des clés vraiment aléatoires. Nous choisissons de répartir uniformément cette variabilité combinatoire sur toutes les clés, et donc celles-ci doivent avoir chacune 7 lettres. Et toutes les étapes précédemment décrites seront exécutées avec de telles clés.

La séquence amorce sera générée selon la formule (X est maintenant le symbole des lettres) :

$$Y_{p,q} = X_p \square X_q \qquad (2)$$

Et donc la séquence amorce aura 7x7=49 lettres de long. Pour un message de moins de 50 lettres, cette séquence sera le masque jetable. Pour un message plus long, le masque sera généré selon la formule :

$$X_n = X_{n-49} \square X_{n-24} \qquad (3)$$

Où l'ordre des termes est important car l'opérateur □ défini par la table de chiffrement n'est plus symétrique.

Maintenant, on peut aussi comprendre le nom donné à ce chiffre : partant de 4 clés jouant le rôle de graines, induisant un processus tournant pour produire les alphabets permutés dérivés en une table de chiffrement qui est le cœur de sa sécurité et se déployant en un masque potentiellement infini. Soit globalement une structure assez similaire à celle d'une spirale à 4 centres.

7. Implémentation et exemple détaillé

Plusieurs feuilles modèles ont été créées pour un usage facile de Spirale. Elles sont rassemblées dans l'annexe D et illustrent en détails un exemple[6] complet bâti avec les clés suivantes : NVIKKIH, CTSQEOU, DNGDKSZ et EAIWDSH.

- annexe D1: Permutations de l'Alphabet.

  Pour faciliter le repérage des lettres encore disponibles dans l'alphabet originel, nous suggérons de rayer les lettres déjà permutées d'un trait épais et pour suivre l'avancement du parcours cyclique de la liste de permutation nous suggérons de faire une marque, par exemple un point, sous une de ses lettres chaque fois qu'elle est utilisée.

- annexe D2: Table de chiffrement.

  Y reporter simplement les résultats de l'annexe D1.

[6] Il s'agit du même exemple, en anglais, que celui du document originel.

- annexe D3: Séquence amorce et Masque jetable.

Ce modèle est conçu pour générer jusqu'à 400 caractères de masque, pour un texte plus long enchaîner sur une feuille identique. Comme la séquence amorce est trop longue pour appliquer l'idée d'une bande de papier glissant le long du masque, nous disposons les lettres de telle façon que les termes impliqués dans la récurrence (de rangs n-49 et n-24) soient sur une même colonne et ainsi lues aisément. La relation de récurrence (3) peut aussi s'écrire :

$$X_p \square X_{p+25} = X_{p+49} \qquad (3bis)$$

Cela implique que les lignes du modèle doivent avoir 25 cases et que le résultat n'est pas dans la même colonne mais à sa gauche :

…	X_p	…
…	X_{p+25}	…
X_{p+49}	X_{p+50}	…

Nous écrivons donc les résultats, dans cette feuille modèle, à partir de l'extrême gauche. Ces cases grisées contiennent alors la valeur manquante dans la dernière case de la ligne respectivement au dessus et nous y reportons donc ces valeurs.

- annexe D4: Chiffrement et Déchiffrement.

Elle est conçue pour traiter 200 caractères, pour un texte plus long il suffit d'enchaîner sur une feuille identique. Comme nous utilisons un alphabet minimal, le texte clair ne peut contenir de chiffres et nous devons aussi supprimer tous les espaces et signes de ponctuation. Le processus se déroule ligne par ligne, de haut en bas pour le chiffrement en entrant dans la table de chiffrement avec la lettre claire et sa lettre masque et de bas en haut pour le déchiffrement en entrant dans cette table avec la lettre masque et la lettre chiffrée (dans la même colonne).

Les versions vierges de ces feuilles modèles sont rassemblées dans l'annexe E. A l'aide de ces modèles un utilisateur débutant peut travailler rapidement et mettre seulement 1 heure pour suivre toutes les étapes et chiffrer les 75 lettres de l'exemple.

8. Défis

Pour inciter les cryptanalystes à briser ce chiffre nous proposons ici différents textes chiffrés[7] correspondant à des situations affaiblissantes d'utilisation :

- Ciphertext 1, issu d'un texte de 314 lettres commençant par le texte de l'exemple détaillé;
- Ciphertext 2, issu d'un texte de 659 lettres chiffré avec les mêmes clés que ciphertext 1;
- Ciphertext 3, issu d'un texte de 949 lettres chiffré avec les clés 1 et 2 communes à celles des ciphertext 1 et 2;

[7] Il s'agit encore des textes en anglais du document originel. Pour être dans l'esprit d'un usage opérationnel de Spirale, les textes 2 à 4 proviennent du renseignement militaire ouvert.

- Et pour finir, Ciphertext 4 un texte de 485 lettres chiffré de façon sécurisé avec 4 clés originales. Tous ces textes chiffrés sont dans l'annexe F.

9. Extensions de l'alphabet

Avec un alphabet limité à des lettres, l'expression des nombres ou dates doit être faite littéralement (2015 = deux zéro un cinq ou deux mille quinze) ce qui prend beaucoup de place dans un message. Une solution simple à ce défaut est d'étendre l'alphabet, ainsi :

A … Z 0 1 2 3 4 5 6 7 8 9

Cela n'implique aucune complication dans l'algorithme : la seule différence est l'extension jusqu'à 36 cases du tableau alphabet de l'annexe E1 et autant pour la table de chiffrement. La séquence amorce et le masque seront alors une suite de lettres et de chiffres. Et les 4 clés de 7 caractères pourront inclure lettres et chiffres. Avec cette extension il y a aussi une augmentation des combinaisons à 36^7 pour les clés et à $36^7 x 36^7$ pour la paire d'alphabets permutés, donc avec l'ensemble des clés c'est un accroissement considérable à 36^{28} des caractéristiques combinatoires de ce chiffre ainsi équivalent à un système à 144 bits.

La généralisation peut aller encore plus loin et inclure aussi les caractères typographiques pour rendre plus lisible le message ou permettre le traitement de segments particuliers comme une formule mathématique ou chimique et des données économiques. Un tel alphabet pourrait être (le caractère *espace* est ici représenté par _) :

A … Z 0 … 9 _ , . ( ) + - * / ^ < = > % € £ $

Dans ce cas, les permutations devraient se faire sur 53 caractères et étendre d'autant la table de chiffrement et donc la résistance du chiffre aux attaques par force brute. Les versions correspondantes des annexes E1 et E2 sont dans les annexes G1 et G2. Un exemple de texte clair utilisant un alphabet encore plus riche (59 caractères) et sa version chiffrée, obtenue avec un programme écrit en python, sont présentés dans l'annexe G3.

Comme Spirale est conçu pour un usage manuel il peut fonctionner avec n'importe quel alphabet, y compris les plus exotiques :

Α Β Γ Δ Ε Ζ Η Θ Ι Κ Λ Μ Ν Ξ Ο Π Ρ Σ Τ Υ Φ Χ Ψ Ω

ا ب ج د ه و ز ح ط ي ك ل م ن س ع ف ص ق ر ش ت ث خ ذ ض ظ غ

अ आ इ ई उ ऊ ऋ ॠ ए ऐ ओ औ अं अँ अः ऌ ॡ प पा पि पी पु पू पृ पॄ पे पै पो पौ पं पाँ पः पॢ पॣ

Il est alors juste nécessaire de créer la table de Vigenère correspondante et de lui associer deux permutations de l'alphabet pour construire une table de chiffrement. Dans le cas d'une langue s'écrivant de droite à gauche, les feuilles modèles sont toujours utiles et seule l'annexe E3 doit être inversée pour donner l'annexe E3bis.

10. Références

1. B. Kallick, Handycipher: a Low-tech, Randomized, Symmetric-key Cryptosystem (2014), version 4.9, available at http://eprint.iacr.org/2014/257.pdf
2. B. Schneier, The Solitaire encryption algorithm, version 1.2, (1999), available at https://www.schneier.com/solitaire.html.

11. Annexes

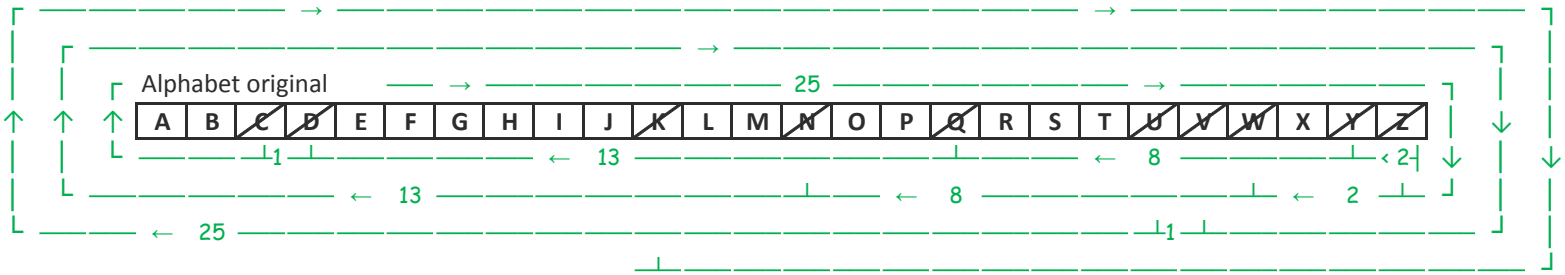
A	Table de Vigenère
B	Table de chiffrement : Exemple
C	Algorithme de Permutation : Exemple
D1	Exemple détaillé - Permutations de l'alphabet
D2	Exemple détaillé – Table de chiffrement
D3	Exemple détaillé – Séquence amorce & Masque jetable
D4	Exemple détaillé – Chiffrement ou Déchiffrement
E1	Permutations de l'alphabet
E2	Table de chiffrement
E3	Séquence amorce & Masque jetable
E3a	Séquence amorce & Masque jetable (pour les écritures de droite à gauche)
E4	Chiffrement ou Déchiffrement
F	Défis
G1	Permutations de l'alphabet étendu
G2	Table de chiffrement (alphabet étendu)
G3	Exemple d'application avec un alphabet étendu
G3a	Fenêtre interactive avec la sortie du programme en python

Table de Vigenère

⊕	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
A	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
B	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	A
C	C	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
D	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
E	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	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	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
K	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
L	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	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

□				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
nouveaux rangs →				17	26	21	7	10	3	12	20	14	23	2	15	9	18	6	19	22	25	11	1	16	13	5	4	8	24
↓ lettres				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
			↓→	T	K	F	X	W	O	D	Y	M	E	S	G	V	I	L	U	A	N	P	H	C	Q	J	Z	R	B
A	13	1	Y	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
B	24	2	Q	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	A
C	4	3	D	C	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
D	3	4	C	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
E	17	5	Z	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	D
F	20	6	W	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	23	7	N	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	22	8	V	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	11	9	U	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	26	10	K	J	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
K	10	11	I	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
L	19	12	T	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	K
M	18	13	A	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	7	14	X	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	25	15	S	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	16	16	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	2	17	E	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	21	18	M	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	15	19	L	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	12	20	F	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	9	21	R	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	8	22	H	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	6	23	G	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	14	24	B	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	1	25	O	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	5	26	J	Z	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

Clé de permutation de l'alphabet →	B	H	M	A	Y		
	2	8	13	1	25			← rang dans l'alphabet original



rayez la lettre dans l'alphabet original quand elle est permutée, pour la sauter ultérieurement

Alphabet permuté

	Y	Q	D	C	Z	W	N	V	U	K															
rang dans l'alphabet permuté →	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
recherche d'une lettre →	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
rang dans l'alphabet permuté →			4	3							10			7			2				9	8	6		1	5

Alphabet original

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

compter dans ce sens pour la permutation ←

après permutation d'une lettre, rayez la dans l'alphabet avec un crayon foncé

Clé 1 de permutation de l'alphabet →

N	V	I	K	K	I	H
14	22	9	11	11	9	8
..	..	..	.	.	.	.

← rang dans l'alphabet original

← marques pour tracer l'avancement dans le processus de permutation

Alphabet permuté pour les **Lignes** de la Table de Chiffrement

	M	Q	G	V	I	Y	O	W	R	D	L	U	E	P	K	N	T	J	C	A	X	B	S	Z	H	F
rang dans l'alphabet permuté →	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
recherche d'une lettre →	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
son rang dans l'alphabet permuté →	20	22	19	10	13	26	3	25	5	18	15	11	1	16	7	14	2	9	23	17	12	4	8	21	6	24

Alphabet original

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

compter dans ce sens pour la permutation ←

après permutation d'une lettre, rayez la dans l'alphabet avec un crayon foncé

Clé 2 de permutation de l'alphabet →

C	T	S	Q	E	O	U
3	20	19	17	5	15	21

← rang dans l'alphabet original

← marques pour tracer l'avancement dans le processus de permutation

Alphabet permuté pour les **Colonnes** de la Table de Chiffrement

	X	D	J	Q	L	T	S	O	M	I	H	B	A	N	F	P	U	W	E	C	V	G	K	Z	Y	R
rang dans l'alphabet permuté →	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
recherche d'une lettre →	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
son rang dans l'alphabet permuté →	13	12	20	2	19	15	22	11	10	3	23	5	9	14	8	16	4	26	7	6	17	21	18	1	25	24

Table de Chiffrement

				lettre de la CLÉ 4 ou du MASQUE																								
	□			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
		du nouveau rang vers la lettre		13	12	20	2	19	15	22	11	10	3	23	5	9	14	8	16	4	26	7	6	17	21	18	1	25	24
		⌜ → ⌝		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
				X	D	J	Q	L	T	S	O	M	I	H	B	A	N	F	P	U	W	E	C	V	G	K	Z	Y	R
lettre de la CLÉ 3 ou du TEXTE CLAIR	A	20	1	M	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
	B	22	2	Q	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	A
	C	19	3	G	C	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
	D	10	4	V	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
	E	13	5	I	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	D
	F	26	6	Y	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G	3	7	O	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	H	25	8	W	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	I	5	9	R	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	18	10	D	J	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
	K	15	11	L	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
	L	11	12	U	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	K
	M	1	13	E	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N	16	14	P	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	7	15	K	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	P	14	16	N	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	2	17	T	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R	9	18	J	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	23	19	C	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T	17	20	A	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	U	12	21	X	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	V	4	22	B	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	W	8	23	S	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	X	21	24	Z	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	Y	6	25	H	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Z	24	26	F	Z	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

du nouveau rang vers la lettre ⌜ ↓ ⌟

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

remplissez la matrice selon :

$$Y_{p,q} = X_p \square X_q$$

avec la Table de Chiffrement

puis remplissez les 49 premières cases ci-dessous en lisant la matrice diagonalement depuis le coin supérieur gauche

et générez le reste du masque selon $X_p \square X_{p+25} = X_{p+49}$ à partir de p = 1

(copiez les cases grisées dans celles de même rang)

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
B	H	V	U	B	S	B	O	Y	A	G	V	L	G	K	O	A	S	T	Q	P	P	I	X	A
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
↙ D	V	T	J	F	F	K	I	Z	G	N	P	P	M	O	X	U	T	Y	C	Y	D	G	H	W
50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
W	S	I	N	J	K	R	P	C	O	P	S	Z	K	V	G	J	B	O	U	L	O	Z	E	K	P
75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
P																									
100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125
125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150
150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200
200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225
225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250
250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275
275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300
300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325
325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350
350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375
375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400

Puis copiez dans l'Annexe D4 les tronçons de 25 lettres (sans les cases grisées)

Chiffrement →

↓ Texte Clair

S	P	I	R	A	L	E	I	S	A	O	N	E	T	I	M	E	P	A	D	C	R	Y	P	T

↓ Masque

B	H	V	U	B	S	B	O	Y	A	G	V	L	G	K	O	A	S	T	Q	P	P	I	X	A

↓ Texte Chiffré

H	X	Y	Y	E	Q	X	L	U	F	B	J	Q	L	A	H	Y	T	Y	M	H	X	O	N	C

Déchiffrement →

Chiffrement →

↓ Texte Clair

O	S	Y	S	T	E	M	D	E	S	I	G	N	E	D	T	O	R	E	P	L	A	C	E	S

↓ Masque

D	V	T	J	F	F	K	I	Z	G	N	P	P	M	O	X	U	T	Y	C	Y	D	G	H	W

↓ Texte Chiffré

H	Q	K	Y	E	A	W	S	J	R	R	R	E	U	Q	Q	W	N	K	G	I	U	N	W	N

Déchiffrement →

Chiffrement →

↓ Texte Clair

O	L	I	T	A	I	R	E	W	H	E	N	O	N	E	H	A	S	N	O	C	A	R	D	S

↓ Masque

S	I	N	J	K	R	P	C	O	P	S	Z	K	V	G	J	B	O	U	L	O	Z	E	K	P

↓ Texte Chiffré

M	T	R	S	P	D	X	F	O	N	S	M	C	J	H	A	E	D	F	K	Z	Q	A	F	L

Déchiffrement →

Chiffrement →

↓ Texte Clair

↓ Masque

↓ Texte Chiffré

Déchiffrement →

Chiffrement →

↓ Texte Clair

↓ Masque

↓ Texte Chiffré

Déchiffrement →

Chiffrement →

↓ Texte Clair

↓ Masque

↓ Texte Chiffré

Déchiffrement →

Chiffrement →

↓ Texte Clair

↓ Masque

↓ Texte Chiffré

Déchiffrement →

Chiffrement →

↓ Texte Clair

↓ Masque

↓ Texte Chiffré

Déchiffrement →

Alphabet original

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

compter dans ce sens pour la permutation ←

après permutation d'une lettre, rayez la dans l'alphabet avec un crayon foncé

Clé 1 de permutation de l'alphabet →

← rang dans l'alphabet original

← marques pour tracer l'avancement dans le processus de permutation

Alphabet permuté pour les **Lignes** de la Table de Chiffrement

rang dans l'alphabet permuté →	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
recherche d'une lettre →	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
son rang dans l'alphabet permuté →																										

Alphabet original

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

compter dans ce sens pour la permutation ←

après permutation d'une lettre, rayez la dans l'alphabet avec un crayon foncé

Clé 2 de permutation de l'alphabet →

← rang dans l'alphabet original

← marques pour tracer l'avancement dans le processus de permutation

Alphabet permuté pour les **Colonnes** de la Table de Chiffrement

rang dans l'alphabet permuté →	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
recherche d'une lettre →	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
son rang dans l'alphabet permuté →																										

Table de Chiffrement

				lettre de la CLÉ 4 ou du MASQUE																										
	□			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
	nouveaux rangs → ↓ lettres ⌜ → ↓→																													
				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	⌜ ↓ ⌟
lettre de la CLÉ 3 ou du TEXTE CLAIR	A		1	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
	B		2	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	A
	C		3	C	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
	D		4	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
	E		5	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	D
	F		6	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G		7	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	H		8	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	I		9	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J		10	J	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
	K		11	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
	L		12	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	K
	M		13	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N		14	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O		15	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	P		16	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q		17	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R		18	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S		19	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T		20	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	U		21	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	V		22	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	W		23	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	X		24	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	Y		25	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Z		26	Z	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

	Clé 4						
Clé 3							

remplissez la matrice selon :

$$Y_{p,q} = X_p \square X_q$$

avec la Table de Chiffrement

puis remplissez les 49 premières cases ci-dessous en lisant la matrice diagonalement depuis le coin supérieur gauche

et générez le reste du masque selon $X_p \square X_{p+25} = X_{p+49}$ à partir de p = 1

(copiez les cases grisées dans celles de même rang)

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	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
↙																								
50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125
125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150
150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200
200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225
225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250
250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275
275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300
300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325
325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350
350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375
375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400

Puis copiez dans l'Annexe E4 les tronçons de 25 lettres (sans les cases grisées)

Key 3	Key 4						

remplissez la matrice selon :

$$Y_{p,q} = X_p \square X_q$$

avec la Table de Chiffrement

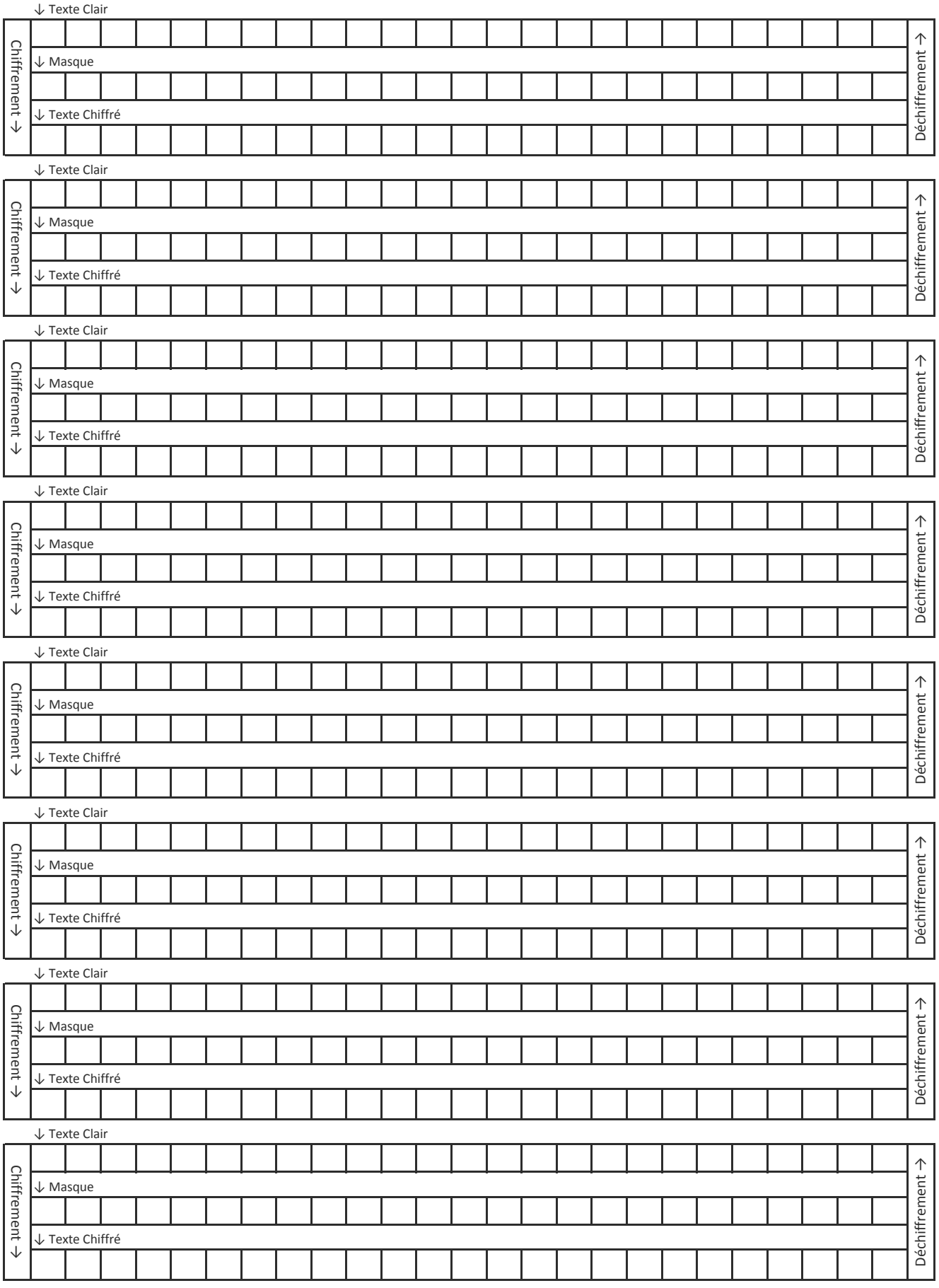
puis remplissez les 49 premières cases ci-dessous en lisant la matrice diagonalement depuis le coin supérieur gauche

et générez le reste du masque selon $X_p \square X_{p+25} = X_{p+49}$ à partir de p = 1

(copiez les cases grisées dans celles de même rang)

25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26
75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51
100	99	98	97	96	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81	80	79	78	77	76
125	124	123	122	121	120	119	118	117	116	115	114	113	112	111	110	109	108	107	106	105	104	103	102	101
150	149	148	147	146	145	144	143	142	141	140	139	138	137	136	135	134	133	132	131	130	129	128	127	126
175	174	173	172	171	170	169	168	167	166	165	164	163	162	161	160	159	158	157	156	155	154	153	152	151
200	199	198	197	196	195	194	193	192	191	190	189	188	187	186	185	184	183	182	181	180	179	178	177	176
225	224	223	222	221	220	219	218	217	216	215	214	213	212	211	210	209	208	207	206	205	204	203	202	201
250	249	248	247	246	245	244	243	242	241	240	239	238	237	236	235	234	233	232	231	230	229	228	227	226
275	274	273	272	271	270	269	268	267	266	265	264	263	262	261	260	259	258	257	256	255	254	253	252	251
300	299	298	297	296	295	294	293	292	291	290	289	288	287	286	285	284	283	282	281	280	279	278	277	276
325	324	323	322	321	320	319	318	317	316	315	314	313	312	311	310	309	308	307	306	305	304	303	302	301
350	349	348	347	346	345	344	343	342	341	340	339	338	337	336	335	334	333	332	331	330	329	328	327	326
375	374	373	372	371	370	369	368	367	366	365	364	363	362	361	360	359	358	357	356	355	354	353	352	351
400	399	398	397	396	395	394	393	392	391	390	389	388	387	386	385	384	383	382	381	380	379	378	377	376

Puis copiez dans l'Annexe E4 les tronçons de 25 lettres (sans les cases grisées)


↓ Texte Clair
Chiffrement →
↓ Masque
↓ Texte Chiffré
Déchiffrement →

Ciphertext 1

XEXEQPVDKYMVCCRZTMRLCCKQBKPOEVZXYQDDCIOEINTLVQJKATRBDWEEMVMYOOEIOOVMOCRSBJGSNZUQJZTX
ODHAOTRIEJRPENVKDJYVLNPOERZSFZTIHTZJMMOTBGRJCCZMVOUNWMKTPCPPCASJFAVUEJPTJRTWFCHIGZTGTCJ
EYRZDISQEKTKPNIBNAPQSUKCUPWKSZBSNOATKXKGHRAMONICEEGJBZGBLRFRHBYTHITNLXRFCZPLZOEUTBMJOE
GLLEHSNBAYNWONHAQVSDDFVOTDMEGQEAEZHMQZVYYREHBDBFHYRVYJTBO

Ciphertext 2

BDXVLCJKYIFKACDRUUDLVCOEVKYUCOQBHIVDETOYIWCUERVAJXUTXZNDLSXHOBXAONQLPMQZGIBJLLIMCKCXSB
ZRYJUSOJDBTHYPRNVKEKMXSLGMFRSQRQKZTSLBDWYJYJMLBPEAGOVCLZUMMRYPMDIWDRVZSAVYIHIOMVTXHX
SJOQEWVATGCKGKKRKKVRPXUNWGMFKZBEQZZLDKCNRZWQKFCYDUICEKZUEANTNOPYUXKSDIDRGAVQDBMGSJP
JJHNPEEGOGWDNMPXXCVLFLKLEQEYDKAUSVDCXJBMIGKCXDJBSWLJNLGGHPSJJRXORUNPSEILGSVXAQRSWVRSKR
RGEUJSQKGPRFNGJBQPTXNRFQZSXKPVZWMZKGIVMKVUTJQNJMEMDIPKZOMWTLNWGWSQRUEPEXMHPEBBNTB
PKSEQSELOCJOYPJCCMIPVTXWYITOZWJWVKOSDJYBFXIJAWDVWMVKRKZKXFNRFOQVOIWEVHZFFZDPOVEEYJZPTR
EISBXYYYBYPHTYTAIAVWPJYMAIIGSJEMYURFMGXVLFNXWBQGZPTMXWRJFTZFWGNUJGEDYZBKAXECSHMAPTNXD
IRNHOIPVPUNXNIPOHLPPUSLLSWDRFCDZRIIWIGNDAROFQWVCXLUPHJKGDCTHETNDZGQW

Ciphertext 3

IALVBQTIJDXJUDGFJTYZGNADIJIUHCUHNQDGTKGSIYBQNRAADFQJDVBAGPJBHHARTXRLUSHMLPGJCCLLLIRGBMDX
BVIEELBYLAMRJFYSKOEGSCUMTSYVBKYOUGXJCNWUJAWJHYTAPQMIZFRBISVJHRWOXUYCIDUOPTKPDIBLPNLBLSB
GOHLPIZOKNSJTQMUEGBMQFGCIYVJBWTADUXZBSBPAKGAYEURCJRMVKEBGDUPNQGEAQISTCOAHOOGNGVLNJX
KQZYGWHFPAEOXAQBKZOKERXNBBONYWOMPBZXONEKBIXFGNSTLMUYCNPZQVWXSWWSKUAZZWDSGYOSVPRN
UPSHZCPTZDNPMOTTFKCXJBNLYRBMEBJMWBNYXKRKHJLAJOGQDHAHNVDIMQRXPZGLMHHTPRZSZEXYMURXOYC
LLBGXUTEKRJARZMDUPIZZWTNDHSRAIZWKSKPIRCVIIPAWEHNTAKIWOMGUGYYQZWRPTMULGWTOLRIJOREOMF
UKAXQVEBADYXRMFQLGQSRQEZESRTMJMADBATJTUMCFOXAPJOKRXUGZTQNMWNPNSAXATXZFXCWHMOFCPAC
CDBLRVKFYDEKPYQTIKQQDPQGZENWUNBSUBQLHPKWXYMWNAESEDLSIKFMJSPAMXBPQQNSCHRYVNAHPBYNPF
DRDVNOIOAFUOKHZSYUTTHALPDVXAQTAGFXUETTSPBNMEUCFVJWDTCYZHMNNEVBYESVWRZZUXFQQMPXZVOK
SLYFOLUKZAEYKIQHKAHETGDDCMGXWHLRPJKFJMHUKEXGFAXKIXLKJQPSMFNYTIDNDNOVBFXTLZFANGFDXMBMN
FSRZSZPWBMBTZSWZLDMMWLUMHCLIHKROLULWCHCNFPUJWRDBRAVPDHLNBWFXUELNXHXSLAZPJJCZKRXYTLX
LWWLRIAMKLZHZRGWIZLXGZKDFPVTRGTC

Ciphertext 4

FULDQYOBJCEQPSDHNLYLYBOXOIIFJCLHJLCIBBZKJBDIPLGMDTRIQRLZIXJVCQJXFJZVVHBVLNNKDWKFRKVDMVQEIG
MTAQVZQYCGVEMNWTQGBBCASKZHMFDUUYVPAXNJMVVVFCGRRPDNHLVMQJLKLRAIWWYBQWYBXNNQYDAXQ
PCHEDDTEKBOEPUDOBMYDYGNPXJIXEBYLTUIMGNTJNISDAGOQEPBZUNAPFPRXFSUWTOQYZLZUHTHZNOCRWWP
CJQBMACNXFINPNDHOTQQFCEQDZBRREZSJIXNVGFJMHGKEVGVKTQQAZGOENOTJZUPWGHKDSGDHAHFHHTURJD
PDDHIHWEMOBGHWHQGCJXSOGGUPQNCTWUDIFJRXCNHABXOTJFORNMIFBPZRNRPSLBTDNMFONQDFQSYNLW
WLEUTCUTSHTRKAKMVNWTGQALUADQHZGDHKCNTFVBXWLMQIQMCOPVHIXOGUJIFIOFTRKRWO

Alphabet original

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	0	1	2	3	4	5	6	7	8	9

Clé 1 de permutation de l'alphabet →

← rang dans l'alphabet original

← marques pour tracer l'avancement dans le processus de permutation

Alphabet permuté pour les **Lignes** de la Table de Chiffrement

caractère																																				
	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	27	28	29	30	31	32	33	34	35	36
	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	0	1	2	3	4	5	6	7	8	9
rang																																				

Alphabet original

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	0	1	2	3	4	5	6	7	8	9

Clé 2 de permutation de l'alphabet →

← rang dans l'alphabet original

← marques pour tracer l'avancement dans le processus de permutation

Alphabet permuté pour les **Colonnes** de la Table de Chiffrement

caractère																																				
	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	27	28	29	30	31	32	33	34	35	36
	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	0	1	2	3	4	5	6	7	8	9
rang																																				

Permutations de l'Alphabet Étendu

	,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$

compter dans ce sens pour la permutation ←

37	**38**	**39**	**40**	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**	**50**	**51**	**52**	**53**
	,	**.**	**(**	**)**	**+**	**-**	*****	**/**	**^**	**<**	**=**	**>**	**%**	**€**	**£**	**$**

	,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$

compter dans ce sens pour la permutation ←

37	**38**	**39**	**40**	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**	**50**	**51**	**52**	**53**
	,	**.**	**(**	**)**	**+**	**-**	*****	**/**	**^**	**<**	**=**	**>**	**%**	**€**	**£**	**$**

Annexe G2

Table de Chiffrement

Spirale (Ph.Allard)

lettre de la CLÉ 4 ou du MASQUE

□	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	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$
nouveaux rangs →																																																						
↓ lettres	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	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	52	53
┌ → ↓→																																																					

lettre de la CLÉ 3 ou du TEXTE CLAIR

A	1	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	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$
B	2	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	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A
C	3	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B
D	4	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C
E	5	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D
F	6	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E
G	7	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F
H	8	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F	G
I	9	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F	G	H
J	10	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F	G	H	I
K	11	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F	G	H	I	J
L	12	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F	G	H	I	J	K
M	13	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F	G	H	I	J	K	L
N	14	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F	G	H	I	J	K	L	M
O	15	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	16	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	17	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	18	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	19	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	20	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	21	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	22	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	23	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	24	X	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	25	Y	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	26	Z	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	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
0	27	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	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
1	28	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	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	0
2	29	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	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	0	1
3	30	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	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	0	1	2
4	31	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	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	0	1	2	3
5	32	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	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	0	1	2	3	4
6	33	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	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	0	1	2	3	4	5
7	34	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	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	0	1	2	3	4	5	6
8	35	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	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	0	1	2	3	4	5	6	7
9	36	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	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	0	1	2	3	4	5	6	7	8
	37		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	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	0	1	2	3	4	5	6	7	8	9
,	38	,	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	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	0	1	2	3	4	5	6	7	8	9	
.	39	.	(	)	+	-	*	/	^	<	=	>	%	€	£	$	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	0	1	2	3	4	5	6	7	8	9		,
(	40	(	)	+	-	*	/	^	<	=	>	%	€	£	$	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	0	1	2	3	4	5	6	7	8	9		,	.
)	41	)	+	-	*	/	^	<	=	>	%	€	£	$	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	0	1	2	3	4	5	6	7	8	9		,	.	(
+	42	+	-	*	/	^	<	=	>	%	€	£	$	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	0	1	2	3	4	5	6	7	8	9		,	.	(	)
-	43	-	*	/	^	<	=	>	%	€	£	$	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	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+
*****	44	*	/	^	<	=	>	%	€	£	$	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	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-
/	45	/	^	<	=	>	%	€	£	$	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	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*
^	46	^	<	=	>	%	€	£	$	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	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/
<	47	<	=	>	%	€	£	$	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	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^
=	48	=	>	%	€	£	$	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	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<
>	49	>	%	€	£	$	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	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=
%	50	%	€	£	$	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	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>
€	51	€	£	$	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	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%
£	52	£	$	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	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€
$	53	$	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	0	1	2	3	4	5	6	7	8	9		,	.	(	)	+	-	*	/	^	<	=	>	%	€	£

Alphabet : ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 ,.:’'"()+-*/^<=>&@%€£$

Texte clair* : SPIRALE is a one-time pad cryptosystem designed in 2015/05 to replace SOLITAIRE when one has no cards. It is based in parts on the generalized Fibonacci sequence xn = xn-49 * xn-24. As it is free it costs nothing (0 €). It also allows to express chemical formulas: FeS2 + O2 -> Fe2O3 + SO2.

* comme il n'y a pas de symbole de fin de ligne dans cet alphabet, le texte clair doit être sur une seule ligne continue.

Clés : NVIKKIH CTSQEOU DNGDKSZ EAIWDSH

Alphabet permuté 1 : +XOD='7S&"3QG€,J£’0NC:H<6RA-V9U%5M@Y1E8B KW$2)^L4I*(PZ/>T.F

Alphabet permuté 2 : € RA&.PM/1HC"SN+W%^3£=X*YO)JF2(LD5,7’>G<I$'6VQ-8:0UE9BK@TZ4

Texte chiffré* : DY2R"S7->EQFS@MT&1T@X%*"AHE:9QR@F@@TDT€£0DECK$N"'NO8>P:E£*H0 X’C 4FI7YC693&=&-
£.K^.A72J*.O’RG)(S820XX<YX/U(€PQWCN/,GL(5XE75"PNEP,7ILC£U:- ,-D5R9,€U5+V£CE"RQ"PW2/ ",V"NJ+-'>H5"7OUK:=@6V:€3’)(O€%£C9"
>^&,46C'N70$3"X'78LY+FU@=W(O8^*$-VF1L6TOV<OY3KO^I<OAOD/&(*<@(<P5S:8 3^€8"/7.B",9VM0BA*9',O=’

* le texte chiffré se retrouve lui aussi sur une seule ligne.

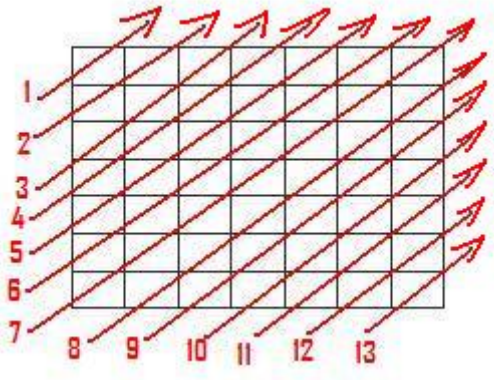
```
PythonWin 3.4.1 (default, Aug  7 2014, 13:13:27) [MSC v.1600 32 bit (Intel)] on win32.
Portions Copyright 1994-2008 Mark Hammond - see 'Help/About PythonWin' for further copyright information.
>>>   -- SPIRALE 2.1  -- Cryptosystem for text with Letters, Numerals and Typographic
characters according to selected alphabet --

- Encryption process from keys (NVIKKIH|CTSQEOU|DNGDKSZ|EAIWDSH) and alphabet
[ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 ,.:''"()+-*/^<=>&@%€£$] -

Permutation of alphabet according to following ranks : [14, 22, 9, 11, 11, 9, 8]  for
NVIKKIH:
Permuted Alphabet (59 characters) = +XOD='7S&"3QG€,J£'0NC:H<6RA-V9U%5M@Y1E8B
KW$2)^L4I*(PZ/>T.F
the permuted alphabet is in file NVIKKIH.txt

Permutation of alphabet according to following ranks : [3, 20, 19, 17, 5, 15, 21]  for
CTSQEOU:
Permuted Alphabet (59 characters) = €
RA&.PM/1HC"SN+W%^3£=X*YO)JF2(LD5,7'>G<I$'6VQ-8:0UE9BK@TZ4
the permuted alphabet is in file CTSQEOU.txt

['@', 'G', '(', 'T', '9', 'Q', 'N']
['L', 'W', 'A', '9', '=', '6', '3']
['E', 'P', '>', '2', ')', 'Z', 'W']
['@', 'G', '(', 'T', '9', 'Q', 'N']
['7', ')', 'W', '£', 'O', '@', '=']
['$', 'K', '*', 'X', ':', 'U', 'R']
['+', '€', '8', 'K', '0', 'H', 'E']
Generated Long Key (49 characters) = @LGEW(@PAT7G>99$)(2=Q+KWT)6N€*£9Z38XOQWK:@N0U=HRE

Keystream (290 characters) =
@LGEW(@PAT7G>99$)(2=Q+KWT)6N€*£9Z38XOQWK:@N0U=HREB50,GM1<+)2,'+Y6'G8@6K(8<TO&=£ZJJ
I9)0HZENHOO$>NR £W965E<B0,'@K7QTWEAGTG'YRSB*^+@J4YG'N£:89OF''8%^"3
>"*7<."">A/C@$^IGD/)39*)IRDK9OUBNPN4MD€K'5Z(£YK9<"2E(5O=XC'&1H('0+BZG8Y(ZC@@MD1=C43X£(7%56
0=4EAM18F')Y'XPA::2H£J.C^B>E'"B'/LB£+$KX,$40M7 ("M'
the keystream sequence of characters is also in file keystream.txt

The generated ciphertext is in 'ciphertext.txt'.

Plaintext: SPIRALE IS A ONE-TIME PAD CRYPTOSYSTEM DESIGNED IN 2015/05 TO REPLACE
SOLITAIRE WHEN ONE HAS NO CARDS. IT IS BASED IN PARTS ON THE GENERALIZED FIBONACCI
SEQUENCE XN = XN-49 * XN-24. AS IT IS FREE IT COSTS NOTHING (0 €). IT ALSO ALLOWS TO
EXPRESS CHEMICAL FORMULAS: FES2 + O2 -> FE2O3 + SO2.

Ciphertext: DY2R"S7->EQFS@MT&1T@X%*"AHE:9QR@F@@TDT€£0DECK$N"'NO8>P:E£*H0 X'C
4FI7YC693&=&-£.K^.A72J*.O'RG)(S820XX<YX/U(€PQWCN/,GL(5XE75"PNEP,7ILC£U:-
,-D5R9,€U5+V£CE"RQ"PW2/ ",V"NJ+-'>H5"7OUK:=@6V:€3')(O€%£C9"
>^&,46C'N70$3"X'78LY+FU@=W(O8^*$-VF1L6TOV<OY3KO^I<OAOD/&(*<@(<P5S:8
3^€8"/7.B",9VM0BA*9',O='

>>>
```

PARCOURS DE RELÈVEMENT D'UN TABLEAU

Plan

1. introduction

Dans la notice décrivant le chiffre Spirale[1], nous avons eu à aborder le problème du relèvement d'un tableau. Il s'agissait alors de lire dans un certain ordre les valeurs d'un tableau de 7x7 cases. Nous avions alors opté pour un parcours en diagonales, pour éviter les éventuelles répétitions horizontales ou verticales dues au procédé de remplissage, ascendantes et commençant à l'angle supérieur gauche :

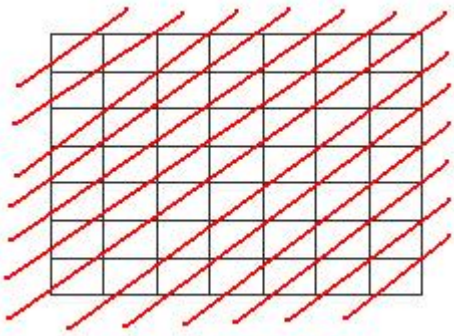


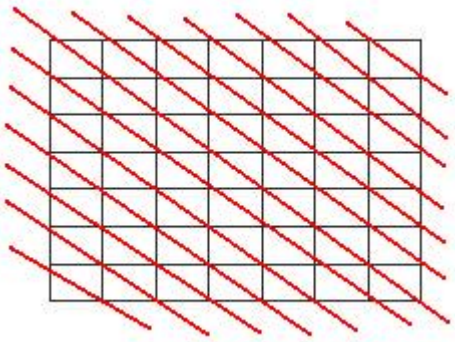
Nous avions signalé le caractère arbitraire et simple de ce choix et mentionné la possibilité d'autres solutions. Nous approfondissons ici tout le champ du possible en conservant toute fois l'option de la diagonale et la taille du tableau.

[1] Spirale – Un chiffre à masque jetable, 2015.

2. Orientation des diagonales

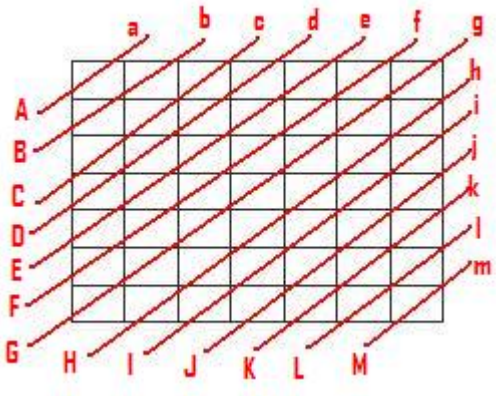
Deux possibilités seulement existent :



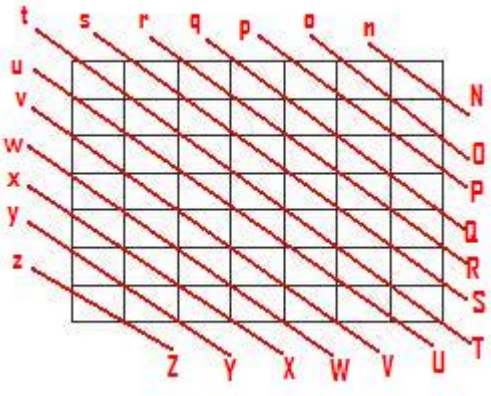


3. Repérage des lignes

À partir des deux orientations possibles, nous définissons deux réseaux que nous notons A et N en fonction des lettres attribuées à la première ligne de chaque réseau :



Réseau A



Réseau N

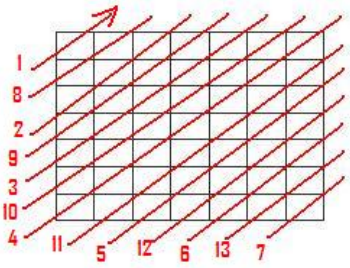
Une ligne peut être parcourue dans deux sens possibles : ascendant ou descendant. Elle est alors désignée différemment pour indiquer ce sens : en majuscule pour le sens ascendant et en minuscule pour le sens descendant. Par exemples : C pour la ligne allant de C à c, q pour la ligne allant de q à Q.

4. Description des parcours

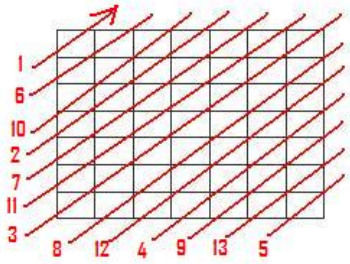
Un parcours doit passer par toutes les cases du tableau, une fois et une seule. Il ne peut donc s'appuyer que sur un seul des réseaux A ou N. Comme il est constitué d'une séquence de lignes parcourues dans un des 2 sens possibles, nous le décrirons par la suite des lettres désignant chaque ligne avec son sens de parcours. Ainsi le parcours standard de Spirale est noté ABCDEFGHIJKLM.

5. Exemples de parcours

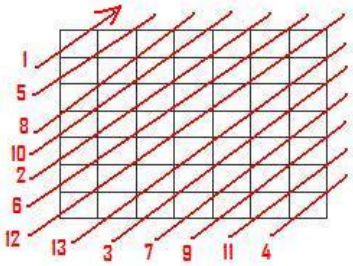
Notre convention de notation permet de désigner simplement et sans ambigüité n'importe quel parcours (les numéros dans les figures indiquent au préalable l'ordre séquentiel du parcours) :

- Ascendant, espacé d'une ligne 

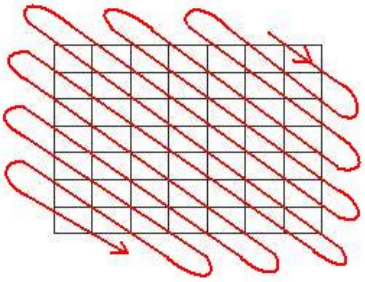
ACEGIKMBDFHJL

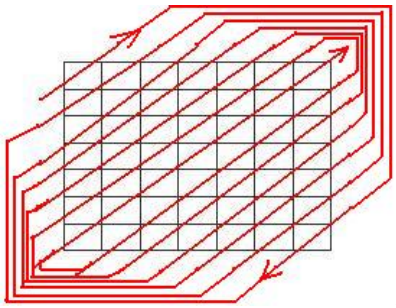
- Ascendant, espacé de 2 lignes 

ADGJMBEHKCFIL

- Ascendant, espacé de 3 lignes 

AEIMBFJCKDLGH

- Descendant, sinueux adjacent 
nOpQrStUvWxYz

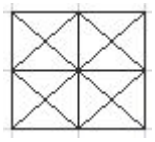
- Spirale convergente 
AmBlCkDjEiFhG

6. Dénombrement des parcours

Il y a 2 réseaux exploitables. Dans chaque réseau il y a 13 lignes, cela fait donc 13 ! = 6 227 020 800 séquences possibles. Pour une séquence, chaque ligne peut être parcourue dans 2 sens possibles que nous avons exprimés par majuscule et minuscule mais que nous pourrions aussi exprimer par un masque de 13 digits binaires : 0 pour une minuscule et 1 pour une majuscule. Ainsi la séquence orientée AmBlCkDjEiFhG est la conjonction de la permutation AMBLCKDJEIFHG et du masque de sens 1010101010101. Présenté ainsi le problème devient très clair : pour chaque choix de lignes il y a 2^{13} = 8 192 combinaisons des sens de parcours. En résumé, en se limitant à des segments orientés diagonaux, il y a 2 x 13 ! x 2^{13} ≈ **10^{14}** parcours possibles pour relever le contenu des cases du tableau 7x7.

7. Applications

- *Chiffre Spirale* : Spirale a déjà 4 degrés de liberté avec les 4 clés de 7 caractères produisant une richesse combinatoire équivalente à celle d'un chiffre à 128 bits. Si nous introduisons un $5^{ème}$ degré avec un changement systématique du parcours de lecture de la matrice donnant la séquence amorce alors cela entraîne un accroissement considérable de la variabilité combinatoire de Spirale allant jusqu'à 46 bits supplémentaires. Au minimum nous pouvons faire usage, contre la cryptanalyse, de ce degré supplémentaire de liberté en affectant à chaque utilisateur un ou plusieurs parcours exclusifs qui joueraient le rôle de *sel* ou signature. Cela dans un contexte de correspondance secrète entre des agents et une autorité qui les supervise et qui a connaissance de ces sels personnels.
- *Chiffrement par transposition* : la classique méthode de transposition par permutation des lignes et colonnes autorise, toujours dans le cas de notre tableau 7x7, un nombre de combinaisons égal à 7! x 7! = 25 401 600. Il est très inférieur à celui (10^{14}) obtenu en cheminant en diagonal. Nous voyons donc tout l'intérêt qui l'y aurait à utiliser ce mode de parcours. Le problème pratique étant alors de générer, simplement et le plus pseudo-aléatoirement possible, les séquences de majuscules et minuscules décrivant le parcours et jouant le rôle de clés.



DIAGONALES

Un chiffre par transposition

Plan

1. Introduction

Dans un document précédent [1], nous avons esquissé tout le bénéfice combinatoire que l'on peut tirer du parcours généralisé en diagonales dans un tableau pour en lire ou permuter les éléments. Nous développons ici en détails ces idées pour bâtir progressivement un nouveau système de chiffrement manuel, par transposition, que nous appelons *Diagonales*. Il n'est pas conçu pour être aussi sophistiqué et résistant que Spirale [2] mais d'une mise en œuvre bien plus rapide. Si Spirale a plutôt vocation à être le système manuel de chiffrement de secours d'une correspondance secrète durable (diplomatique ou militaire) à protéger fortement, *Diagonales* est prévu pour des messages courts (de moins de 50 caractères) à durée de validité assez courte typique des ordres du champ de bataille ou des consignes internes à un réseau clandestin.

2. Transposition par relèvement en diagonales

Nous travaillons sur un tableau 7x7, d'où le maximum de 49 caractères. Nous illustrerons chaque étape sur l'exemple suivant :

Une attaque simulée aura lieu demain matin à quatre heures

Le texte à chiffrer est d'abord rangé ligne par ligne dans un tableau 7x7, les éventuelles dernières cases vides étant remplies par des lettres quelconques dans le plus grand hasard possible. Les espaces et signes de ponctuation doivent être supprimées, et les lettres accentuées remplacées par les même sans accent.

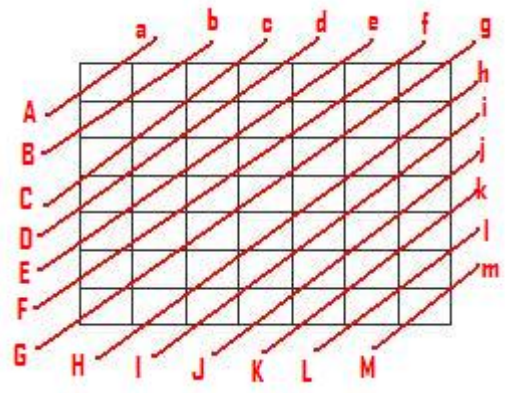
D'où le tableau suivant :

u	n	e	a	t	t	a
q	u	e	s	i	m	u
l	e	e	a	u	r	a
l	i	e	u	d	e	m
a	i	n	m	a	t	i
n	a	q	u	a	t	r
e	h	e	u	r	e	s

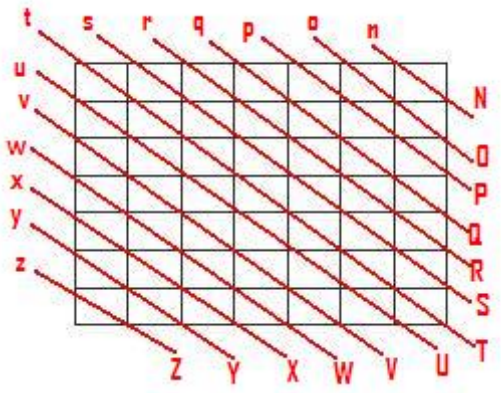
Table du texte clair

Nous savons déjà par [1] qu'un parcours en diagonal quelconque, parmi les 2 x 13! x 2^{13} ≈ **10^{14}** possibles, permet de lire les lettres de ce tableau. À la différence du procédé classique par permutation des lignes et colonnes, les lettres voisines sur une même ligne se trouveront alors dispersées de manière irrégulière qui mettra en défaut la méthode classique de cryptanalyse par recherche des bigrammes et trigrammes les plus fréquents dans la langue.

Par [1] nous savons qu'un parcours diagonal repose sur :



Réseau A



réseau N

- Le choix d'un des 2 réseaux A ou N de diagonales ;
- Une permutation des 13 lignes A…M ou N…Z de ce réseau ;
- L'orientation de chacune de ces lignes, indiquée par la majuscule ou la minuscule.

Toutes ces informations étant exprimées et condensées, selon la convention décrite dans [1], en une chaîne de lettres de la forme XpTyruVoqWNZs, par exemple pour le réseau N. La majuscule signifiant le sens ascendant et la minuscule le sens descendant. C'est cette suite de lettres qui est la véritable clé du chiffre par transposition. Elle est représentée sur la figure suivante où le chiffre en bleu indique l'ordre séquentiel de parcours des segments :

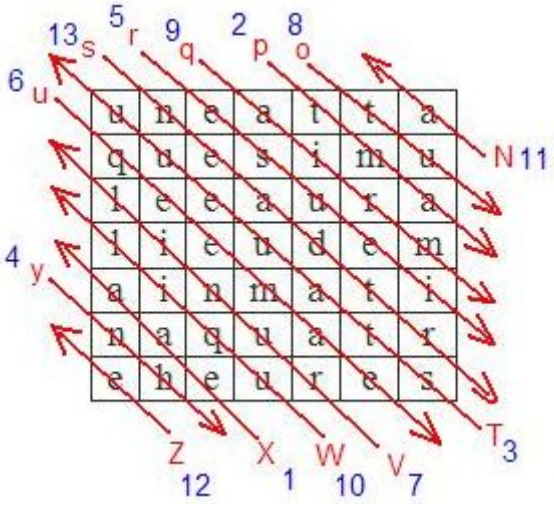


Schéma ordonné des segments orientés

Ce parcours se lit ainsi : 1er segment X (ascendant), 2ème segment p (descendant), 3ème segment T (ascendant), etc. Cela donne les lectures suivantes :

eaa tma staueuu nh esuei qeemae runil tu airm uqil a e neadtr

et finalement la transposition suivante du message initial :

EAATMASTAUEUUNHESUEIQEEMAERUNILTUAIRMUQILAENEADTR

Une suite descriptive telle que XpTyruVoqWNZs, malgré sa complexité, si elle était utilisée de manière très répétitive pourrait être percée. Alors que l'usage systématique d'une clé différente pour chaque message permet de tirer profit du grand nombre de combinaisons possibles $2 \times 13! \times 2^{13} \approx 2^{46,5}$. Cette quasi-égalité arithmétique signifie que le chiffre par transposition Diagonales est équivalent, d'un point de vue combinatoire, à un chiffre de 46 bits.

Le problème pratique, pour exploiter cette richesse combinatoire, est de concevoir une méthode de construction de l'ensemble des suites descriptives des parcours diagonaux. C'est cette méthode qui fait l'objet de la suite de cet article. Elle s'appuie sur l'usage de 2 clés K1 et K2, qu'il conviendrait plutôt d'appeler proto-clés car leur seul rôle est d'engendrer la clé

véritable : la séquence des segments orientés. Fonctionnellement le crypto-système Diagonales peut être décrit par le schéma suivant :

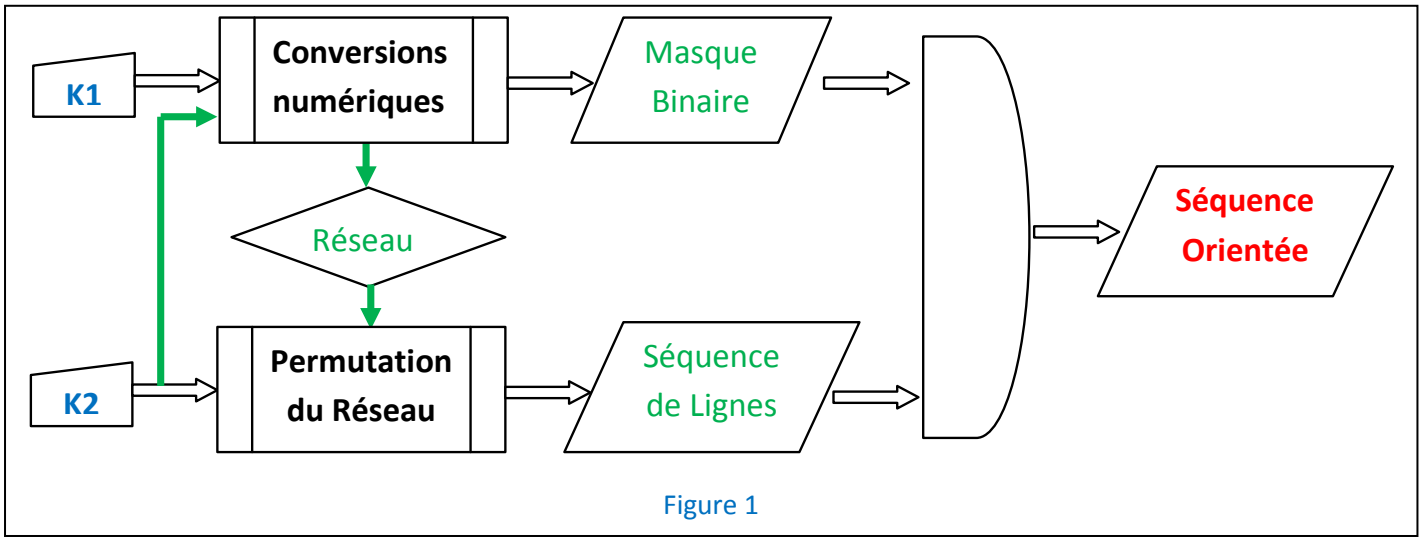


Figure 1

3. Choix du réseau

Ce choix est binaire, pour l'effectuer nous allons utiliser la parité d'un nombre que nous allons construire et qui servira ultérieurement et principalement pour définir le *masque binaire* d'orientation des lignes.

Par [1] nous savons déjà qu'il y a 2^{13} = 8192 combinaisons possibles de valeur du masque. Pour les atteindre il suffirait de tirer aléatoirement un entier compris entre 0 et 8191. C'est ce que nous allons faire mais en travaillant non pas en système décimal mais en système hexadécimal [4]. En effet nous pouvons écrire 13 = 1 + 3x4, ce qui signifie que 3 groupes de 4 bits apportent l'essentiel du nombre. Le $13^{ème}$ bit sera déterminé plus loin. D'autre part un groupe de 4 bits prend les valeurs comprises entre 0 et 15 qui sont représentées en base 16 par les caractères 0, …, 9, A, B, C, D, E, F.

L'idée est donc de disposer au départ d'une suite pseudo-aléatoire K1, de 3 chiffres hexadécimaux, jouant le rôle de clé. Cette clé pouvant, par exemple, être créée personnellement par une procédure comme celle décrite dans [3].

Pour le choix du réseau nous ferons, simplement et arbitrairement, le compte des bits 1 dans les 3 groupes. Si le nombre est impair nous choisissons le réseau A. En fait il s'agit d'une fonction de hachage simplissime sur l'ensemble des 12 bits, d'autres fonctions pourraient aussi convenir.

Finalement, la sélection d'un réseau suit les étapes suivantes :

- à partir d'une clé K1 = $H_1H_2H_3$
- conversion des chiffres H_i en binaire
- décompte du nombre total n de bits 1

- si n est impair alors choix du réseau A sinon choix du réseau N

L'annexe A illustre ces étapes sur un exemple :

- clé K1 = 44C
- séquence binaire [0100 0100 1100]
- n = 4
- réseau N : NOPQRSTUVWXYZ

4. Permutation des lignes

Ayant 13 lignes à permuter cela offre 13! = 6 227 020 800 séquences de 13 lettres distinctes, pour les permuter nous appliquerons le même algorithme tournant que celui utilisé dans Spirale pour permuter les alphabets. Cet algorithme est conditionné par la donnée d'une suite K2 de lettres choisies de manière quelconque parmi les 26 lettres de l'alphabet et jouant le rôle de clé. Dans notre cas actuel, quelle doit-être la longueur *n* de la clé pour offrir autant de combinaisons qu'il y a de permutations ou séquences ? il suffit de poser :

$$13! = 6\ 227\ 020\ 800 = 26^n$$

Cela implique n ≈ 6,92 et donc avec une clé de 7 lettres nous engendrerons un nombre de combinaisons équivalent à celui des permutations des 13 lignes.

Poursuivons notre exemple en adoptant la clé K2 = CTSQEOU. Après permutation (annexe B) cela donne la séquence XPTYRUVOQWNZS. Cette permutation a été effectuée en fonction des décalages [3,20,19,17,5,15,21] tirés du rang des lettres de la clé. C'est à partir de ces valeurs que nous déterminons le $13^{ème}$ bit : le reste modulo 2 de leur somme. Ici cela donne 100 et donc 0 (annexe A). Là encore il s'agit d'une fonction de hachage, de K2, simple à calculer et d'autres fonctions pourraient être adoptées.

5. Orientations des lignes

Nous disposons maintenant de l'ensemble des bits du masque des orientations. Nous avons placé le dernier défini tout à gauche (annexe A) par simplicité, mais nous pourrions lui attribuer n'importe quel autre emplacement et définir ainsi autant de variantes du chiffre. Pour choisir l'orientation des lignes nous adoptons une convention : si dans ce masque le bit de rang i est égal à *1* (respectivement *0*) alors dans le réseau permuté la ligne de rang i sera désignée par une *majuscule* (respectivement une *minuscule*) qui signifie qu'elle est parcourue dans le sens *ascendant* (respectivement *descendant*).

Ainsi le masque 0010001001100 appliqué au réseau permuté XPTYRUVOQWNZS donne le descriptif xpTyruVoqWNzs de la séquence de segments diagonaux orientés à emprunter pour parcourir le tableau.

Finalement l'action des clés est croisée : K1 définit essentiellement le masque d'orientation et parallèlement le réseau de lignes diagonales, K2 définit intégralement la permutation de ce réseau et très partiellement l'orientation de celui-ci. Ce choix d'interaction croisée est voulu pour compliquer la tache des cryptanalystes et contrer les recherches indépendantes des deux clés.

6. Mise en œuvre du chiffre

Nous avons détaillé dans l'annexe C les différentes étapes, courtes et rapides, du chiffre. La ligne *permuté* est destinée à recevoir les marques d'avancement du processus de permutation à partir des lettres de K2. La ligne *relevé* sert à marquer l'avancement du processus de relèvement du tableau à partir des lettres du descriptif. Les traits pleins et déliés tracés sur le tableau matérialisent les sens de parcours. Pour guider l'utilisateur dans le repérage des diagonales et de leurs sens, nous avons porté en bordure du tableau les lettres indexes des deux réseaux. Aidé de ce modèle l'utilisateur peu entraîné ne nécessite qu'une quinzaine minutes pour chiffrer un texte de 49 lettres.

Le processus de déchiffrement se fait naturellement en deux étapes :

- Construction du descriptif de la séquence de segments diagonaux orientés, de manière identique à la phase de chiffrement ;
- Remplissage du tableau, lettre par lettre, en lisant le texte chiffré de gauche à droite et en parcourant le tableau suivant la séquence des segments diagonaux orientés.

7. Défis

Pour inciter les cryptanalystes à briser ce chiffre nous proposons ici différents textes chiffrés correspondant à des situations affaiblissantes d'utilisation :

- Texte chiffré 1 : le texte clair contient une partie du texte de l'exemple
  ONURRUTNMEDEIEPLESATSIZAVIQUDVENEARUMAEOLARTDNREH

- Texte chiffré 2 : le texte clair est crypté avec les mêmes clés que le texte 1
  DEZREENLEAGTREVHAMSEAOGREIDURUNUOALULDSCQLSUAREEC

- Texte chiffré 3 : texte clair nouveau crypté avec deux nouvelles clés
  GTSLRAORSEELUTETISIEECSREVAETEHRMUCCRAIAAEEHETDRO

8. Extensions du chiffre

Pour chiffrer un texte long nous pouvons convenir de fractionner le texte en blocs de 49 caractères. Pour assurer une sécurité maximale il convient alors d'utiliser des clés K1, K2 différentes pour chaque bloc. Une solution rapide ne demandant pas de refaire les calculs pour chaque bloc consiste à effectuer une simple permutation circulaire de 3 ou 4 digits, dans un sens pour le masque et en sens inverse pour le réseau permuté, renouvelée à chaque bloc. L'annexe D en donne un exemple, pour limiter la taille du texte nous y avons appliqué certaines des conventions énoncées dans [5].

La solution alternative au fractionnement du texte est l'augmentation de taille du tableau. Pour un tableau carré de taille p, il y a 2.p-1 diagonales parallèles et donc (2p-1)! permutations de ces lignes. Augmenter la taille du tableau augmentera donc la richesse combinatoire de ce chiffre et sa résistance aux attaques par force brute. Mais dans la foulée il faut augmenter la taille des clés pour engendrer autant de combinaisons des lettres qu'il y a de permutations des 2p-1 lignes.

Il y a intérêt à ne travailler qu'avec des tableaux de taille impaire p = 2.k+1, en effet :

$$2.p-1 = 4.k+1$$

Signifie que nous pouvons étendre notre démarche des paragraphes précédents en prenant une clé K1 de k caractères hexadécimaux pour définir le réseau et son masque d'orientation. Le cas p = 13 est un bon compromis entre simplicité et puissance :

- Tableau 13x13 $2.p-1 = 25 = 4x6 + 1$ => clé K1 de 6 chiffes hexadécimaux
  $25! = 1{,}55.10^{25} = 26^{n}$ => n = 17,8 clé K2 de 18 lettres

La désignation des 25 lignes diagonales utilise la quasi-totalité de l'alphabet : A, …, Y. La distinction entre les 2 réseaux associés doit se faire maintenant par mention du coté *Gauch*e ou *Droit* du tableau d'où partent ces lignes. La désignation A…M ou N…Z du tableau 7x7 n'était due qu'à un heureux hasard : 2x7-1 = 13. Pour une taille supérieure à 13 il faut plus de 25 symboles pour désigner les lignes et nous pourrions adopter le principe de la numération de position en cumulant des digits littéraux : A, …, Z, AA, AB, …, AZ, BA, BB, etc. Cela permettrait de conserver la convention Majuscule-Minuscule pour indiquer le sens de parcours : ligne az descendante, ligne BA ascendante par exemples.

Dans tous les cas le principe du choix du réseau reste le même et seule sa formulation change légèrement :

- à partir d'une clé K1 = $H_1 \ldots H_k$
- conversion des chiffres H_i en binaire
- décompte du nombre total n de bits 1
- si n est impair alors choix du réseau à Gauche sinon choix du réseau à Droite

Les annexes E1 et E2 illustrent en détails l'application du chiffre au même texte long que celui de l'annexe D.

9. Références

1. Ph. Allard, Parcours de relèvement d'un tableau, 2015.
2. Ph. Allard, Spirale – un chiffre à masque jetable, 2015.
3. Ph. Allard, La création de clés, 2015.
4. fr.wikipedia.org/wiki/Système_hexadécimal
5. Ph. Allard, Conventions accessoires pour alphabet limité, 2015.

10. Annexes

A	Exemple
B	Algorithme de permutation : Exemple
C	Modèle d'utilisation
D	Exemple de plusieurs blocs
E1	Modèle d'utilisation 13x13 : Exemple
E2	Modèle d'utilisation 13x13 : Exemple

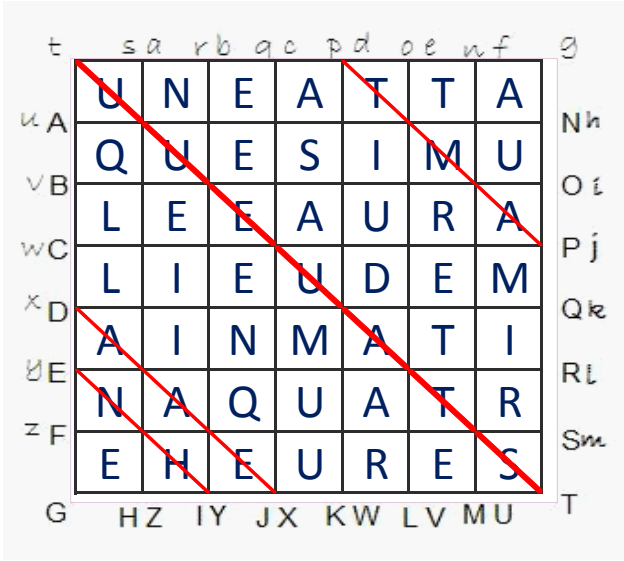
Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rang	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

clé K1		4			4			C						
Valeur$_2$		0100			0100			1100						
Masque	0	0	1	0	0	0	1	0	0	1	1	0	0	4

clé K2	C	T	S	Q	E	O	U	
Rang	3	20	19	17	5	15	21	100
permuté:	..	..	..	..	..	.	.	

Réseau	~~N~~	~~O~~	~~P~~	~~Q~~	~~R~~	~~S~~	~~T~~	~~U~~	~~V~~	~~W~~	~~X~~	~~Y~~	~~Z~~	réseau N
Permuté	X	P	T	Y	R	U	V	O	Q	W	N	Z	S	← annexe B
Masque	0	0	1	0	0	0	1	0	0	1	1	0	0	
Orienté	x	p	T	y	r	u	V	o	q	W	N	z	s	
relevé:	.	.	.	.										

Texte clair:	une attaque simulée aura lieu demain matin à 4 heures



sens ascendant

sens descendant

vérifier le nombre de lettres après le chiffrement

Texte Chiffré	AAE TMA STAUEUU NH …

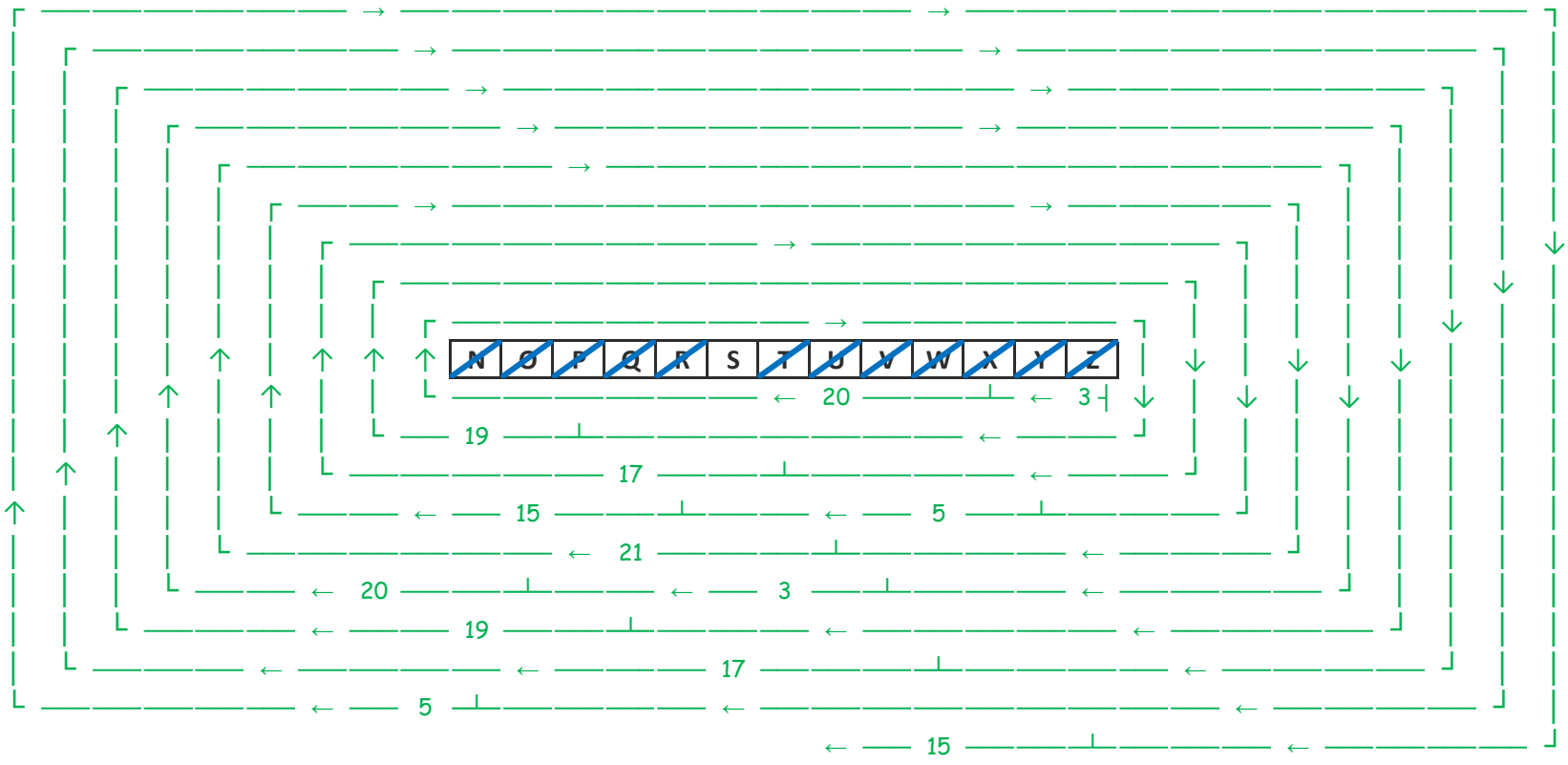
Clé K2 de permutation du réseau →

C	T	S	Q	E	O	U
3	20	19	17	5	15	21
..	..	..	..	..	.	.

← rang dans l'alphabet

← marques pour tracer l'avancement dans le processus de permutation

Réseau de base :



rayez la lettre dans le réseau de base quand elle est permutée, pour la sauter ultérieurement

Réseau permuté :

X	P	T	Y	R	U	V	O	Q	W	N	Z	S

Lettre	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
Rang	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

clé K1															
Valeur$_2$															
Masque															

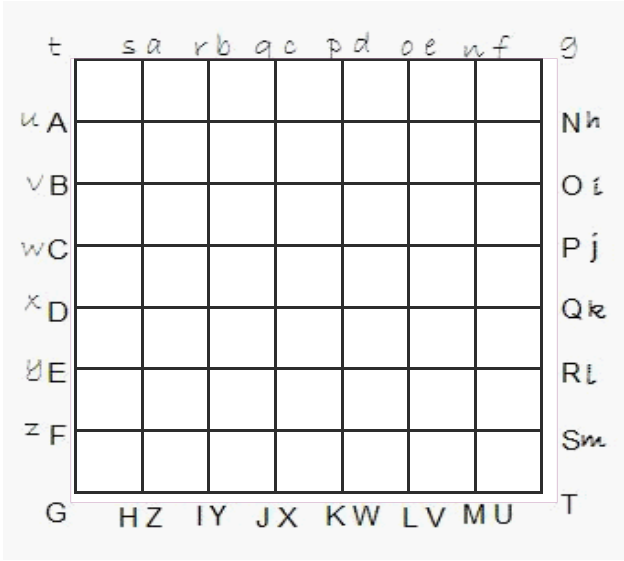
clé K2							
Rang							

permuté:

Réseau														
Permuté														
Masque														
Orienté														

relevé:

Texte clair:	

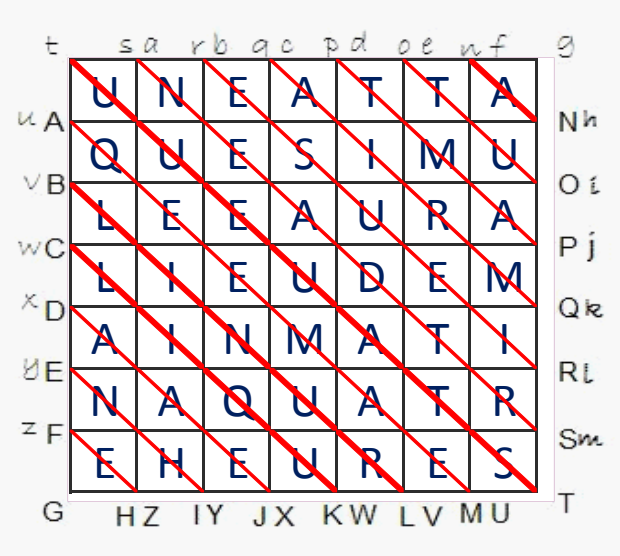


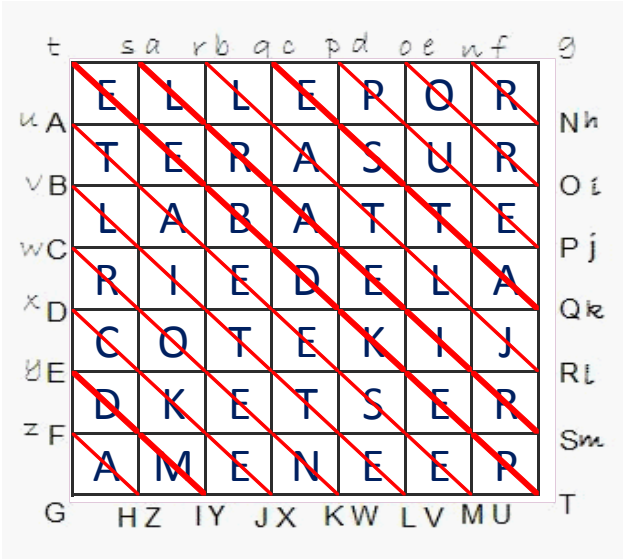
vérifier le nombre de lettres après le chiffrement

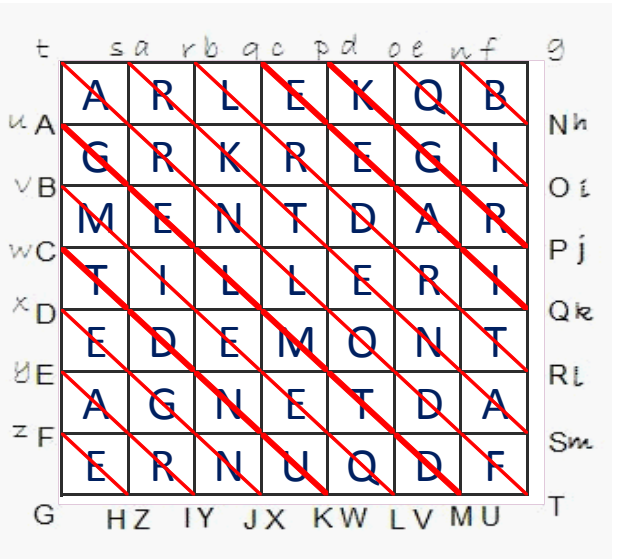
Texte Chiffré	

Texte Clair	une attaque simulée aura lieu demain matin à 4 heures, elle portera sur la batterie de la côte 904 et sera menée par le 27ème régiment d'artillerie de montagne

0010001001100	← 4 bits	0010011000010	0110000100010
xpTyruVoqWNzs	→ 3 lettres	nzSxpTYruvoQw	oQWnzsxPtyrUv







vérifier le nombre de lettres après le chiffrement

Texte Chiffré 1	AAETMASTAUEUUNHESUEIQEEMAERUNILTUAIRMUQILAENEADTR

Texte Chiffré 2	RARIEARLCKEPUEPEKDBEEMDLATLJTAEESELITTEORATSEROEN

Texte Chiffré 3	QIIAEEUNDTBERKTENAEGNRGKARNLODFARLRDRTDTMLEGMIEEQ

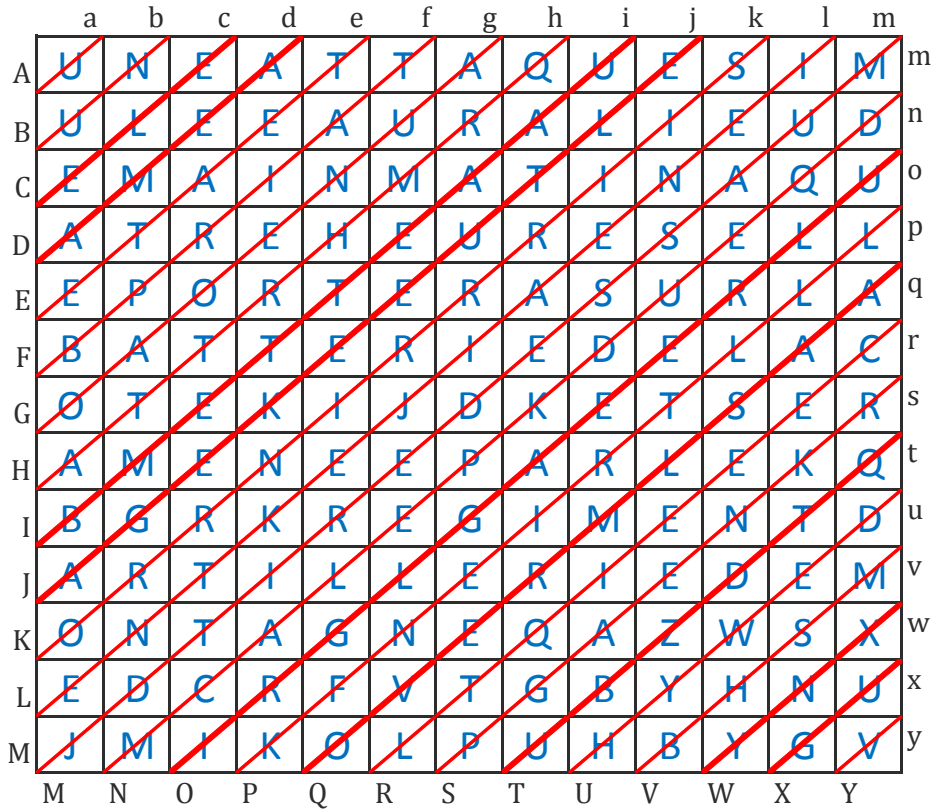
Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rang	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

clé K1		A				4				1				3				C				1				
Valeur$_2$		1010				0100				0001				0011				1100				0001				
Masque	0	1	0	1	0	0	1	0	0	0	0	0	1	0	0	1	1	1	1	0	0	0	0	0	1	9

clé K2	Y	Q	G	K	V	R	R	F	P	L	W	Z	F	E	O	E	Z	N	
Rang	25	17	7	11	22	18	18	6	16	12	23	26	6	5	15	5	26	14	258
permuté:	..	..	..	..	..	..	.	.	.	.	.	.	.	.	.	.	.	.	

Réseau	~~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~~	à gauche
Permuté	A	I	B	O	N	R	T	K	M	V	G	L	C	S	H	X	D	J	W	E	U	F	Y	P	Q	
Masque	0	1	0	1	0	0	1	0	0	0	0	0	1	0	0	1	1	1	1	0	0	0	0	0	1	
Orienté	a	I	b	O	n	r	T	k	m	v	g	l	C	s	h	X	D	J	W	e	u	f	y	p	Q	

Texte Clair	une attaque simulée aura lieu demain matin à 4 heures, elle portera sur la batterie de la côte 904 et sera menée par le 27ème régiment d'artillerie de montagne



Orienté	a	I	b	O	n	r	T	k	m	v	g	l	C	s	h	X	D	J	W	e	u	f	y	p	Q
relevé:	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Texte Chiffré	UBMETTEAAUNUIRGLGAEERLUDQEUDKPELACMCEEEIQTLUBZDTQSIIRRRINRROMUASSEDERITDJMSHBAUNEOAOIENEAIJEKTNEELERKNEAG PQRMHRTTAGUAMEAAGEKEEUTLEYNXTEATEDEWYHTAIRPBVLLLTRIENFKOVERMLSAA

CARROUSEL

Un chiffre par transposition

Plan

1. Introduction

Nous avons développé un algorithme tournant de permutation déjà utilisé, comme module interne, dans deux chiffres Diagonales [1] et Spirales [2]. Dans le premier cas il s'agit de permuter une courte chaîne de 13 lettres. Dans le second cas la chaîne peut être nettement plus longue car jouant le rôle d'alphabet elle peut atteindre, avec seulement des caractères latins, 26 caractères ou 36 avec les chiffres ou une soixantaine avec les caractères typographiques. Finalement, utilisé en soi, cet algorithme peut constituer le mécanisme unique d'un algorithme de chiffrement par transposition pouvant travailler sur un texte de longueur quelconque et rédigé dans un alphabet quelconque. Nous développons dans ce qui suit tous les aspects de ce système de chiffrement que nous appelons Carrousel.

2. Le chiffrement

Rappelons le processus de permutation : le texte est vu comme une liste circulaire de caractères sur laquelle nous nous déplaçons par sauts irréguliers[1], en commençant à l'extrémité finale. L'amplitude des sauts est définie par une suite d'entiers tirée d'une chaîne de caractères, jouant le rôle de clé, en substituant à chaque caractère son rang dans l'alphabet utilisé. Lorsqu'un saut aboutit sur un caractère du texte original, ce caractère est barré et est

[1] Comme le pompon présenté aux enfants sur un carrousel.

reporté à la fin d'une deuxième liste qui constitue ainsi progressivement le texte transposé. Si, dans le parcours, le caractère d'arrivée est déjà barré il faut le sauter et passer au suivant[2]. Un texte étant naturellement beaucoup plus long que la clé il faut parcourir celle-ci plusieurs fois jusqu'à épuisement de tous les caractères non barrés du texte : si le texte a n caractères et la clé p caractères alors la division euclidienne n = q.p + r signifie qu'il faut q cycles de parcours de la clé et utiliser encore une fois r caractères de celle-ci.

L'annexe A illustre un exemple complet emprunté au chiffre Diagonales. La dernière lettre de la clé (7 caractères) et du texte (13 caractères) n'ont pas été marquées pour manifester cette dernière étape. L'annexe B montre un état du processus inachevé de transposition d'un texte de 26 lettres par une clé de 5 lettres. Comme nous l'avons déjà signalé, l'algorithme Carrousel peut s'appliquer à n'importe quel alphabet. C'est ce que nous illustrons dans l'annexe C où un texte en Anglais de 82 caractères, écrit avec un alphabet de 36 caractères incluant les chiffres à sa fin, est partiellement transposé par une clé de 12 caractères, incluant de manière cohérente avec l'alphabet utilisé, des lettres et des chiffres.

Nous proposons cette feuille modèle pour l'exécution à la main du chiffre. Les textes clair et chiffré sont alternativement écrits ligne par ligne. Pour faciliter au lecteur le suivi du déroulement du processus de transposition, nous avons inscrit 3 informations au dessus de chaque caractère déjà transposé du texte clair :

- Le numéro de l'étape dans laquelle ce caractère a été sélectionné, reporté puis barré
- Le caractère de la clé, déterminatif du saut qui a abouti à ce caractère du texte clair
- L'amplitude du saut, déduit du caractère de la clé

3. Le déchiffrement

Nous illustrons son processus sur une autre feuille modèle, remplie cette fois-ci avec tout le texte chiffré (annexe D) : le texte clair est toujours vu comme une liste circulaire parcourue par sauts, mais le texte chiffré est lu de gauche à droite en commençant par l'extrémité initiale car c'est là que se trouve le premier caractère transposé. Ce premier caractère est reporté dans la liste, encore vide, du texte clair à l'emplacement défini, comme dans le chiffrement, par le premier caractère de la clé et le saut d'amplitude correspondante à partir de l'extrémité finale. Ce caractère est ensuite barré dans le texte chiffré et le caractère suivant à droite est traité de la même façon pour être reporté dans la liste du texte clair par un saut partant du caractère précédemment transposé, d'une amplitude définie par le 2ème caractère de la clé et dans le même sens de parcours. Le texte clair se remplit ainsi progressivement, par des caractères d'abord dispersés et isolés. Là encore, pour guider le lecteur, nous avons reporté au dessus de chaque caractère du texte clair les 3 informations caractéristiques de sa transposition. Toujours pour aider le lecteur, nous avons poussé dans l'exemple le processus de déchiffrement un peu plus loin que dans la phase de chiffrement.

[2] Ce n'est que justice, il ne faut pas présenter le pompon aux mêmes enfants !

4. Mise en œuvre du chiffre

Pour un usage personnel du chiffre nous donnons, en annexe E, la version vierge de la feuille modèle convenant indifféremment au chiffrement ou au déchiffrement. Un programme, écrit en Python, a également été développé et il est distribué librement. L'annexe F montre les résultats qu'il affiche dans le cas de notre exemple, d'abord au chiffrement puis au déchiffrement.

5. Défis

Pour inciter les cryptanalystes à briser ce chiffre nous proposons ici différents textes chiffrés correspondant à des situations affaiblissantes d'utilisation :

- Texte chiffré 1 : le texte clair, en Anglais, de 148 lettres de l'alphabet de base contient des partie du texte de l'exemple traité ;
- Texte chiffré 2 : le texte clair, en Anglais, de 124 lettres est crypté avec la même clé de 17 lettres que le texte 1 ;
- Texte chiffré 3 : texte clair, en Anglais, de 577 caractères pris dans un alphabet de 62 caractères et crypté avec une clé de 16 caractères.

Ces différents textes et l'alphabet enrichi sont donnés dans l'annexe G.

6. Extensions du chiffre

Elles ne s'exercent pas sur la longueur du texte ou la nature et la longueur de l'alphabet dont nous avons déjà dit et vu qu'elles sont quelconques. C'est avec la clé que nous allons jouer.

Changements de sens de parcours

La forme littérale de la clé est commode pour sa mémorisation ou sa transmission à un utilisateur, mais c'est sa conversion en nombres entiers qui est significative. Ils expriment l'amplitude des sauts, toujours effectués dans le même sens. Nous pourrions accepter aussi des sauts dans le sens rétrograde que nous exprimerions par une valeur négative. Ainsi la clé numérique [7, 22, -13, 5, -8] signifierait que, lors de son parcours cyclique, les $3^{ème}$ et $5^{ème}$ sauts seraient respectivement de 13 et 8 caractères dans le sens rétrograde de parcours de la liste circulaire du texte. Si nous voulons conserver la forme littérale de la clé, nous pouvons convenir d'utiliser les minuscules pour les sauts rétrogrades. La clé précédente s'écrirait alors GVmEh. Ces changements de sens de parcours du texte enrichissent considérablement la force du chiffre en lui donnant un caractère encore plus chaotique aux yeux des cryptanalystes.

Masque jetable

Jusque là nous avons utilisé des clés nettement plus courtes que le texte et qui devaient être parcourues plusieurs fois jusqu'à transposition complète de celui-ci. Mais nous pouvons aussi

envisager la même évolution conceptuelle qui a fait passer historiquement du chiffre de Vigenère (substitution poly-alphabétique) au chiffre à masque jetable : utiliser une clé de même longueur que le texte, de structure aussi aléatoire que possible et utilisée une seule fois. Nous créons ainsi un chiffre par transposition à masque jetable jouissant vraisemblablement de la même force que le chiffre par substitution à masque jetable.

Génération de clés

Dans le fonctionnement normal du chiffre et aussi du programme associé, les données fondamentales sont la clé et le texte. Si nous fixons la clé ainsi que le texte, par exemple 3 copies de l'alphabet utilisé, l'application du programme en mode chiffrement donne une permutation de ces caractères dans laquelle nous pouvons puiser un segment jouant ultérieurement un rôle de clé. Dans la pratique, pour augmenter le caractère pseudo-aléatoire de la chaîne permutée il faut exécuter plusieurs fois l'algorithme. Le programme associé à Carrousel a été facilement modifié pour accepter en donnée fondamentale le nombre de permutations à appliquer [3].

7. Références

1. Diagonales – un chiffre par transposition, 2015.
2. Spirale – un chiffre à masque jetable, 2015.
3. Création de clés, 2015.

7. Annexes

A	Exemple de transposition d'une chaîne courte
B	Exemple de transposition d'une chaîne longue
C	Chiffrement : Exemple détaillé
D	Déchiffrement : Exemple détaillé
E	Feuille modèle vierge
F	Résultat du programme : Exemple détaillé
G	Textes chiffrés des défis

Algorithme de Permutation : Exemple

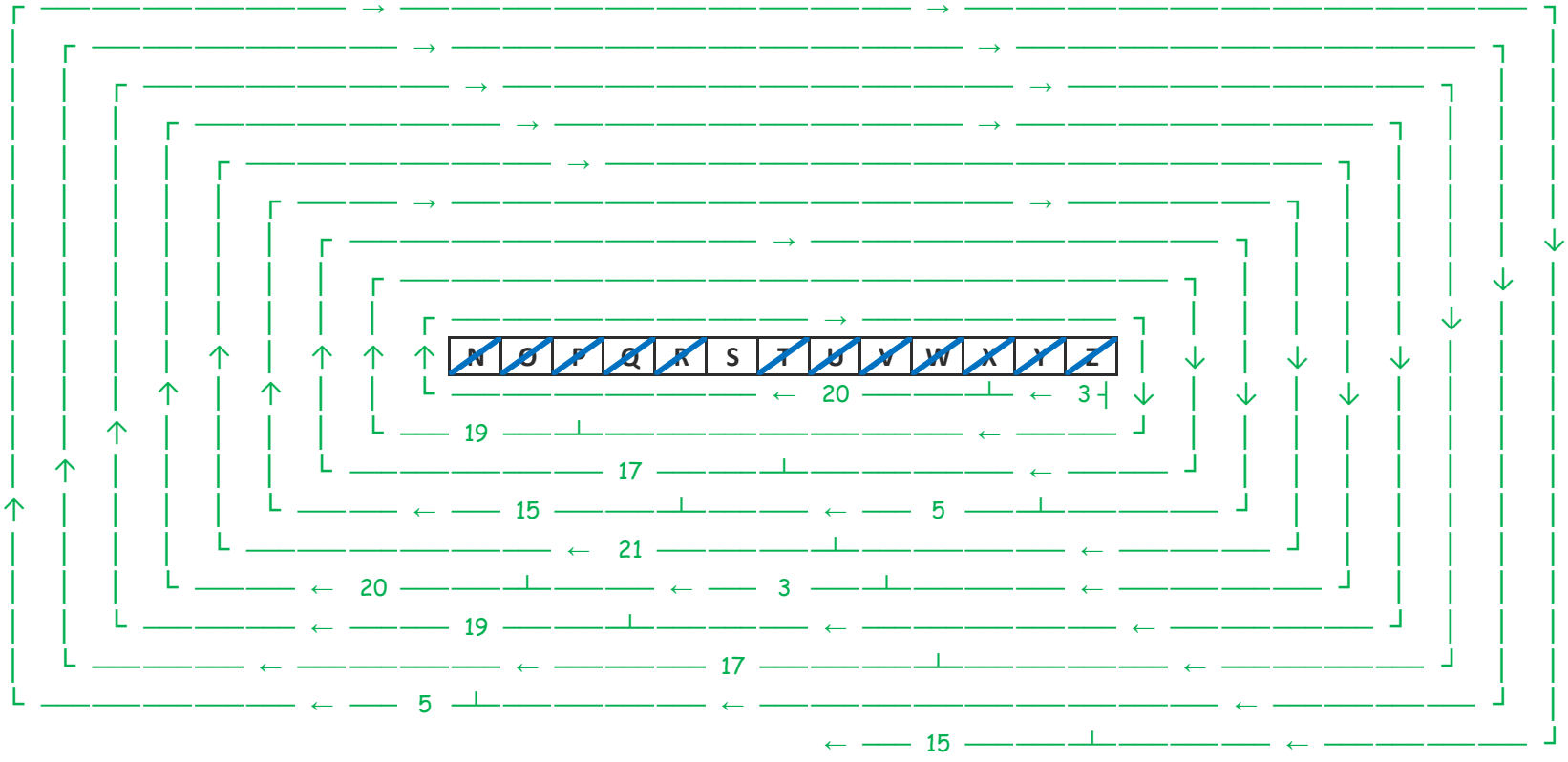
Clé K2 de permutation du réseau →

C	T	S	Q	E	O	U
3	20	19	17	5	15	21
..	..	..	..	..	.	.

← rang dans l'alphabet

← marques pour tracer l'avancement dans le processus de permutation

Réseau de base :



rayez la lettre dans le réseau de base quand elle est permutée, pour la sauter ultérieurement

Réseau permuté :

X	P	T	Y	R	U	V	O	Q	W	N	Z	S

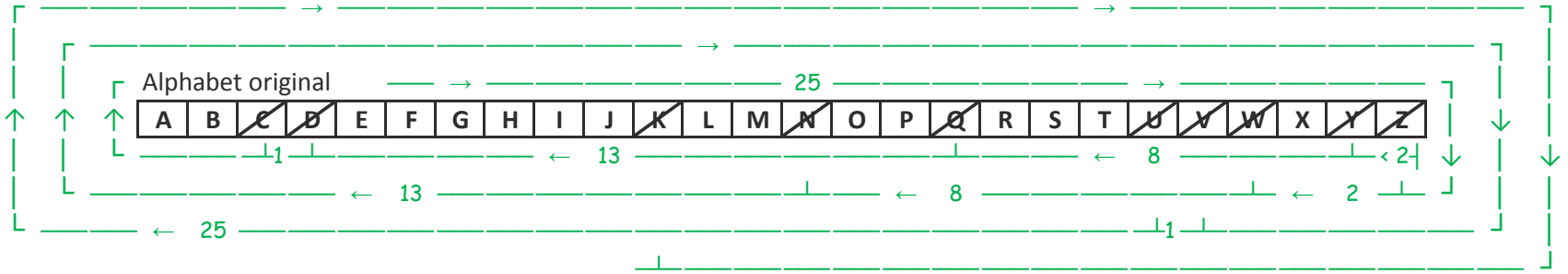
Algorithme de Permutation : Exemple

Clé de permutation de l'alphabet →

B	H	M	A	Y		
2	8	13	1	25		
..	..	..	..	..		

← rang dans l'alphabet original

← marques pour tracer l'avancement dans le processus de permutation



rayez la lettre dans l'alphabet original quand elle est permutée, pour la sauter ultérieurement

Alphabet permuté

Y	Q	D	C	Z	W	N	V	U	K														

J	A	M	E	S	B	O	N	D	0	0	7		
10	1	13	5	19	2	15	14	4	27	27	34		
..	..	..	..	.	.	.	.	.	.	.	.		

← clé de transposition

← rang dans l'alphabet

← marques pour tracer l'avancement dans le processus de transposition

↓ Texte Clair

			8 N 14														7 O 15				11 0 27			
C	A	R	~~R~~	O	U	S	E	L	I	S	A	C	R	Y	P	T	~~O~~	S	Y	S	~~T~~	E	M	D

↓ Texte Chiffré

F	O	Y	T	2	I	O	R	H	T	T	H	X	E	5	E									

↓ Texte Clair

					16 E 5		6 B 2		5 S 19			15 M 13												
E	S	I	G	N	~~E~~	D	~~I~~	N	~~2~~	0	1	~~5~~	T	O	T	R	A	N	S	P	O	S	E	A

↓ Texte Chiffré

10 0 27	14 A 1	13 J 10	4 E 5					3 M 13						12 7 37							2 A 1	1 J 10		
~~T~~	~~E~~	~~X~~	~~T~~	O	F	A	N	~~Y~~	L	E	N	G	T	~~H~~	B	Y	A	K	E	Y	~~O~~	~~F~~	A	N

↓ Texte Chiffré

↓ Texte Clair

						9 D 4																		
Y	L	E	N	G	T	~~H~~																		

↓ Texte Chiffré

↓ Texte Clair

↓ Texte Chiffré

↓ Texte Clair

↓ Texte Chiffré

↓ Texte Clair

↓ Texte Chiffré

↓ Texte Clair

↓ Texte Chiffré

J	A	M	E	S	B	O	N	D	0	0	7		
10	1	13	5	19	2	15	14	4	27	27	34		
..	..	..	..	..	..	.	.	.	.	.	.		

← clé de transposition
← rang dans l'alphabet
← marques pour tracer l'avancement dans le processus de transposition

↓ Texte Clair

			8 N 14				18 B 2		17 S 19								7 O 15				11 0 27			
			R				E		I								O				T			

↓ Texte Chiffré

F	O	Y	T	Z	I	O	R	H	T	T	H	X	E	5	E	I	E	Y	O	O	R	E	C	T

↓ Texte Clair

					16 E 5		6 B 2		5 S 19			15 M 13												
					E		I		2			5												

↓ Texte Chiffré

G	G	F	S	D	R	T	A	Y	S	N	A	E	N	E	E	A	0	L	A	M	R	N	E	S

10 0 27	14 A 1	13 J 10	4 E 5					3 M 13						12 7 34							2 A 1	1 J 10		
T	E	X	T					Y						H							O	F		

↓ Texte Chiffré

L	B	A	S	A	U	E	A	N	G	Y	K	Y	O	C	Y	S	T	N	S	O	T	T	1	P

↓ Texte Clair

						9 D 4																		
						H																		

↓ Texte Chiffré

D	I	N	N	L	S	P																		

↓ Texte Clair

↓ Texte Chiffré

↓ Texte Clair

↓ Texte Chiffré

↓ Texte Clair

↓ Texte Chiffré

↓ Texte Clair

↓ Texte Chiffré

Chiffrement ou Déchiffrement

																				←clé de transposition
																				←rang dans l'alphabet

←marques pour tracer l'avancement dans le processus de transposition

↓ Texte Clair

↓ Texte Chiffré

↓ Texte Clair

↓ Texte Chiffré

↓ Texte Clair

↓ Texte Chiffré

↓ Texte Clair

↓ Texte Chiffré

↓ Texte Clair

↓ Texte Chiffré

↓ Texte Clair

↓ Texte Chiffré

↓ Texte Clair

↓ Texte Chiffré

↓ Texte Clair

↓ Texte Chiffré

↓ Texte Clair

↓ Texte Chiffré

↓ Texte Clair

↓ Texte Chiffré


```
PythonWin 3.4.1 (default, Aug  7 2014, 13:13:27) [MSC v.1600 32 bit (Intel)] on win32.
Portions Copyright 1994-2008 Mark Hammond - see 'Help/About PythonWin' for further copyright information.
>>> CARROUSEL 1.0  -- A Transposition Cipher --

Encryption process from key (JAMESBOND007) and 36-alphabet
[ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
Transposition of text according to following ranks : [10, 1, 13, 5, 19, 2, 15, 14, 4,
27, 27, 34]  for JAMESBOND007
The generated ciphertext was written to 'ciphertext.txt'.

Plaintext:
CARROUSELISACRYPTOSYSTEMDESIGNEDIN2015TOTRANSPOSEATEXTOFANYLENGTHBYAKEYOFANYLENGTH

Ciphertext:
FOYT2IORHTTHXE5EIEYOORECTGGFSDRTAYSNAENEEA0LAMRNESLBASAUEANGYKYOCYSTNSOTT1PDINNLSP

>>>CARROUSEL 1.0  -- A Transposition Cipher --

Decryption process from key (JAMESBOND007) and 36-alphabet
[ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
Arrangement of text according to following ranks : [10, 1, 13, 5, 19, 2, 15, 14, 4, 27,
27, 34]  for JAMESBOND007
The arranged plaintext was written to 'plaintext.txt'.

Ciphertext:
FOYT2IORHTTHXE5EIEYOORECTGGFSDRTAYSNAENEEA0LAMRNESLBASAUEANGYKYOCYSTNSOTT1PDINNLSP

Plaintext:
CARROUSELISACRYPTOSYSTEMDESIGNEDIN2015TOTRANSPOSEATEXTOFANYLENGTHBYAKEYOFANYLENGTH

>>>
```

Texte 1 :

WRNSHISSSFSIYHEGHEADTSSNLIROPRAEYEENRHDLESSEDFETNAXTRISHSIRYNYPOTTSOIUSENTOLEGEAHANRTLGRE
TGTPTTEWNECETAIETEOEOTDIUCNTUCABIMSTSHRMEKISEAAONVTTTTHEAPS

Texte 2 :

LRQKQIQFEXOATAHEXAUIIHPOAEREEHSQEOQYQLUQSNXXTTTXEGOOTQSTLWNTESNLEMXLRAVRTIMCANNINALX
QIEAVETXQXNEXAXHDMAQDHQREIVOHUSOIAXTQDHT

Texte 3 :

,YTH FTESTK MHEE CNLRRGTOFHLT -N CI ORTBFOHSEEDN,IGSVOMIESEIB,HNAYB GR OSOTEA NFDGHO DFIEURIY
DSSOSG;VLWAGSDS O EEOHHB AW O EBWSIUOISN,TNI- OBCMENTA SEAD A AN DSFIAAD H,II.ATTF N E EIDRR
HVNWHABHNMY ET ATNDOTIT K ACDLWERASYEA IWNOGHLBA A ER U HE ,SEA EOSGE UH,D R;A GEIR-AAN E
CBCLI T IEPR !-DR ITKDNELOASAHEE SI SNMHANGS PNOL MFSNDTEA DAELMAIHD -TDI OL B NRIENRUAL.EK;EIR
IOTN LR AHAO FCT" D N TH R.EAIHTNN EM SII RDLRUOLH RE HILEMN OTLH O WAUR,OEASLYIDMNT C G DHOR
TS"ALNSE MNHK;.RH OMNANTIBATO, OEEWE CEDGT,- :TO T R 'SOEEOSIIOSIE ANDHFSRT,VA HLHAMR OTH N HDC

Alphabet pour le texte 3 :

ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 ,.;:’'"!?()+-*/^<=>&@%€£$

ALGORITHME de PERMUTATION

Nous avons développé plusieurs systèmes de chiffrement manuel dont tout ou partie repose sur un algorithme de permutation des caractères d'une chaîne ou texte plus ou moins long [1,2,3]. Dans ce document nous approfondissons les propriétés de cet algorithme.

1. Exécution manuelle

Rappelons le processus de permutation : le texte est vu comme une liste circulaire de caractères sur laquelle nous nous déplaçons par sauts irréguliers, en commençant à l'extrémité finale. L'amplitude des sauts est définie par une suite d'entiers tirée d'une chaîne de caractères, jouant le rôle de clé, en substituant à chaque caractère son rang dans l'alphabet utilisé. Lorsqu'un saut aboutit sur un caractère du texte original, ce caractère est barré et est reporté à la fin d'une deuxième liste qui constitue ainsi progressivement le texte transposé. Si, dans le parcours, le caractère d'arrivée est déjà barré il faut le sauter et passer au suivant. Un texte étant naturellement beaucoup plus long que la clé il faut parcourir celle-ci plusieurs fois jusqu'à épuisement de tous les caractères non barrés du texte : si le texte a N caractères et la clé p caractères alors la division euclidienne n = q.p + r signifie qu'il faut q cycles de parcours de la clé et utiliser encore une fois r caractères de celle-ci.

L'annexe A illustre un exemple complet emprunté au chiffre Diagonales. La dernière lettre de la clé (7 caractères) et du texte (13 caractères) n'ont pas été marquées pour manifester cette dernière étape. En fait cette dernière lettre de la clé n'a pas d'influence réelle car il ne reste qu'un seul caractère à tirer à ce moment là.

Comme le nombre n de caractères éligibles diminue à chaque saut il arrive que le compte de lettres à sauter s dépasse celui-ci, ce qui se traduit par un ou plusieurs tours de décompte autour du texte. En pratique cela revient à ne décompter que le reste de la division euclidienne de s par n : s = k.n +d.

2. Implémentation programmée

Le choix du déplacement par sauts sur un texte qui est fixe est dû au fait qu'il s'agit d'un chiffre manuel où seul le crayon peut se déplacer. Dans l'écriture du programme associé à cet algorithme nous avons mis à profit le caractère dynamique des données et remplacé un saut s

vers la gauche et l'extraction du caractère par un décalage circulaire à droite d amenant le caractère sélectionné à la gauche du texte encore libre. La structure de plus en plus lacunaire du texte initial dans la version manuelle est remplacée par une sous-chaîne compacte de plus en plus courte et support du décalage circulaire. L'annexe B illustre en détails ce processus sur le même exemple que dans l'annexe A. Le parcours cyclique de la clé a été remplacé de manière équivalente par sa duplication jusqu'à la longueur *N* du texte à permuter. La longueur de clé *n* encore à exploiter diminue en même temps que le texte restant à permuter.

L'annexe C détaille la procédure, écrite en Python, pour cette implémentation programmée. Par simplicité elle est paramétrée par les données de l'annexe A.

3. Propriétés mathématiques

Décomposition de la permutation

Nous savons déjà qu'une permutation est décomposable en produit de transpositions et aussi en produit de cycles à supports disjoints [4]. La reformulation informatique de notre algorithme de permutation établit un autre schéma de décomposition à l'aide de permutations circulaires [5] : *une permutation est décomposable en produit de permutations circulaires de pas variables et à supports strictement inclus les uns dans les autres.*

Illustrons cette décomposition sur un autre exemple en représentant en lignes superposées les différents décalages circulaires et en traçant en bleu les éléments du support propre à chacun d'eux :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 7 & 6 & 5 & 8 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 6 & 7 & 8 & 1 & 2 & 3 \\ 4 & 2 & 3 & 5 & 6 & 7 & 8 & 1 \\ 4 & 2 & 7 & 8 & 1 & 3 & 5 & 6 \\ 4 & 2 & 7 & 6 & 8 & 1 & 3 & 5 \\ 4 & 2 & 7 & 6 & 5 & 8 & 1 & 3 \\ 4 & 2 & 7 & 6 & 5 & 8 & 1 & 3 \\ 4 & 2 & 7 & 6 & 5 & 8 & 1 & 3 \end{pmatrix}$$

Les permutations circulaires successives, ici effectuées vers la gauche pour montrer la généralité du résultat, ont respectivement pour pas : 3, 5, 3, 4, 3, 0 et 0. Il suffit de 7 permutations circulaires pour permuter les 8 éléments, le dernier étant implicitement positionné par la permutation circulaire ayant fourni l'avant-dernier élément. Ce résultat est évidement valable quelque soit la taille N de l'ensemble à permuter.

Spectre circulaire de la permutation

Revenons à l'exemple littéral de l'annexe A, nous voyons que la décomposition n'est pas unique si les décalages circulaires incluent des tours complets des supports. C'est ainsi que

plusieurs clés dont les lettres ont des valeurs v_i congrues à d_i modulo n_i produisent la même séquence et donc la même permutation (annexes D1 et D2).

Et finalement la seule information réellement pertinente est la séquence des décalages d_i, où $(1 \leq i \leq N-1)$, qui vérifient $d_i = s_i \bmod n_i$ et donc $0 \leq d_i < n_i = N-i+1$. Elle exprime la décomposition de la permutation en un produit de N-1 permutations circulaires de pas d_i sur une liste de taille décroissante n_i. C'est pourquoi nous considérons cette séquence $[d_1,\ldots,d_{N-1}]$ comme le *spectre circulaire* de la permutation. Il est de taille N-1 comme nous l'avons déjà énoncé. Nous notons cette séquence entre crochets pour mieux faire la différence avec la notation en deux lignes entre parenthèses de Cauchy. C'est cette séquence numérique qu'il faudrait introduire comme donnée, fondamentale et exhaustive, à l'entrée de l'algorithme. Pour l'exemple numérique précédent et *en convenant de toujours décomposer en permutations circulaire à droite*, elle est [5, 2, 3, 1, 1, 0, 0]. Comme elle résume toute l'information relative à une permutation nous exprimons cette équivalence en notant :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 7 & 6 & 5 & 8 & 1 & 3 \end{pmatrix} \equiv [5 \quad 2 \quad 3 \quad 1 \quad 1 \quad 0 \quad 0]$$

Dans la pratique le cerveau humain, de part ses fonctions cognitives du langage, est plus apte à manipuler et mémoriser une séquence de lettres. C'est pourquoi nous avons fait le choix de clés littérales.

Signature de la permutation

Le choix possible des valeurs $0 \leq d_i < n_i$ et la décroissance des $n_i = N-i+1$ avec $1 \leq i \leq N-1$ nous ramène naturellement au dénombrement des permutations d'un ensemble de taille N :

$$\prod_{i=1}^{N-1} n_i = n \cdot (n-1) \cdot \cdots \cdot 2 = N!$$

La permutation circulaire de pas *p* est la composition itérée *p* fois de la permutation circulaire élémentaire. La signature de la permutation circulaire élémentaire d'une liste de taille *k* est $\sigma = (-1)^{k-1}$ [5]. Nous savons que l'application faisant correspondre sa signature à une permutation est un morphisme du groupe des permutations sur le groupe [-1,+1] muni du produit usuel. La signature de la permutation circulaire de pas *p* d'une liste de taille *k* est donc $\sigma = (-1)^{p.(k-1)}$.

En revenant aux notations de l'annexe B, la signature de la permutation de taille *N* et dont le spectre circulaire est $[d_1, \ldots, d_i, \ldots, d_{N-1}]$ avec $0 \leq d_i < n_i = N-i+1$ est donc donnée par

$$\sigma = \prod_{i=1}^{N-1} (-1)^{d_i \cdot (n_i - 1)} = (-1)^{\sum_{i=1}^{N-1} d_i \cdot (n-i)}$$

4. Références

1. Spirale, un chiffre à masque jetable, 2015.
2. Diagonales, un chiffre par transposition, 2015.
3. Carrousel, un chiffre par transposition, 2015.
4. fr.wikipedia.org/wiki/Permutation
5. fr.wikipedia.org/wiki/Permutation_circulaire

5. Annexes

A	Algorithme de Permutation : par sauts à gauche
B	Algorithme de Permutation : par décalage à droite
C	Implémentation programmée en Python
D1	Algorithme de Permutation : clé équivalente 1
D2	Algorithme de Permutation : clé équivalente 2

Algorithme de Permutation : par sauts à gauche

(Ph.Allard)

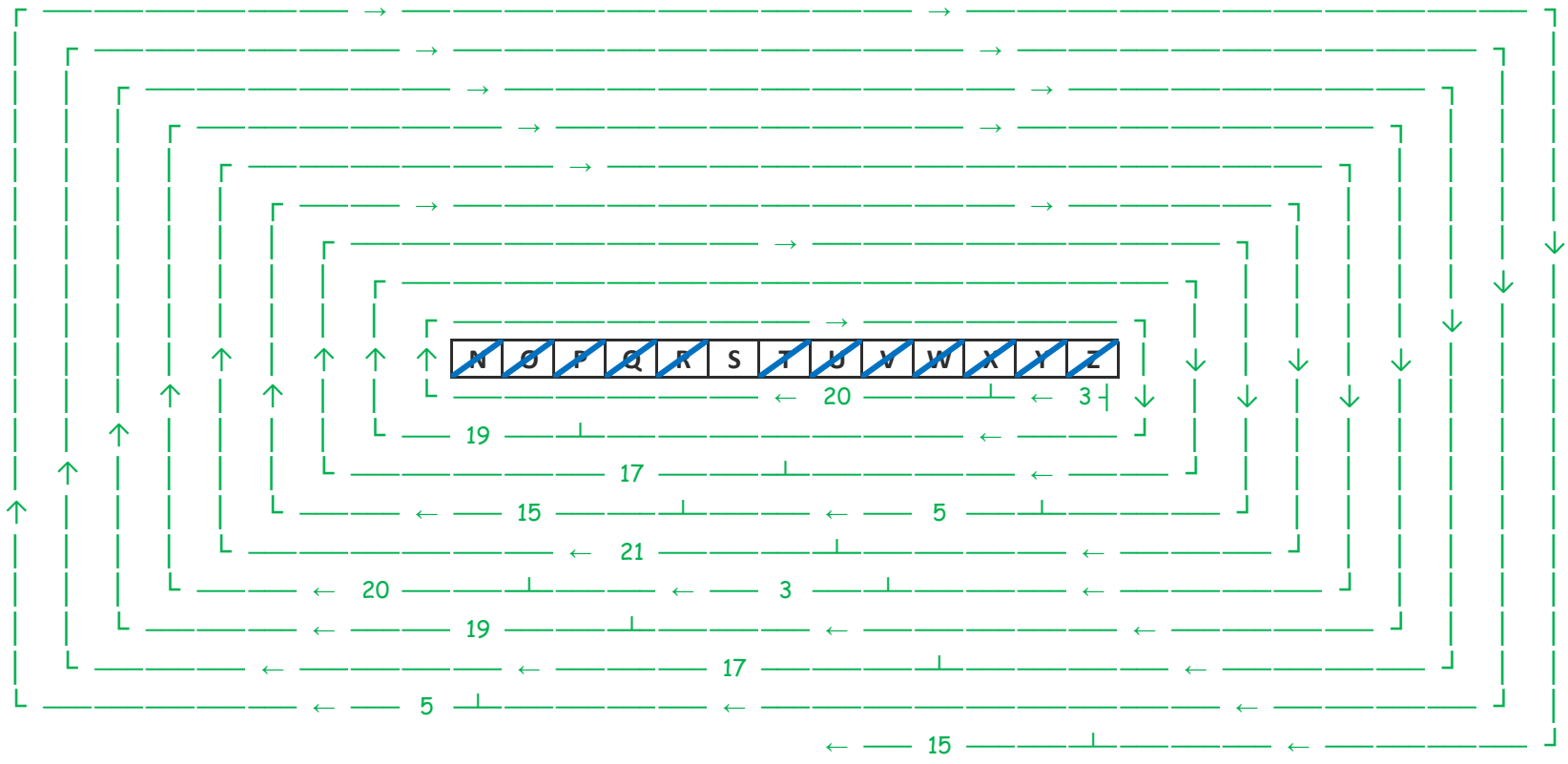
Clé de permutation →

C	T	S	Q	E	O	U
3	20	19	17	5	15	21
..	..	..	..	..	.	.

← rang dans l'alphabet

← marques pour tracer l'avancement dans le processus de permutation

Chaîne à permuter :



rayez la lettre dans la chaîne quand elle est permutée, pour la sauter ultérieurement

Chaîne permutée :

X	P	T	Y	R	U	V	O	Q	W	N	Z	S

Algorithme de Permutation : par décalage à droite

(Ph.Allard)

Clé de permutation	C	T	S	Q	E	O	U	C	T	S	Q	E	O
saut s vers la gauche	3	20	19	17	5	15	21	3	20	19	17	5	15
taille n de la chaîne à décaler	13	12	11	10	9	8	7	6	5	4	3	2	1
décalage d vers la droite	3	8	8	7	5	7	0	3	0	3	2	1	0

← rang dans l'alphabet

← s = k.n + d

→ d = 3	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
→ d = 8	X	Y	Z	N	O	P	Q	R	S	T	U	V	W
→ d = 8	P	Q	R	S	T	U	V	W	Y	Z	N	O	
→ d = 7	T	U	V	W	Y	Z	N	O	Q	R	S		
→ d = 5	Y	Z	N	O	Q	R	S	U	V	W			
→ d = 7	R	S	U	V	W	Z	N	O	Q				
→ d = 0	U	V	W	Z	N	O	Q	S					
→ d = 3	V	W	Z	N	O	Q	S						
→ d = 0	O	Q	S	W	Z	N							
→ d = 3	Q	S	W	Z	N								
→ d = 2	W	Z	N	S									
→ d = 1	N	S	Z										
→ d = 0	Z	S											
	S												

← chaîne à permuter

← après décalage à droite de d = 3

← après décalage à droite de d = 8

← après décalage à droite de d = 8

← après décalage à droite de d = 7

← après décalage à droite de d = 5

← après décalage à droite de d = 7

← après décalage à droite de d = 0

← après décalage à droite de d = 3

← après décalage à droite de d = 0

← après décalage à droite de d = 3

← après décalage à droite de d = 2

← après décalage à droite de d = 1

← après décalage à droite de d = 0

X	P	T	Y	R	U	V	O	Q	W	N	Z	S

← chaîne permutée

```
## Algorithm to Generate Permutations   (Ph. Allard)
# demo version

# list of ranks of characters in key
extraction_list = [3,20,19,17,5,15,21]
lk = len(extraction_list)       # length of extraction list and key

# Right Circular Permutation function
def RightCircPerm(L,k,p):
    fixed = L[:-k]          # fixed points in list L
    orbit = L[-k:]          # part to shift in list L
    orbit = orbit[-p:]+orbit[:-p]   # right shift of step p
    fixed.append(orbit[0])  # extension of fixed points in list
    del orbit[0]            # reduction of orbit
    L = fixed + orbit       # permuted list
    print(L)                # to show advancement
    return L

# right circular permutation of orbits equivalent to extraction of characters from the right according to key

text_list = ['N','O','P','Q','R','S','T','U','V','W','X','Y','Z']
N = len(text_list)

print(text_list)

for i in range(1,N):
    ji=extraction_list[0]           # jump to position of element to extract from top right of list
    ni = N-i+1                      # length of list to shift
    si = ji % ni                    # right shift step
    print('permutation step = ',i,'  orbit length = ',ni,'  circular shift = ',si)
    text_list = RightCircPerm(text_list,ni,si)
    extraction_list.append(extraction_list[0])  # circular running along the key
    del extraction_list[0]

#-------------------------------------------------------------------------
```

```
PythonWin 3.4.1 (default, Aug  7 2014, 13:13:27) [MSC v.1600 32 bit (Intel)] on win32.
Portions Copyright 1994-2008 Mark Hammond - see 'Help/About PythonWin' for further copyright information.
>>>
>>> ['N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']
permutation step =  1   orbit length =  13   circular shift =  3
['X', 'Y', 'Z', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W']
permutation step =  2   orbit length =  12   circular shift =  8
['X', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'Y', 'Z', 'N', 'O']
permutation step =  3   orbit length =  11   circular shift =  8
['X', 'P', 'T', 'U', 'V', 'W', 'Y', 'Z', 'N', 'O', 'Q', 'R', 'S']
permutation step =  4   orbit length =  10   circular shift =  7
['X', 'P', 'T', 'Y', 'Z', 'N', 'O', 'Q', 'R', 'S', 'U', 'V', 'W']
permutation step =  5   orbit length =  9   circular shift =  5
['X', 'P', 'T', 'Y', 'R', 'S', 'U', 'V', 'W', 'Z', 'N', 'O', 'Q']
permutation step =  6   orbit length =  8   circular shift =  7
['X', 'P', 'T', 'Y', 'R', 'U', 'V', 'W', 'Z', 'N', 'O', 'Q', 'S']
permutation step =  7   orbit length =  7   circular shift =  0
['X', 'P', 'T', 'Y', 'R', 'U', 'V', 'W', 'Z', 'N', 'O', 'Q', 'S']
permutation step =  8   orbit length =  6   circular shift =  3
['X', 'P', 'T', 'Y', 'R', 'U', 'V', 'O', 'Q', 'S', 'W', 'Z', 'N']
permutation step =  9   orbit length =  5   circular shift =  0
['X', 'P', 'T', 'Y', 'R', 'U', 'V', 'O', 'Q', 'S', 'W', 'Z', 'N']
permutation step =  10   orbit length =  4   circular shift =  3
['X', 'P', 'T', 'Y', 'R', 'U', 'V', 'O', 'Q', 'W', 'Z', 'N', 'S']
permutation step =  11   orbit length =  3   circular shift =  2
['X', 'P', 'T', 'Y', 'R', 'U', 'V', 'O', 'Q', 'W', 'N', 'S', 'Z']
permutation step =  12   orbit length =  2   circular shift =  1
['X', 'P', 'T', 'Y', 'R', 'U', 'V', 'O', 'Q', 'W', 'N', 'Z', 'S']
>>>
```

Algorithme de Permutation : clé équivalente

(Ph.Allard)

Clé de permutation	C	T	S	Q	E	O	U	I	J	O	T	G	A
saut s vers la gauche	3	20	19	17	5	15	21	9	10	15	20	7	1 ← rang dans l'alphabet
taille n de la chaîne à décaler	13	12	11	10	9	8	7	6	5	4	3	2	1
décalage d vers la droite	3	8	8	7	5	7	0	3	0	3	2	1	0 ← s = k.n + d

→ d = 3	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	← chaîne à permuter
→ d = 8	X	Y	Z	N	O	P	Q	R	S	T	U	V	W	← après décalage à droite de d = 3
→ d = 8	P	Q	R	S	T	U	V	W	Y	Z	N	O		← après décalage à droite de d = 8
→ d = 7	T	U	V	W	Y	Z	N	O	Q	R	S			← après décalage à droite de d = 8
→ d = 5	Y	Z	N	O	Q	R	S	U	V	W				← après décalage à droite de d = 7
→ d = 7	R	S	U	V	W	Z	N	O	Q					← après décalage à droite de d = 5
→ d = 0	U	V	W	Z	N	O	Q	S						← après décalage à droite de d = 7
→ d = 3	V	W	Z	N	O	Q	S							← après décalage à droite de d = 0
→ d = 0	O	Q	S	W	Z	N								← après décalage à droite de d = 3
→ d = 3	Q	S	W	Z	N									← après décalage à droite de d = 0
→ d = 2	W	Z	N	S										← après décalage à droite de d = 3
→ d = 1	N	S	Z											← après décalage à droite de d = 2
→ d = 0	Z	S												← après décalage à droite de d = 1
	S													← après décalage à droite de d = 0

Permutation : ↓	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	X	P	T	Y	R	U	V	O	Q	W	N	Z	S
spectre circulaire :	3	8	8	7	5	7	0	3	0	3	2	1	

Algorithme de Permutation : clé équivalente

(Ph.Allard)

Clé de permutation	C	T	S	Q	E	O	U	U	Y	K	N	I	B
saut s vers la gauche	3	20	19	17	5	15	21	21	25	11	14	9	2
taille n de la chaîne à décaler	13	12	11	10	9	8	7	6	5	4	3	2	1
décalage d vers la droite	3	8	8	7	5	7	0	3	0	3	2	1	0

← rang dans l'alphabet

← s = k.n + d

→ d = 3	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	← chaîne à permuter
→ d = 8	X	Y	Z	N	O	P	Q	R	S	T	U	V	W	← après décalage à droite de d = 3
→ d = 8	P	Q	R	S	T	U	V	W	Y	Z	N	O		← après décalage à droite de d = 8
→ d = 7	T	U	V	W	Y	Z	N	O	Q	R	S			← après décalage à droite de d = 8
→ d = 5	Y	Z	N	O	Q	R	S	U	V	W				← après décalage à droite de d = 7
→ d = 7	R	S	U	V	W	Z	N	O	Q					← après décalage à droite de d = 5
→ d = 0	U	V	W	Z	N	O	Q	S						← après décalage à droite de d = 7
→ d = 3	V	W	Z	N	O	Q	S							← après décalage à droite de d = 0
→ d = 0	O	Q	S	W	Z	N								← après décalage à droite de d = 3
→ d = 3	Q	S	W	Z	N									← après décalage à droite de d = 0
→ d = 2	W	Z	N	S										← après décalage à droite de d = 3
→ d = 1	N	S	Z											← après décalage à droite de d = 2
→ d = 0	Z	S												← après décalage à droite de d = 1
	S													← après décalage à droite de d = 0

Permutation : ↓	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	X	P	T	Y	R	U	V	O	Q	W	N	Z	S
spectre circulaire :	3	8	8	7	5	7	0	3	0	3	2	1	

LA CRÉATION DE CLÉS

Un problème méta-cryptologique

Plan

1. Introduction

Quelque soit le crypto-système symétrique auquel on est confronté, classique et manuel ou moderne et numérique, à un moment il faut introduire une donnée alphanumérique, la ou les clés, qui personnalise le système pour un utilisateur particulier. La distribution des clés parmi plusieurs utilisateurs est un problème fondamental que nous nous proposons d'aborder ici. Le schéma d'organisation des correspondants que nous envisageons est hiérarchisé : entre une Autorité et ses Agents. Selon le contexte il pourra s'agir du Ministère des Affaires Étrangères et d'ambassades, d'une ambassade et d'agents locaux, d'un État-major et de commandants d'unités ou encore d'un Officier Traitant et d'agents secrets infiltrés. Comme on le voit le nombre d'agents à fournir peut varier de moins d'une dizaine à plusieurs centaines. La durée de validité de ces clés peut être très variable aussi, de quelques semaines pour une mission à des années pour une guerre qui s'éternise. Nous prendrons ainsi en compte la possibilité d'approvisionner des agents pour plusieurs années d'activité. Fondamentalement, l'alternative est entre distribution aux utilisateurs de clés toutes prêtes ou création par les utilisateurs eux-mêmes de clés au coup par coup.

2. Distribution d'un livre de clés

C'est la solution traditionnellement adoptée par un service diplomatique ou une armée. Elle est simple pour les utilisateurs mais dangereuse en terme de sécurité car ces documents doivent être acheminés puis conservés en lieux fixes ou mobiles. Et pendant chacune de ces phases ils courent le risque d'être perdus, photocopiés, volés ou capturés.

La parade à ces aléas inhérents à la distribution est la création directe par les utilisateurs des clés dont ils ont besoin. Nous proposons dans cet article plusieurs solutions pour y parvenir. Le principe général est de puiser dans une source une chaîne de caractères qui sera utilisée, directement ou après transformation, comme clé.

3. Création à partir d'un livre

C'est cette solution que nous allons développer en détails ici. Elle est particulièrement adaptée à un réseau clandestin disposant de peu de ressources matérielles et devant produire un grand nombre de clés, soit par la durée de son activité soit par le type de crypto-système employé. Par exemple le chiffre Spirale [1] demande 4 clés de 7 caractères pour chaque message envoyé. Cette solution passe par plusieurs étapes :

- Choix du livre ;
- Choix de la page ;
- Choix de la ligne ;
- Extraction de caractères et construction de la clé ;
- Correction statistique.

1. Choix du livre

Pour ne pas attirer l'attention il doit avant tout être neutre dans le contexte où se trouve l'agent, un roman à la mode par exemple, ou mieux encore être en adéquation avec le milieu infiltré : un manuel financier à Wall Street, le Capital à Moscou, le petit livre rouge à Pékin, la bible dans le Middle West, le coran à La Mecque, etc[1].

Il le faut suffisamment épais pour offrir plusieurs centaines de pages exploitables, de l'ordre du nombre de jours dans l'année. De nombreuses pages sont perdues soit parce que non numérotées (préface, table des matières,…) soit parce que leur structure est inadaptée à notre usage (index, glossaire, texte très court,…). Au final la partie utile commencera à la page p_i et finira à la page p_f, soit un nombre $n_P = p_f - p_i + 1$ de pages disponibles.

2. Choix de la page

L'idée fondamentale est :

- utiliser une page par jour ;
- cheminer entre elles de façon aléatoire selon le jour ;
- sans risque de répétition dans l'année ou d'une année sur l'autre.

[1] Les lieux communs ont parfois du bon…

Notre problème fondamental est donc de bâtir un algorithme simple et efficace, satisfaisant aux conditions ci-dessus, faisant passer du jour à un nombre entier compris entre p_i et p_f.

Nous proposons la solution suivante :

Partant du format classique d'écriture des dates jj/mm/aaaa, nous pouvons facilement en tirer un nombre J en considérant les quatre premiers digits comme des chiffres décimaux :

$$J = jjx100+mm \quad (1)$$

puis appliquer la formule :

$$P = p_i + J \bmod n_P \quad (2)$$

pour désigner une page P. Par exemple, avec un livre exploitable des pages 11 à 153, nous utilisons les pages :

- 18 Mai 2015 J = 1805 P = 100 = 11 + 1805 mod 143
- 28 Février 2016 J = 2802 P = 96
- 15 Octobre 2017 J = 1510 P = 91

Au bout d'un an d'utilisation nous retomberons sur les mêmes pages, pour éviter cela nous devons faire intervenir l'année. Mais toujours d'une manière simple pour l'utilisateur. L'opération modulo disperse bien ses résultats si l'argument varie beaucoup, en général par un produit ou mieux une exponentiation. Cette dernière solution doit être écartée car elle dépasse rapidement les capacités d'une calculatrice de poche et est impossible à calculer manuellement, il nous reste le produit par un facteur pas trop grand pour être effectué à main. En d'autres termes, trouver un hachage sur la valeur de l'année. Nous proposons une solution simple : la somme de ses chiffres. D'où les nouveaux résultats :

- 18 Mai 2015 J = 1805x8 P = 151
- 28 Février 2016 J = 2802x9 P = 61
- 15 Octobre 2017 J = 1510x10 P = 96

Et pour voir l'effet sur les jours suivants :

- 19 Mai 2015 J = 1905x8 P = 93
- 29 Février 2016 J = 2902x9 P = 103
- 16 Octobre 2017 J = 1610x10 P = 95

Nous constatons ainsi les variations 151 → 93, 61 → 103, 96 → 95.

En conclusion, la formule (2) avec J défini par la formule

$$J = (jjx100+mm) \times \sum a \quad (3)$$

donne bien un déplacement plutôt erratique dans les pages du livre et la non-répétitivité systématique d'une année à l'autre.

Si plusieurs correspondants utilisent le même livre et rédigent un message le même jour, ce serait alors avec la même page et peut être la même clé ce qui n'est pas acceptable. Il convient donc de les différentier. Pour cela il suffit que chacun apporte son *grain de sel* S, un entier, et travaille avec la valeur J+S. Pour être arithmétiquement fonctionnelles et distinguer deux correspondants, les valeurs S_1 et S_2 de leur sel doivent vérifier simultanément

$$S_1 \neq S_2 \neq 0 \qquad \text{mod } n_P \tag{4}$$

Dans la pratique cela revient à attribuer à chacun le numéro, différent, d'une des pages exploitables.

3. Choix de la ligne

Le nombre n_L de lignes d'une page varie naturellement selon le format du livre et le type d'édition, mais il est en général d'environ la trentaine. Nous pouvons reprendre le principe de la formule (2) et choisir la ligne L selon la formule :

$$L = 1 + J \bmod n_L \tag{5}$$

Poursuivons notre exemple avec des pages de $n_L = 32$ lignes :

- 8 Mai 2015 J = 1805x8 P = 151 L = 9
- 28 Février 2016 J = 2802x9 P = 61 L = 3
- 15 Octobre 2017 J = 1510x10 P = 96 L = 29

S'il faut encore distinguer des agents utilisant la même source, leurs sels doivent vérifier des conditions supplémentaires garantissant des lignes différentes :

$$S_1 \neq S_2 \neq 0 \qquad \text{mod } n_L \tag{6}$$

4. Extraction de caractères et construction de la clé

Il s'agit maintenant d'extraire, dans la ligne sélectionnée, des caractères pour façonner une clé qui soit difficile à découvrir. Cela impose en particulier de ne pas prendre de mots entiers qui seraient des proies pour une attaque par dictionnaire. Les solutions sont nombreuses et le résultat d'un compromis entre imagination et simplicité de mise en œuvre. Nous pourrions par exemple commencer au $7^{ème}$ caractère et en extraire un ensuite tous les 2 ou 3 caractères.

Dans la notice initiale du chiffre Spirale qui nécessite 4 clés de 7 lettres, nous suggérions la procédure suivante : extraire les 7 premières lettres et les 7 dernières, indépendamment des mots ou de la ponctuation, faire de même avec une autre ligne décalée de 5 plus bas par exemple (mais d'autres règles de choix conviendraient aussi) ; écrire ensuite, un extrait par ligne, dans un tableau 7x4 puis le lire verticalement depuis le coin supérieur droit. Cela revient à inverser ces chaînes de caractères et à les entrelacer. Et finalement découper cette longue chaîne en 4 segments de 7 lettres.

Exemple: - texte de la page "***We got in***to Milan … unloa***ded us in***
……
said this had … around ***his neck***."[2]

w	e	g	o	t	i	n
d	e	d	u	s	i	n
s	a	i	d	t	h	i
h	i	s	n	e	c	k

- 4 clés créées nnikiih ctsteou dngdise eaiwdsh

5. Correction statistique

L'usage d'un livre est très simple mais a un défaut intrinsèque : les probabilités d'occurrence des lettres dans les clés sont naturellement proches de celles des lettres du langage du livre et donc non égales. Ces différences prévisibles de fréquence pourraient être mises à profit pour optimiser des attaques par force brute. Une façon simple de corriger partiellement ce défaut serait de remplacer dans les chaînes sélectionnées quelques lettres des plus hautes fréquences par des lettres des plus basses fréquences.

Les fréquences observées des lettres dépendent du langage, du nombre de textes analysés et de leurs natures. Une source[3] donne des résultats concernant plusieurs langues :

Langue	+ fréquentes	- fréquentes
Français	E A S I N T	X J Y Z K W
Anglais	E T A O I N	V K X J Q Z
Espagnol	E A O S N I	H Z J X W K
Portugais	A E O S I R	X Z J K Y W
Italien	E I A O N L	Q K Y X W J
Allemand	E N I R S A	V P J Y X Q
Néerlandais	E N A I R T	J Z F Y X Q

Fréquences naturelles de lettres

Les clés corrigées de l'exemple précédent pourraient alors être : NVIKKIH, CTSQEOU, DNGDKSZ et EAIWDSH.

4. Création à partir d'un journal

Cette solution ne peut vraiment s'envisager que pour des correspondants se trouvant dans un même pays. Le caractère quotidien du journal évitant le risque de réemploi au bout d'un certain temps et sa structure en pages, au plus quelques dizaines, et en colonnes, environ une demi-douzaine, entraînent des aménagements aux propositions précédentes.

[2] *A Farewell to Arms*, E.Hemingway, p81, Charles Scribner's Sons edition.
[3] Source: http://www.bibmath.net/crypto/index.php

Une solution simple permettant de différentier tous les utilisateurs et d'éviter les collisions lors de la création des clés consiste à attribuer à chacun d'eux une page, une colonne et une ligne particulière. La renouvellement quotidien du journal assure le renouvellement de la source et évite tous les calculs des formules précédentes.

Par contre, la construction des clés et leur correction statistique conservent les règles énoncées plus haut.

5. Création avec un programme

Jusqu'à maintenant tous les procédés que nous avons exposés sont d'une mise en œuvre manuelle. Un outil informatique peut rendre de grand service par sa rapidité mais la construction d'un programme faisant simplement appel au générateur de nombre aléatoire disponible dans tout langage de programmation ne peut être la solution. En effet, à chaque exécution du programme le générateur produit de nouveaux nombres or l'outil dont les correspondants ont besoin doit vérifier une condition bien particulière : utilisé indépendamment en des instants différents, il doit fournir le même résultat, à savoir la clé.

Nous devons donc élaborer un procédé ayant deux propriétés contradictoires :

- Etre déterministe pour être reproductible ;
- Générer un résultat de nature aléatoire.

Nous savons déjà que par, le calcul, il est seulement possible de générer des résultats ayant suffisamment peu de structure discernable pour paraître chaotiques et être qualifiés de pseudo-aléatoires. C'est à ce niveau que nous allons travailler en proposant l'emploi détourné du chiffre Carrousel [2] fondé exclusivement sur un algorithme de permutation des caractères du texte clair. Le programme associé est disponible librement, si nous le faisons travailler en mode de chiffrement sur un texte constitué, par exemple, de 3 exemplaires concaténés d'un même alphabet alors le résultat sera une longue chaîne de caractères dans laquelle nous pouvons puiser un segment qui jouera le rôle de clé. Le fait d'avoir mis plusieurs exemplaires de l'alphabet dans le texte à permuter permet de rencontrer, éventuellement, plusieurs occurrences du même caractère dans le segment choisi. Ce qui lui donne, en tant que future clé, une plus grande variété combinatoire. Dans le même but, plusieurs applications successives de l'algorithme de permutation sont utiles pour enrichir cette variété. De plus, le nombre d'exemplaires de chaque caractère étant le même dans le texte il n'est plus nécessaire d'appliquer des corrections statistiques d'origine linguistique pour rétablir l'équiprobabilité d'occurrence dans cette source de clés. Selon l'alphabet utilisé nous créons des clés de types différents adaptés au chiffre :

- [A, B, …, Y, Z] clé littérale, de majuscules
- [A, …, Z, a, …, z] clé littérale, de majuscules et minuscules
- [A, …, Z, 0, …, 9] clé alphanumérique pour [2]
- [0, …, 9, A, B, C, D, E, F] clé hexadécimale pour [3]
- [0, …, 7] clé octale

Finalement nous avons développé une version du programme associé qui admet comme seule donnée fondamentale le nombre de permutations à effectuer sur le texte multi-alphabets. Un paramètre interne au programme est décisif : la clé de permutation. Elle doit être initialement convenue entre les correspondants et joue implicitement le rôle de signature des clés générées. L'annexe donne un exemple des résultats produits par ce programme.

Une autre convention doit être établie entre les correspondants : comment passer du jour du message au nombre de permutations générant la suite de caractères source de la clé du message. À titre d'exemple, les formules (3) et (2) peuvent être reprises en faisant jouer au numéro de page calculé celui de nombre de tours de permutation à appliquer.

Si pour, des raisons de discrétion absolue ou par manque de matériel, il n'est pas possible d'utiliser ce programme une solution de secours peut être d'effectuer chaque jour à la main un tour de permutation de la longue chaîne générée la veille pour y puiser les clés de ce jour. Pour réduire le travail de permutation d'une longue chaîne multi-alphabets, une solution est de travailler sur un seul alphabet et de conserver les résultats obtenus au fil du temps. Puis de combiner, par exemple en les entrelaçant, plusieurs de ces résultats.

6. Références

1. Spirale – un chiffre à masque jetable, 2015.
2. Carrousel – un chiffre par transposition, 2015.
3. Diagonales – un chiffre par transposition, 2015.

```
PythonWin 3.4.1 (default, Aug  7 2014, 13:13:27) [MSC v.1600 32 bit (Intel)] on win32.
Portions Copyright 1994-2008 Mark Hammond - see 'Help/About PythonWin' for further copyright information.
>>> KEY_GENERATOR 1.0 --

Permutation process from 12-key (JAMESBOND007) and 36-alphabet [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789] for 20 cycles :

Transposition of characters according to following ranks : [10, 1, 13, 5, 19, 2, 15, 14, 4, 27, 27, 34]  for JAMESBOND007
1-Permuted : 0ZMHYWH3Z8DC10MHVTBVRUYQFEWQ42G0TPOAVTC6A8M2RKBN54J8A7ENGU77OLLF93Y3SNS1541POJFSEGDJIDLZ6XQ5I9IPC29XU6BXKRKW
2-Permuted : 92ISO722EKPCQW13954U7RCA8AYVBUFLNHLVUVMK5S54TDTD3YKO0RO4MIPNJNCW13F6Q0EF0GXZM8JBYHHGR6JLS76XEWZ819APGTZQBXDI
3-Permuted : A9RBJP4UADZMVYQ2WXGIR710S5C9ZGJC43JURUIB0E3B5HV66FDL9XMY5EH0KDC7F38T6WOWLFPL1K84O2SHTKGNQNSQYIEOX1V8MN2AT7PZ
4-Permuted : V1T4KHBG5PLI9CVUIQFEXRX9E01W2M8CY2GR7IRTLO6ZXSUKT8HJA71F3Y3WD6MPW3SNSYM7CJ8NQDKGJ4B25BHD60QAOZALPFUO5490VNZE
5-Permuted : UF5GD3ZM0ZNRW19GZAJY7XPAOLXI95KMFUH7RETVCMT2QBIBNSSGVNQ86O2YHKIH73E4QC1PC8ODVPDFKB44XT26SW60JE5J8WRL3Y19U0LA
6-Permuted : RWXFH225LLDTIXWME08ON78VMCPZ13DI8G2RXY5UC1N9A4ET4EBHU0VSTJUCSBR3P3OY61QHMKL69ZPJDZGBQV4KQYS9KA0GO77J6FFAIWN5
7-Permuted : 77QJSU93CN65ZPI5A9KJ0NOU1C8EF6PRSM4X7OXIMQ410GYVYO42RW9ENKG1BTT2H3MFSXV3IDJKWLZ8H2FZAUBB6CQAD5LHLPRGT8WVEYD0
8-Permuted : RPA8BG16CDKXE8Z35ADKW0LRQMOAWTZTE5B7NJQEIVYF9FOUFMG47YWO4DMX4V5U3318QP92RPGBINLKS9J20IZTS16VH0C2JHXHNS7UYC6L
9-Permuted : XH0K4MFTM6BQAOE60VPDYWJ7VIL57NL5O3ZN0KAYR9FWAJJI81FBRCIMYH5PGUXG23QS68WUTZHTZDNDB1899E2VQXSUSLC4G3724EPRO1KC
10-Permuted : 739DG5WNIKTA5LATLUZHCYGR9RJ0P4NXM620WD0OTW87V8KESQJZX1Z1FS38FIQMU3VESOIG5L2VE6DP4FK1AY9U6PQRBCMBH2N4YOH7JXBC
11-Permuted : N2APF374RBV00J5NCRLS1CHXWTGLHYDQ1T9WYH9J5ISPUKDYEV827XEQ8B6OJEA5G39OQLZMXN4UAK6ZGWDFVO1IS8674CIZ2U0BFM3RKPTM
12-Permuted : 0UVZJ6PYTTU9LG04C7NBX127I5HC3F6AQN1YCSAKXZEHRDHOO9K9NPAVS4TL8Y03M3WM6JE5QDBI5BKLF7PWUJFEQOSRGMR24GWZ812XD8VI
13-Permuted : WGUL8THF5VIACHLYMRD4PX4NZX2C28K0V4FC1BVDQEO37PSJMWD10859EGNJKO9653I1SGA3A6ZE0TBNJPZ7RKWY6LQXFIT9BMY2SQU7HOUR
14-Permuted : YMRNKN38XUEVC2CFIX6G8PB0EQ4MUSB99YW1X4UHAAM2RZBK1IPFWO0WOF4GDJAT33ZQQH560K2YLVTD8HLP7D7OSJ67JR51Z5C9EVGNSLIT
15-Permuted : C57DD42SQIYUM4C8R7KFO8ZWAABIGETAWF7XPGRS051UXL4DQZZWYLLIMJYHPKVN63EV620T9B9OCUV6K3NHRHPJQGSN8TXF2311O9M0BJE5
16-Permuted : 13R6PYUEAEORIBMSTNBJLO2Y50ZRMOVVI8PP8F7B90QG7NGHVEL7CJCZ18F2ZDU4T3A9S4LNAT1JCIUKD2D3XSHK6HQ0K5QW96XFMW5W4GYX
17-Permuted : X6XKZFGO0YJ7RZIE50T8JL9C092T5MUUZSH8OJR4ALVMNDFS9ANP1GCEQK84LHRYN35WQBC4VVFKMEIBPU627B3DS26WDXA71TPW1I3YGHOQ
18-Permuted : PT7BL8MM9OKRT2ROXWVKGJ11LA9531IREE3OL8XGVC9506JBW5DHXHMAVDSBNS7F430I6ZCYUUWDIYETZGKUN42HQ4SYPQ0PFN87QZ6CF2JA
19-Permuted : 8NNTNS51AJDX59TMQYUDHGFXCV1X6QE7AO2LJK7FUCW3WK84I063P2I59PEZDBR8Y3LZS2MFRI7HROYVLMBG0GUS6BQCZA9HW4OPVET1J4K0
20-Permuted : O40VDE3QVKH7X151ACIP2HWPCUFQTVYR5MUJGDNJRMI6YBKGZLK284R0WZO264XSF3CEQ9I87EPSTJOUN5TMWFGBSZ61L0A37YLH9ANX8BD9

The generated keys were written to 'keys.txt'.
Characters (108):
ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
Keys (108):
O40VDE3QVKH7X151ACIP2HWPCUFQTVYR5MUJGDNJRMI6YBKGZLK284R0WZO264XSF3CEQ9I87EPSTJOUN5TMWFGBSZ61L0A37YLH9ANX8BD9
```

CONVENTIONS ACCESSOIRES POUR ALPHABET LIMITÉ

1. Introduction

En général les systèmes manuels de chiffrement se limitent, par souci de simplicité, à l'usage des seules 26 lettres de l'alphabet majuscule A à Z. C'est le cas pour Diagonales par exemple mais pas pour Spirale qui permet de traiter n'importe quel alphabet. Cette restriction entraîne un certain nombre de conséquences :

- Les lettres accentuées sont remplacées par les même sans accents ;
- Les espaces et tous les signes de ponctuation sont supprimés, d'où un texte concaténé très compact pouvant être difficile à lire ou ambigu ;
- Les nombres doivent être écris littéralement ce qui peut les rendre extrêmement longs
- Il est difficile voir impossible d'exprimer des formules mathématiques ou chimiques

Tant que le texte reste lisible, clair et assez court on peut tolérer ces déformations mais c'est impossible pour des messages au contenu très scientifique ou technique, économique ou linguistique. Nous proposons ici deux conventions destinées à pallier à ces lacunes.

2. Conventions De Viaris étendues

À la fin du dix-neuvième siècle, De Viaris avait déjà proposé des conventions de transcription propres à résoudre ces difficultés. Nous donnons dans l'annexe A l'exposé intégral de ces conventions, reprises par Delastelle dans son ouvrage de 1902. Nous pouvons les adopter dans leur ensemble moyennant quelques compléments adaptés à notre époque.

Le symbole #, équivalent anglo-saxon de *numéro* sera traité identiquement : KQK.

Les espaces seront remplacés, seulement quand cela est nécessaire, indifféremment par W ou K avec le plus de variabilité possible. L'emploi unique et systématique d'une même lettre se remarquerait et deviendrait une faiblesse potentielle du chiffre.

Pour les symboles modernes ou linguistiques, nous conservons la logique de De Viaris en adoptant, cette fois, W comme autre délimiteur :

L	M	N	O	P	Q	R	S	T	U	V
@	%	&	¡	¿	€	[ ]	_	$	£	~

Ces conventions qui utilisent la rareté d'apparition des lettres K et W en Français peuvent encore s'appliquer à d'autres langues latines (Espagnol, Italien, Portugais). Pour les langues germaniques d'autres choix conviendraient mieux : par exemple Q et Z pour l'Anglais et X et Q pour l'Allemand. Ces conventions induisent une modification des fréquences des lettres qui transparaitraient malgré un chiffre par transposition mais elles passeraient inaperçues avec un chiffre par substitution poly-alphabétique.

Exemples

- *Rendez-vous le 27 Mai à 14 h au 32 de la rue Louis Martin* devrait s'écrire :

RENDEZVOUSLEVINGTSEPTMAIAQUATORZEHAUTRENTEDEUXDELARUELOUISMARTIN

Avec ces conventions cela s'écrira, en minimisant les corrections :

RENDEZKSKVOUSLEKBGKMAIAKYKKADKHAUKCBKDELARUELOUISMARTIN

- *The prototype has reached Mach 2.56* devrait s'écrire :

THEPROTOTYPEHASREACHEDMACHTWOPOINTFIFTYSIX

Il s'écrira plus brièvement :

THEPROTOTYPEHASREACHEDMACHQBLEFQ

- *L'adresse de l'auteur est AMD-crypto@orange.fr* s'écrira :

LADRESSEDELAUTEURESTAMDKSKCRYPTOWLWORANGEKMKFR

- *Der Brennstoff R-stoff enthält 57 % diyldiisocyanat* (H_2N-$C_6H_3(CH_3)_2$) s'écrira :

DERBRENNSTOFFXRXSXSTOFFXENTHAXVXLTXEGXQMQDIYLDIISOCYANATXRXHKBKNKSKCKFKHKCKKRKCHKCKKRKKBKXRX

3. UNICODE adaptée

La norme informatique UNICODE [1] a été développée pour donner à tout caractère de n'importe quel système d'écriture de langue un identifiant numérique unique. L'identifiant numérique, appelé *point de code*, a la forme U+xxxx où (où xxxx est un nombre hexadécimal de 4 à 6 chiffres, entre U+0000 et U+10FFFF). L'immense ensemble de points de code est subdivisé en *plans* puis en *blocs*. Le *plan multilingue de base* (PMB, points de code de U+0000 à U+0FFF) contient la plupart des caractères utilisés par les langues modernes les plus courantes dans le monde. Son premier bloc *Latin de base* (U+0000 à U+007F) offre les lettres courantes, les chiffres et la ponctuation. Le bloc suivant *Supplément Latin-1* (U+0080 à U+00FF) apporte d'autres signes de ponctuation et des lettres diacritées (é,è,ê,à,…) courantes dans un grand nombre de langues, dont les langues latines. Une seule lettre utile pour nous, € (U+20AC), se trouve à part dans le *plan idéographique complémentaire* (PIC).

Cette norme répond donc à notre besoin à condition d'en changer la forme. Nous pouvons garder la logique et l'ordre de ces identifiants mais en conservant seulement les deux chiffres hexadécimaux de poids faible et en les exprimant avec les seules lettres dont nous disposons. Il suffit pour cela de se donner une représentation des valeurs de 0 à 15. Nous reprenons ici celle adoptée dans Diagonales [2] pour la base 26 mais en se limitant aux 16 premières lettres :

$Chiffre_{16}$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$Valeur_{10}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P

De plus il nous faut une lettre, de fréquence minimale, jouant le rôle de préfixe et ne faisant pas partie de la table ci-dessus. Nous pouvons ainsi adopter W pour les langues latines et Q pour les langues germaniques.

Ainsi le caractère ! codé U+0021 sera exprimé par WCB ou QCB suivant la langue.

L'annexe B rassemble les codes des caractères les plus courants dans les textes.

Exemple

*SPIRALE is a one-time-pad cryptosystem designed in 2015/05 to replace SOLITAIRE when one has no cards. It is based in parts on the generalized Fibonacci sequence Xn = Xn-49 * Xn-24. As it is free it costs nothing (0 €). It also allows expressing chemical formulas: FeS2 + O2 -> Fe2O3 + SO2.*

s'écrira en laissant les espaces, à quelques exceptions prés dont la suppression ne nuit pas à l'intelligibilité du texte :

SPIRALEQCAISQCAAQCAONEQCNTIMEQCNPADQCACRYPTOSYSTEMQCADESI
GNEDQCAINQCAQDCQDAQDBQDFQCPQDAQDFQCATOQCAREPLACEQCASOLIT
AIREQCAWHENQCAONEQCAHASQCANOQCACARDSQCOITQCAISQCABASEDQC
AINQCAPARTSQCAONQCATHEQCAGENERALIZEDQCAFIBONACCIQCASEQUEN
CEQCAXNQDNXNQCNQDEQDJQCKXNQCNQDCQDEQCOASQCAITQCAISQCAFR
EEQCAITQCACOSTSQCANOTHINGQCIQDAQKMQCJQCOITQCAALSOQCAALLO
WSQCAEXPRESSINGQCACHEMICALQCAFORMULASQDKFESQDCQCLOQDCQCN
QDOFEQDCOQDDQCLSOQDC

4. Références

1. Table des caractères Unicode, disponible à www.unicode.org/fr/charts/ ou fr.wikipedia.org/wiki/Table_des_caractères_Unicode
2. Diagonales – un chiffre par transposition, 2015.

Extrait du *Traité Élémentaire de Cryptographie*, F. Delastelle, 1902, pages 115 et 116.

Représentation des signes numériques et orthographiques

Note. - Le présent paragraphe est extrait de *L'Art de chiffrer et déchiffrer les dépêches secrètes*, par de Viaris.

Nécessité d'une convention. – Il peur arriver que, dans le courant d'une dépêche, on ait absolument besoin d'indiquer la ponctuation ou l'orthographe exacte d'un nom propre ; à coup sûr il arrivera que l'on ait à parler de nombres qu'il serait trop long de traduire en toutes lettres ; quel que soit le système employé, une convention s'impose.

Représentation des chiffres arabes et des nombres. – Voici celle que nous proposons. Les dix chiffres arabes seront représentés par les dix premières lettres de l'alphabet :

A	B	C	D	E	F	G	H	I	J
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**

et, pour avertir de leur signification numérique, on les encadrera entre deux K, ainsi KCK signifiera 3, et KCFIJAK : 36 901.

Les signes orthographiques. – Toutes les autres lettres de l'alphabet placées comme les dix premières entre deux K auront une signification de signes orthographiques :

L	M	N	O	P	Q	R
virgule	point	alinéa	exclamation	interrogation	guillemets	parenthèses
,	**.**		**!**	**?**	**« »**	**( )**

S	T	U	V	X	Y	Z
trait d'union	apostrophe	cédille	tréma	accent aigu	accent grave	accent circonflexe
-	**'**	**¸**	**¨**	**´**	**`**	**^**

Les signes relatifs aux nombres. – Mais on peut aussi, sans crainte de confusion, placer l'une de ces lettres entre deux des dix premières ou entre l'une d'elles et un K et alors lui donner

une signification différente et ayant rapport aux signes numériques. L signifierait « virgule » comme ci-dessus et 25,33 se traduirait par KBELCCK. Les autres lettres voudraient dire :

Q	R	S	T	U
numéro	terminaison ième	séparation de deux nombres	terminaison ièmement	exposant ou puissance

V	X	Y	Z
plus +	moins -	multiplié **x**	divisé /

Les lettres MNOP restent disponibles si l'on avait à établir d'autres conventions relatives aux nombres.

Donnons quelques exemples :

Numéro 27	:	KQBGK
Vingt-septième	:	KBGRK
27-32-14	:	KBGSCBSADK
Vingt-septièmement	:	KBGTK
27^4	:	KBGUDK
27 plus 32	:	KBGVCBK
32 moins 27	:	KCBXBGK
32 multiplié par 27	:	KCBYBGK
32 divisé par 27	:	KCBZBGK

Dans les conventions précédentes, nous n'avons pas parlé du point et virgule (;) qui se traduira par KMLK, ni des deux points (:) que l'on traduira par KMMK.

De Viaris. – *L'Art de chiffrer*, etc.

Chiffre$_{16}$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Valeur$_{10}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P

XX$_{16}$	**Caractère**	**Description**	**Code langue latine**	**Code langue germanique**
20		espace	WCA	QCA
21	!		WCB	QCB
22	"		WCC	QCC
23	#		WCD	QCD
24	$		WCE	QCE
25	%		WCF	QCF
26	&		WCG	QCG
27	‘		WCH	QCH
28	(		WCI	QCI
29	)		WCJ	QCJ
2A	*		WCK	QCK
2B	+		WCL	QCL
2C	,		WCM	QCM
2D	-		WCN	QCN
2E	.		WCO	QCO
2F	/		WCP	QCP
30	0		WDA	QDA
31	1		WDB	QDB
32	2		WDC	QDC
33	3		WDD	QDD
34	4		WDE	QDE
35	5		WDF	QDF
36	6		WDG	QDG
37	7		WDH	QDH
38	8		WDI	QDI
39	9		WDJ	QDJ
3A	:		WDK	QDK
3B	;		WDL	QDL
3C	<		WDM	QDM
3D	=		WDN	QDN
3E	>		WDO	QDO
3F	?		WDP	QDP
40	@		WEA	QEA
5B	[		WFL	QFL
5C	\		WFM	QFM
5D	]		WFN	QFN
5E	^		WFO	QFO
5F	_	barre horizontale	WFP	QFP
A1	¡	exclamation inversé	WKB	QKB
A2	¢	centime	WKC	QKC
A3	£	livre, lire	WKD	QKD
AC	€	euro	WKM	QKM
B0	°	degré	WLA	QLA

BF	¿	interrogation inversé	WLP	QLP
DF	ß	eszett	WNP	QNP
E0	à		WOA	QOA
E7	ç		WOH	QOH
E8	è		WOI	QOI
E9	é		WOJ	QOJ
EA	ê		WOK	QOK
F1	ñ	n tilde	WPB	QPB
F7	÷	division	WPH	QPH
F9	ù		WPJ	QPJ