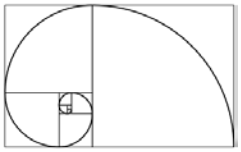


SPIRALE
Le chiffrement manuel revisité[1]

Philippe Allard
AMD-crypto@orange.fr

Plan

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 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

[1] Ce document est la traduction de l'article originel en anglais disponible prochaînement à http://eprint.iacr.org/2015/835.pdf

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.

2. Généralisation de la suite de Fibonacci

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. Le but étant ici de créer un long masque à partir d'une chaîne de lettres de longueur k faisant fonction d'amorce, 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… 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.

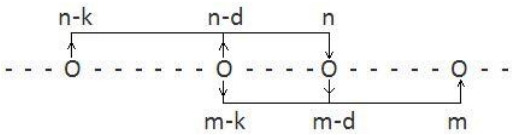
Pour éviter ces derniers défauts l'idée est aussi de repousser le premier terme, par exemple à l'autre bout lui aussi :

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

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 :

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

Nous préférons 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 :



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 :

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

d'où $$k = 2d \qquad (1)$$

3. Génération de la séquence amorce

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, 5, 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				

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}

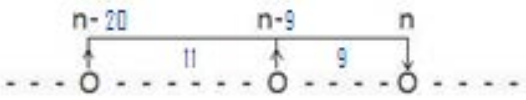
Et elle pourrait être utilisée comme séquence amorce de la récurrence linéaire :

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

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 :



4. Généralisation de l'addition congruente

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 :

⊕	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

Il jouit de propriétés particulières:

Symétrie $X \oplus Y = Y X \oplus X$

Surjectivité $3 = 1 \oplus 2 = 5 \oplus 8 = 6 \oplus 7$ $5 = 2 \oplus 3 = 9 \oplus 6 = 7 \oplus 8$ …

Nombre égal de valeurs résultat et un nombre égale de pré-images pour chacune d'elles

Cette dernière propriété, une surjectivité uniforme, 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.

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, par exemple :

□	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

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. 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

C’est la même table de chiffrement, et l’opérateur associé, qui serait maintenant utilisée pour générer la séquence amorce et non plus la simple addition congruente utilisée dans l’exposé préliminaire du paragraphe 4.

5. Algorithme de permutation

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;

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 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, et comme

$$2^{128} \approx 26^{27,2}$$

Cela signifie qu'avec une clé globale de 28 lettres l'objectif est largement atteint. 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.

Il reste le problème de fournir en sécurité suffisamment de clés aux correspondants. Nous suggérons la procédure suivante, contre l'attaque par dictionnaire, pour les créer : par convention entre correspondants un livre est choisi et une page utilisée par message ; dans cette page ils prennent les 7 premières lettres et les 7 dernières, indépendamment des mots ou de la ponctuation, de la première ligne et de la dernière ligne (mais d'autres règles de choix conviendraient aussi) ; ils les écrivent ensuite, un extrait par ligne, dans un tableau 7x4 puis le lisent verticalement depuis le coin supérieur droit. Cela revient à inverser ces chaînes de caractères et à les entrelacer. Et finalement ils découpent 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

Cette procédure est très simple mais a un défaut lié à l'usage d'un livre : les probabilités d'occurrence des lettres dans les clés sont naturellement proches de celles des lettres du langage du livre et donc non égales. Une façon simple de corriger partiellement ce défaut serait de remplacer dans les chaînes sélectionnées quelques lettres des plus hautes fréquences

[2] *A Farewell to Arms*, E.Hemingway, p81, Charles Scribner's Sons edition.

(e-t-a-o-i-n en Anglais, e-a-s-i-n-t en Français) par des lettres des plus basses fréquences (z-q-x-j-v en Anglais, w-k-z-y-j en Français). Les clés corrigées de l'exemple précédent pourraient alors être : NVIKKIH, CTSQEOU, DNGDKSZ et EAIWDSH.

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 en exemple[3] complet bâti avec les clés définies plus haut :

- 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.

- 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}	…

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

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[4] 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 certaines clés communes à ciphertext 1 et 2;
- 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

[4] 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.

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

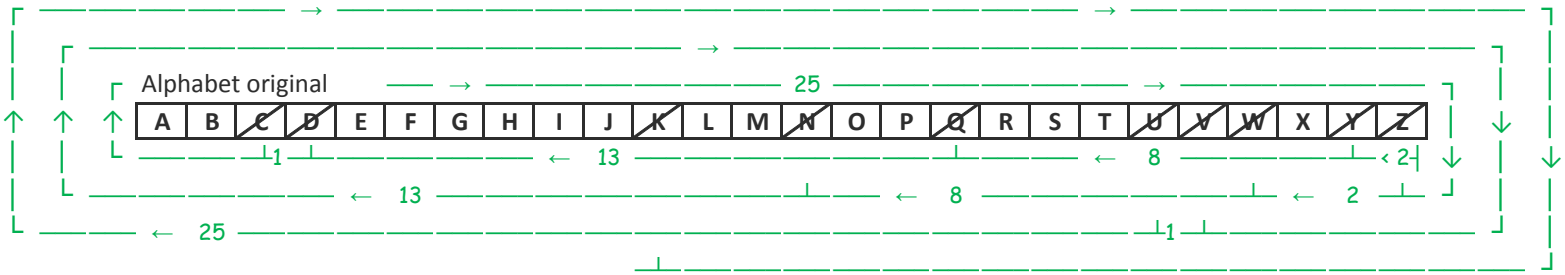
1. B. Kallick, Handycipher: a Low-tech, Randomized, Symmetric-key Cryptosystem (2014), version 4.9, available at http://eprint.iacr.org/2014/257.pdf
2. B. Schneier, The Solitaire encryption algorithm, version 1.2, (1999), available at https://www.schneier.com/solitaire.html.

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

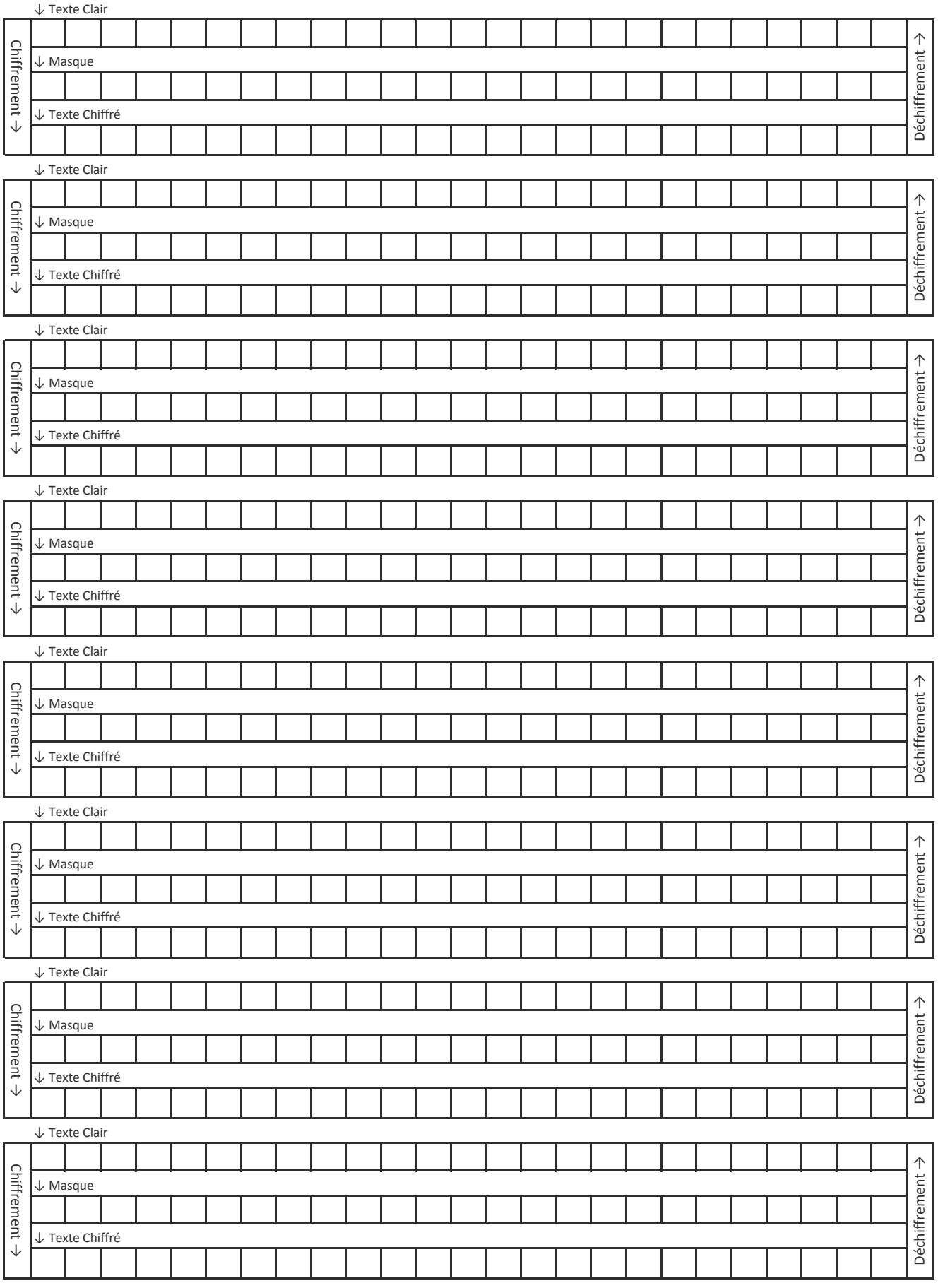
puis remplissez les 49 premières cases ci-dessous en lisant la matrice diagonalement depuis le coin supérieur gauche

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 part on generalized fibonacci sequence xn = xn-49 * xn-24. As it is free it costs 0 €. It allows too to express chemical formulas: FeS2 + O2 -> Fe2O3 + SO2.

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@MTH1T@X%*"AHE:9QR@F@@TDT€£0DECK$N"'NO8>P:E£*H0 X’C 4FI7YC693&=&-
£.K^.A72J*.O’RG)(S820XX<YX/U(€PQWCN/,GL(5XE7FE689%87>ZM2 =X3-"F4%DI,I>0./"B@A">.W/P ",I1C/RA&"&Z<49T65(L-EG*5Z6OO*1B)€A
TKKL-XCMIR4€£6Z€%<A’2V6./€/6KQ2=T'A&U%(VY/XYZ7@9@^RZC^H-D3<O<*X+K%.:CXM8^KQ=

```
>>>   -- 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 (274 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%560=4EAM18F’)Y'XPA::2H£J.C^B>E'"B'/LB
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 PART ON GENERALIZED FIBONACCI
SEQUENCE XN = XN-49 * XN-24. AS IT IS FREE IT COSTS 0 €. IT ALLOWS TOO TO EXPRESS
CHEMICAL FORMULAS: FES2 + O2 -> FE2O3 + SO2.

Ciphertext: DY2R"S7->EQFS@MTH1T@X%*"AHE:9QR@F@@TDT€£0DECK$N"'NO8>P:E£*H0 X’C
4FI7YC693&=&-£.K^.A72J*.O’RG)(S820XX<YX/U(€PQWCN/,GL(5XE7FE689%87>ZM2
=X3-"F4%DI,I>0./"B@A">.W/P ",I1C/RA&"&Z<49T65(L-EG*5Z6OO*1B)€A
TKKL-XCMIR4€£6Z€%<A’2V6./€/6KQ2=T'A&U%(VY/XYZ7@9@^RZC^H-D3<O<*X+K%.:CXM8^KQ=
```