STANDARD FORM NO. 64

Office Memorandum • UNITED STATES GOVERNMENT

TO : Mr. William F. Friedman, Special Assistant.

DATE: 31 August 1954.
J.Fisher

FROM : NSA-7641

SUBJECT: L'Indice de coincidence et ses applications en cryptographie, attachment to KJ-6642(o), 3 August 1954, TOP SECRET CONTROL U.S. OFFICIALS ONLY.

1. Enclosed are copies of pages 1 and 2 of the above document in accordance with your request. Included also is a copy of page 69, since this material is not found in the Paris 1921 edition of L'Indice de Coincidence et ses Applications en Cryptographie.

2. A letter from HQ ASA Europe dated 8 December 1950, enclosing the German translation of L'Indice de Coincidence et ses Applications en Cryptographie by Colonel Andreas Figl, stated that also enclosed were supplementary chapters prepared by Carl Martin to Figl's book on cryptanalysis. (IR-84450, TOP SECRET). The signature of the donor who presented this work to Colonel Figl on Christmas in 1937 might be "Martin".

Francis A. Rupp
Francis A. Rupp
Chief NSA-7641

A b s c h r i f t .

L'Indice de coincidence et ses applications en cryptographie

par
FABYAN.

Paris
(ca 1921)

(L'I)

Bemerkung:

Diese Abschrift stimmt mit einer Abschrift des Originals - das mir nicht zugaenglich ist - ueberein. Aus diesem Grund kann auch keine Garantie uebernommen werden, das diese Abschrift in jedem Detaille mit dem Original uebereinstimmt.

INTRODUCTION

En cryptographie, les tableaux de fréquence ne sont généralement pas considérés comme ayant les propriétés bien définies des courbes mathématiques ou statistiques. Le simple but de tels tableaux est habituellement de permettre au cryptologue décrypteur de faire certaines hypothèses relatives à l'équivalence des lettres du texte chiffré qu'il étudie aux lettres du texte clair correspondant, ces hypothèses étant basées sur la correspondance des fréquences des lettres qui constituent le langage clair et de celles qui se trouvent dans le texte chiffré.

Les cas où les indications numériques des tableaux de fréquences peuvent être utilisées telles quelles et sans l'intervention d'aucune analyse cryptologique, sont plutôt rares. Mais quand cela est possible, ces tableaux fournissent les éléments d'une méthode de décryptement purement mathématique et dont l'application rationnelle est des plus utiles et des plus sûres.

Dans la présente Notice, deux exemples d'une telle méthode, conduisant à la solution mathématique de chiffres relativement complexes, seront donnés en detail.

L'Indice de coincidence et ses applications en cryptographie

par
FABYAN.

Paris
(ca 1921)

Bemerkung: Angeblich wurde dieses Werk seinerzeit vom franzoesischen Generalstab zurueckgezogen.

~~TOP SECRET~~

~~SPECIAL HANDLING REQUIRED~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~The information contained in this document will not be disclosed to foreign nationals or their representatives~~

Dans le premier exemple (Chapitre 1), on montrera comment un système cryptographique comportant l'emploi de plus de cent alphabets intervertis inconnus, peut être résolu sans faire une seule hypothèse au sujet du contenu du texte clair.

Dans le deuxieme exemple (Chapitre II), on verra comment un système comportant un emploi quèlque peu compliqué de substitution à alphabets multiples et de transposition, peut être résolu avec un seul message de longueur moyenne.

On espère que ces solutions intéresseront les étudiants cryptologues, par le fait qu'elles illustrent bien le principe de la méthode à laquelle il est fait allusion plus haut.

Nota.- Pour la commodité de la lecture, les Tables et Figures dans le texte, sont reportées à la fin de chaque chapitre.

-.-.-.-.-.-.-.-.-.-.-.-.-

CHAPITRE PREMIER

.....

S Y S T E M E V O G E L

A. — DESCRIPTION SOMMAIRE

Ce système comporte l'emploi d'un appareil composé essentiellement de six disques concentriques: cinq disques mobiles et un disque exterieur fixe (Fig.1).

Ces six disques sont divisés en 26 segments égaux.

Sur chacun des cinq disques mobiles, numérotés de 1 à 5 a partir du disque extérieur, est inscrit un alphabet interverti: les cinq alphabets sont différents.

Sur l'un des segments du disques extérieur fixe, est inscrite l'indication clair et sur les suivants, dans le sens de la rotation des aiguilles d'une montre, les numéros successifs d'une clef numérique qui doit avoir au plus 25 numeros.

Si la clef numérique a moins de 25 numéros, il reste des segments en blanc à gauche de celui qui porte l'indication clair.

Les cinq alphabets intervertis et la clef numérique constituent les éléments secrets du système, ceux qui ne doivent être connus que des seuls correspondants qualifiés.

Décryptement du Système Cryptographique du commandant SCHNEIDER Paris 1921.

AVANT - PROPOS

Dans l'exposé de la méthode de décryptement du système SCHNEIDER, il est fait allusion à la méthode des coincidences exposée dans une autre brochure.

Nous rappelons ci-après les définitions adoptées dans l'exposé de cette méthode.

Si l'on considère deux séquences de fréquences:

	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)	.	2	1	2	2	1	2	1	.	.	.	1	.	.	2	2	.	1	.	2	2	.	.	.	.	.
2)	.	5	1	1	.	4	.	.	.	2	2	1	.	.	2	6	.	.	2	.	7	2	.	.	.	.

On appelle:

COINCIDENCES, les fréquences communes deux séries;
NON COINCIDENCES, les différences des fréquences correspondantes des deux séries;
DIFFERENCE, le résultat de la soustraction du nombre des non coincidences du nombre des coincidences;
INDICE DE COINCIDENCE, le quotient de la différence par le nombre total des fréquences des deux séquences comparées.

Ainsi, pour les deux séquences ci-dessus, on aurait:

	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	Totaux
1)	.	2	1	2	2	1	2	1	.	.	.	1	.	.	2	2	.	1	.	2	2	.	.	.	1	.	21
2)	.	5	1	1	.	4	.	.	.	2	2	1	.	.	2	6	.	.	2	.	7	2	.	.	.	.	35
Coincidences	.	2	1	1	.	1	.	.	.	.	.	1	.	.	2	2	.	.	.	.	2	.	.	.	.	.	12
Non Coincidence	.	3	.	1	2	3	2	1	.	2	2	.	.	.	.	4	.	1	2	2	5	2	.	.	.	.	32

nombre des lettres . . . . . 21 + 35 = 56
difference . . . . . 12 ⁻ 32 = -20
-20 = -0.35
Indice de coincidence: 56

Dans la pratique, il est inutile de compter le nombre des <u>non coincidences</u> pour trouver les différences: il suffit de retrancher le nombre de lettres de 3 fois le nombre des <u>coincidences</u>.

Dans l'exemple ci-dessus en effet: 3 fois 12 moins 56 donne -20.

Ce sont les DIFFERENCES seules qui sont utilisées, concurremment avec les nombres de lettres, pour établir les INDICES DE COINCIDENCES.