

Quelle confiance dans la cryptologie ? Une approche historique.



Philippe Guillot,

ARCSI

et

Université Paris 8,

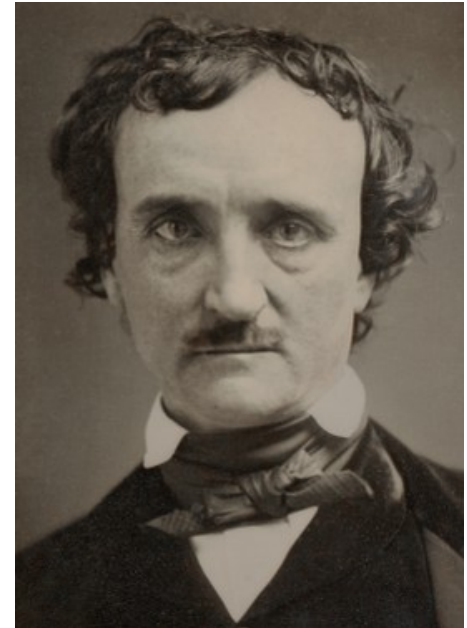
département de mathématiques et d'histoire des sciences





Blaise de Vigenère (1523-1596) en 1585 :
« Il se trouvera à l'encontre assez de manières de chiffres du tout inexpugnables et invincibles à qui n'en aura le secret. »

Edgard Poe (1809-1849) en 1841 :
« L'intelligence humaine ne peut concocter un chiffrement que l'intelligence humaine ne puisse résoudre. »





Fritz Nebel (1891-1977)



George-Jean Painvin (1886-1980)

	A	D	F	G	V	X
A	c	o	8	x	f	4
D	m	k	3	a	z	9
F	n	w	l	0	j	d
G	5	s	i	y	h	u
V	p	1	v	b	6	r
X	e	q	7	t	2	g

FGAXA XAXFF FAFFA AVDFA GAXFX FAAAG DXGGX AGXFD XGAGX GAXGX
 AGXVF VXXAG XFDAX GDAAF DGGAF FXGGX XDFAX GXAXV AGXGG DFAGD
 GXVAX VFXGV FFGGA XDGAX ADVGG A



Édit de Louis XI du 19 juin 1464,
articles 13 et 14:

*« Les courriers et messagers seront visitez par
les commis du grand maistre auxquels ils
seront tenus d'exhiber leurs lettres pour
connoistre s'il n'y a rien qui porte préjudice au
service du Roy et qui contrevienne à ses édits
et ordonnances. »*

<http://www.cosmovisions.com/Cabinet-Noir.htm>



Antoine Rossignol (1600-1682)



Étienne Bazeris (1846-1931)



NSA

The National Security Agency/Central Security Service (NSA/CSS) leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances.

www.nsa.gov/about/mission-values



Blaise de Vigenère, traité des chiffres 1585

« L'écriture est double : la commune dont on use ordinairement, et l'occulte secrète qu'on déguise d'infinies sortes selon sa fantaisie pour ne la rendre intelligible qu'entre soi et ses consachants. Les yeux de l'âme du commun peuple ne sauraient bonnement supporter les lumineux étincellements de la divinité. (...) Afin de les garantir et soustraire du profanement de la multitude, et en laisser la connaissance aux gens dignes, à peu de gens divulguez artifices. »



Al Kindi (801 – 873)

Sur l'extraction de l'obscur

« J'aurais préféré suivre la voie des savants qui m'ont précédé et qui pensaient à obscurcir les trésors de la signification plutôt que de les afficher et de les révéler (...) Par conséquent, j'ai écrit sur ce sujet ce que je pensais être assez clair pour les fils de la sagesse, tout en restant hors de portée des personnes non informées. Que Dieu m'apporte le succès. »

LA CIFRA DEL SIG.
GIOVAN BATTISTA
BELASO, GENTILHOMO
BRESCIANO NVOVAMENTE
DALVI MEDESIMO RIDOT-
ta à grandissima breuità
& perfettione.

LAQVAL CIFRA, BENCHE SIA STAMPATA,
CONTIENE IN SE QVESTA MARAVIGLIOSA
bellezza, che tutto il módo potrà ufarla, & nientedimeno, l'uno
non potrà leggere quello che scriue l'altro; se non sola-
mente quei che haueranno tra loro, un breuissimo contrafegno;
come in questo medesimo foglio s'insegna, insieme cò la
sua dichiarazione, & col modo d'adoperarla.



IN VENETIA, M D LIII.



Joh. Franc. Com. de Gronsfeld.
S.C.M. Gen. Camp. Marejch.



Joan Gronsfeld (1640-1719)

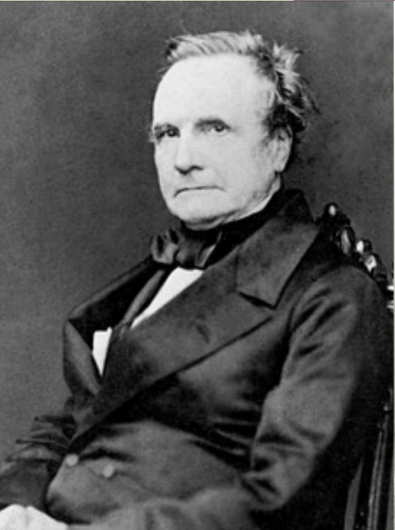
Francis Beaufort (1774-1857)

John Wilkins (1614-1672)

Friedrich Kasiski (1805-1881)

Charles Babbage (1791-1871)

William Friedman (1891-1969)



La cifra del signor
Giovan Battista Belaso
1553

P
54
U. 92

SCIENTIFIC AMERICAN SUPPLEMENT

NEW YORK, JANUARY 27, 1917



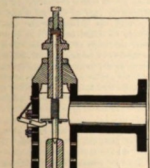
Remains of the Imperial Tribunal, at Rome.

Scientific American supplément du 17 janvier 1917

A Simple Carburetor

No portion of an automobile, or, for that matter, any internal combustion engine, is more important and interesting than the carburetor, and thousands in every land are engaged in strenuous study of the problem of supplying fuel to the engine in the proper form and proportion to secure the greatest efficiency. The results of these studies are seen in the countless devices that are introduced each year, and a noticeable feature of the majority of these devices is their complication. This is undoubtedly due to efforts toward carbureting device automatic under operation, part hands of unskilled operators, who must substitute a very great majority of these v of this class. To anyone, however, wh study of the variations of the barometer, v locality, and also take into consideration the constantly changing character of the fuels supplied, the quest for a completely automatic carburetor, under all circumstances, can hardly fail to appear hopeless; and added to everything else is the human proclivity of "expert-menting" that prevails among engine operators, and results in alterations in the delicate adjustments of these complicated devices that must horrify their designers.

Taking everything into consideration a serious question arises as to the desirability of intruding delicately



A simple float

As there is no float chamber, trued by a needle pressed b has a central seating. A, A to enable the section of the the jet, and as the needle needle is lifted higher and i extreme lift of the needle is top of the carburetor. At by the lever on the left, wh the jet and mix with the of holes in the casing, as latterly throttle, but also extra air valve, if desired. air line around the air port good results are obtained from a fifty per cent mixture of gasoline and paraffin. It is stated that the carburetor will work equally well in any position.

contrived devices in the hands of the unskilled public; and even as to the real desirability and real effectiveness of many of the wonderful attachments found on latter-day carburetors.

A refreshing variation on the ordinary practice of adding a specially contrived attachment to the basic elements of all carburetors for the purpose of meeting each conceivable condition is seen in the accompanying sketch which illustrates a carburetor recently brought out in England. As will be seen this device consists only of a containing casing, containing a simple jet and a needle valve, to which is attached a disk that lifts and lowers in resonance with the varying sound of the engine; and an especially notable feature is the fact that there is only one adjustment provided for in the entire apparatus.

This instrument is not presented as a perfect device, but merely as a suggestion that similar simplicity might well be studied, particularly in view of the mechanical qualifications of those who use carburetors.

Size of Particles of Sand and Dust

As showing the great difference in surface area between relatively fine and coarse sands and dust, it has been calculated that a pound of sand divided into five fractions contains 120,000,000 particles having a surface area of 44,278 square feet; 2000; 100,000,000; and 100,000,000.

found to contain 22,075,824 particles to the pound and had 60,500 square feet of surface, while a pound of dust was found to consist of 192,715,378,000 particles, representing 527,821 square feet.—The Engineer.

A New Cipher Code*

WHEATON defines a cipher as "a private alphabet, system of characters or other mode of writing, contrived for the safe transmission of secrets, also a system by which, abstractedly, a cipher key is defined

A New Cipher Code*

the missing code by possible enemies make necessary the adoption of an entirely new system for transmitting messages by cipher to and from our foreign representatives and agents.

Cipher codes are a necessary adjunct to the conduct of governmental affairs, especially in time of war, but

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	B	C	D	E	F	G	H</																		



$$26 \times 25 \times \dots \times 1 =$$

403 291 466 112 665 635 584 000 000



Mais je dirai bien davantage, car non que de trois enveloppes tant seulement, ainsi de cinquante, voire cent mille, et encore plus jusqu'en infini que cela s'étend, que puissent être réitérés ces surchiffrements, d'alphabet en alphabet les uns sur les autres, il n'importe de rien auquel de tous vous vous preniez pour le déchiffrer, étant en cela tous égaux, autant le dernier comme le premier ou second.

Борукы

А: 24.

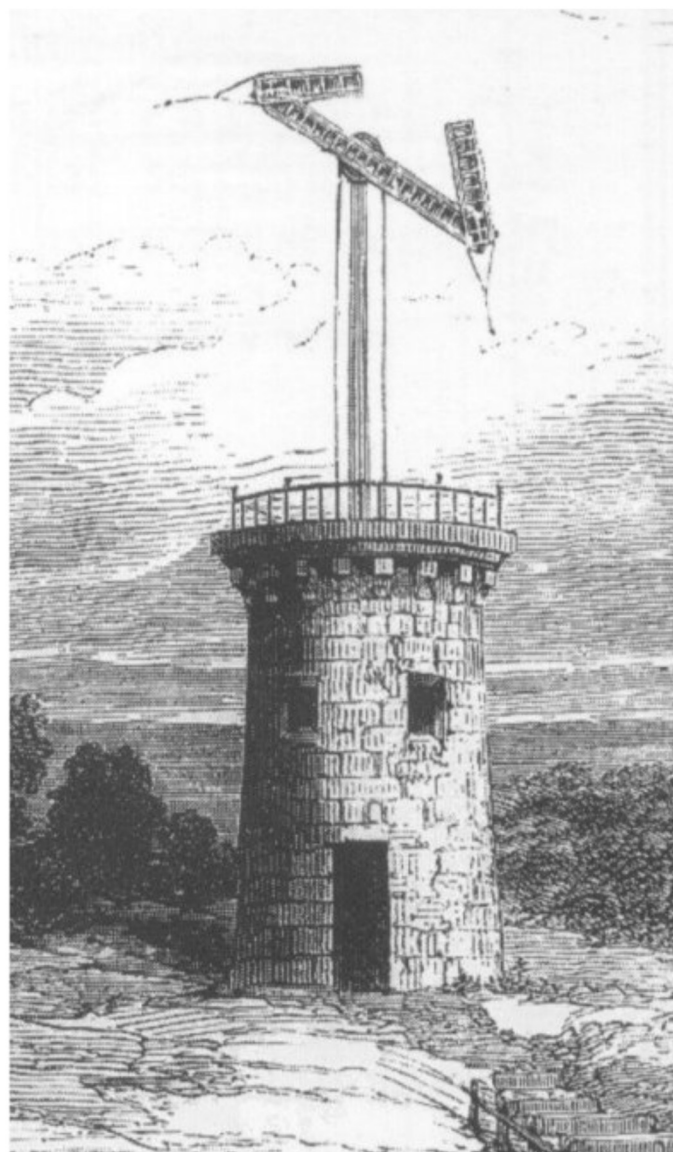
	0	1	2	3	4	5	6	7	8	9	
0	к.	щ.	н.	се.			но.	го.	г.	во.	0
1	ки	от	ти		га.	с.	ре.	у.	г.	ча.	1
2	ко.		тн.	бе.	ме.	ка.	в.	ве.	ле.	ла.	2
3	г.	лж.	ше.	во.	ру.	мо.		б.	ок.	те.	3
4	х.		си.	то.	ц.	да.	ча.	ми.	л.	кба.	4
5	р.	ро.	ва.	бо.	а.	о.	ло.	ба.	х.	ш.	5
6	то.	зе.	ве.	ка.	за.	ки.	ги.	жа.	фо.	не.	6
7	ла.	ти.	са.	е.	им.	ра.	т.	со.	де.	ки.	7
8	об.	зо.	сж.	л.	та.	ли.		ва.	о/са.		8
9	о/с.	ю.		к.	б.	ше.	на.	но.	ф.	по.	9
	0	1	2	3	4	5	6	7	8	9	

Борукыт. Борукыт.
д. 5/12 1920г.

Jan Kowalewski

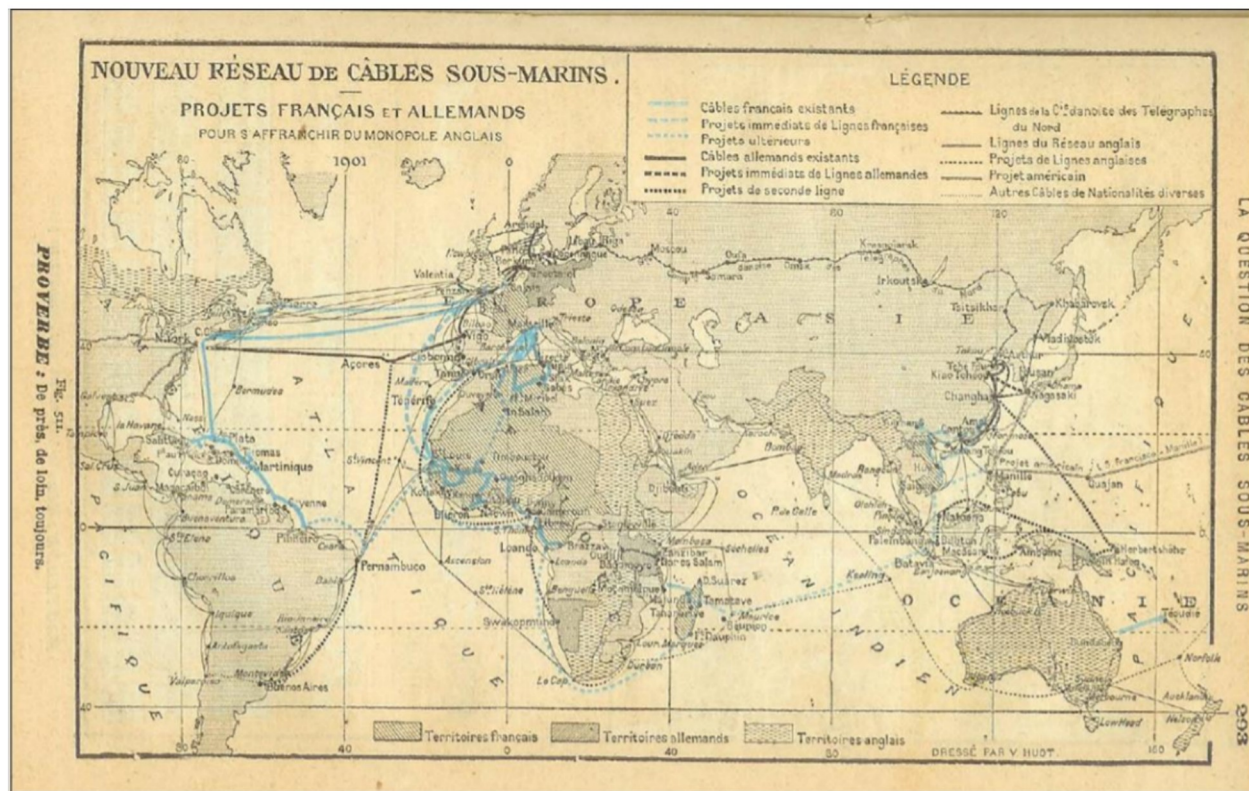


Wacław Sierpinski



PROVERBE : De près, de loin, toujours.

H. GIL.



Quarterly review 1853

Des mesures devront être prises pour parer à une sérieuse objection que l'on soulève à propos des communications privées par télégraphe – la violation du secret – car, dans tous les cas, une demi-douzaine de personnes sont amenées à connaître chaque mot adressé par une personne à une autre. Les employés de la Compagnie Anglaise du Télégraphe s'engagent au secret sous serment, mais nous écrivons souvent des choses que nous ne supporterions pas de voir lues par d'autres avant nous. C'est encore un grave défaut du télégraphe, et il faut y remédier d'une manière ou d'une autre.

DICTIONNAIRE ABRÉVIATIF

CHIFFRÉ

PAR F.-J. SITTLER

4^{me} Édition.

PARIS

IMPRIMERIE LEFEBVRE

Passage du Caire, 87-89.

1879

CORRESPONDANCE SECRÈTE

La loi du 13 Juin 1866 accorde au public la faculté de correspondre en chiffres par le télégraphe.

L'extrême importance de ce mode de communication ne peut échapper à personne. Il est aussi utile dans les relations de famille et les transactions commerciales, que dans les rapports diplomatiques.

Le **Dictionnaire chiffré**, de F.-J. SITTLER, composé dans le but de faciliter la rédaction et la traduction des dépêches secrètes, renferme à peu près tous les mots et expressions d'un usage fréquent.

Pour employer le langage secret, au moyen de ce Dictionnaire, *il suffit d'indiquer à son correspondant la page et la ligne où se trouve le mot ou l'expression qu'on veut lui transmettre*

A cet effet, on adopte d'un commun accord, une *pagination conventionnelle*, en employant dans un ordre quelconque, les numéros depuis 00 jusqu'à 99, et une *combinaison également conventionnelle* des deux chiffres de la page avec ceux de la ligne.

EXEMPLE : Supposons que la première page reçoive le

00	Faire courir le bruit.
01	Des bruits inquiétants.
02	Brûler, brûlure.
03	Brun.
04	Brusquer, brusquerie.
05	Ne brusquez pas.
06	Brusque, brusquement.
07	Brut.
08	Brutalité.
09	Brutal, brutalement.
10	Bruxelles.
11	Bruyant, bruyamment.
12	Bu (syll.).
13	Bucharest.
14	Budget.
15	Bulgare.
16	Bulgarie.
17	Bulletin.
18	Bureau.
19	But.
20	Dans le but de.
21	Dans quel but.
22	Dans un but.
23	Butin.
24	Butte.
25	En butte à, aux.
26	<i>Boziers</i>
27	<i>Blais</i>
28	<i>Bourges</i>
29	<i>Brest</i>
30	<i>Berthier Adolphe</i>
31	<i>Berthier Edouard</i>
32	<i>Banque d'Hypothèque</i>
33	<i>Bureau auxiliaire des Rentes</i>
34	<i>Bureau A Lyon</i>
35	<i>Bureau B Lyon</i>
36	<i>Bureau C Lyon</i>
37	<i>Bureau auxiliaire des Rentes</i>
38	<i>Banque d'Escompte</i>
39	
40	
41	
42	<i>Bourges à Lyon</i>
43	C (lettre).
44	C (syll.).
45	Cabale.
46	Cabine.
47	Cabinet.
48	Cable.

80	Cachemire.
81	Cacher, cachette.
82	Cacheter, cachet.
83	Cachot.
84	Cadastre.
85	Cadavre, cadavéreux.
86	Cadet.
87	Cadrer, cadre.
88	Caen.
89	Café.
90	Cahier.
91	Caïd.
92	Caisse.
93	A la caisse
94	En caisse.
95	Caissier.
96	Caïsson.
97	Calais.
98	Calamité.
99	Calculable.
100	Calculer, calcul.
101	Calèche.
102	Calibrer, calibre.
103	Calicot.
104	Calme.
105	Calomniateur.
106	Calomnie.
107	Calomnier.
108	Avoir été calomnié.
109	Calvados (le).
110	Camarade.
111	Camaraderie.
112	Camp.
113	Camp de Châlons.
114	Campagne.
115	A la campagne.
116	de campagne.
117	En campagne.
118	Camper, campement.
119	Canaliser, canal.
120	Candidat.
121	Candidat du Gouvernement.
122	Candidat de l'opposition.
123	Candidat indépendant.
124	Candidat libéral.
125	Candidature.
126	Candie.
127	Canne.
128	Canon.
129	Canon rayé.

00	Canonner, canonnade.
01	Canonnier.
02	Canot.
03	Canton, cantonnal.
04	Canton de.
05	Cantonnement.
06	Cap.
07	Capable.
08	Capacité.
09	Capitaine.
10	Capitaine de cavalerie.
11	Capitaine d'état-major.
12	Capitaine d'infanterie.
13	Capitaine de gendarmerie.
14	Capitaliser, capital, capitale.
15	Capital social.
16	Capitaliste.
17	Capituler, capitulation.
18	Capote.
19	Capter, captation.
20	Captiver, captivité.
21	Captif.
22	Capturer, capture.
23	Car.
24	Carabine.
25	Carabinier.
26	Caractère, caractériser.
27	Etre d'un caractère.
28	Carat.
29	Cardinal.
30	Cargaison.
31	Caricature.
32	Carnage.
33	Carré, carrément.
34	Carrière.
35	Carrousel.
36	Carte.
37	Carte d'Europe.
38	Carte de France.
39	Cartouche.
40	Cas.
41	Dans ce cas.
42	Dans le cas où, que.
43	Dans tous les cas.
44	En cas de.
45	En tous cas.
46	Casbah.
47	Casemate.
48	Casermer, caserne.
49	Casernement.

50	Casquette.
51	Cassation.
52	Se pourvoir en cassation
53	Casser.
54	Catastrophe.
55	Catégorie.
56	Catégorique, catégoriquement
57	Cathédrale.
58	Catherine.
59	Catholicisme, catholique.
60	Cause.
61	A cause de.
62	En cause.
63	Etre cause de (que).
64	Pour cause de.
65	Causser, causerie.
66	Avoir causé.
67	Caution.
68	Cautionner, cautionnement.
69	Cavalerie.
70	Cave.
71	Cavour.
72	Cayenne.
73	Ce (syll.).
74	Ce, cet, cette.
75	Ce, dont.
76	Ce que.
77	Ce qui.
78	A ce.
79	A ce que.
80	Dans ce.
81	De ce.
82	De ce que.
83	De ce qui.
84	En ce que.
85	En ce qui.
86	Pour ce.
87	Sur ce.
88	Tout ce que.
89	Tout ce qui.
90	Ceci.
91	Céder.
92	Cédez.
93	Ne pouvons céder.
94	Pouvez-vous céder.
95	Ceinture.
96	Cela.
97	Célèbre.
98	Célébrer, célébration.
99	Célébrez.

MINISTÈRE
DE LA GUERRE
ÉTAT-MAJOR DE L'ARMÉE
2^e Bureau
Section des Renseignements

RÉPUBLIQUE FRANÇAISE
DÉPÊCHE TÉLÉGRAPHIQUE

Paris, le 18 Août 1915

18-18 Août 1915
162
C. de...

VERRELSKI, LONDON

N° 8394 - 2- S.R.
11

CXCX2	27592	63300	11100	81538	95198
46727	74627	03126	38192	64121	67026
63392	61015	53629	25323		

Pour le Ministre et par son ordre:
Pour le Général,
Chef d'Etat-Major Général,
Le Colonel Adjoint.

Salisbury

SECRET, OR CYPHER WRITING.

Sm.—Permit me, through the "Journal of the Society of Arts," to make known a system of secret (or cypher) writing I have lately invented and patented the apparatus, and to enclose, for the acceptance of the Society, the apparatus devised for its practical application, which, I believe, will be found to answer all the purposes intended. It is formed, as you perceive, of a series of fixed alphabets printed in *black letters*,

for instance, you wish to
Begin at the left hand,
the next slide move down
black K, and so on until
last slide, which is not
any writing you may wish
communicate the sentence
Begin by spelling from
letter as the cypher:

that, even in this short message, the letter *A* is represented by *B, Q*, and *X*. *B* also represents *H, A*, and *E*. *I*, again, is represented by *R, C*, and *N*, and thus leaves no clue to the deciphering, which I feel certain is impossible under the conditions of the present message. The key of the *micrograph* against *U* would appear thus:—*A, V, I, S, Y, F, I, X, B, A, A, B, V, B, I, T, Q, Y, R*; in these three *B*'s are together, representing *N, T, E*. You may thus vary your alphabet as you please, and still be unable to be deciphered without the key, but with it is as equally easy. It must be at once apparent that the complexity may be much increased by permutating (on well-known principles) each of the moveable alphabets, and in many cases, I believe, it may be made so complete as need be. Of course, the reading and writing may be indifferently from the fixed to the moveable, or the contrary, from left to right, or from right to left, and in any of these variations, and which may be agreed upon by the parties corresponding. You can, with the little apparatus now sent, use a key to the extent of twenty letters; thus, your key is *physically impossible*; spell two letters at a time, using both the *micrograph* and the *microfilm* keys. The keys may be used in like manner, and to any extent.

I need hardly observe that this system is applicable to any language. Its uses must be obvious to all, and the further employment of it will be of great help at the present day (the sheet is certainly) for by its means messages of the most private character may be sent, and not a chance of discovery. This fact I have proved, as well by I communicated with my friend Mr. Coathupe, addressing him from London, and on the same day, July the 20th, sent to the *Times* a short note, which appeared on the 21st, in the second paragraph, second column; it is this:—
G Z Z E S, G V, T N S R X W Y F U O, L X
E O S,
S L U,
S D,
V. B.
The above
discovers of

every of 60

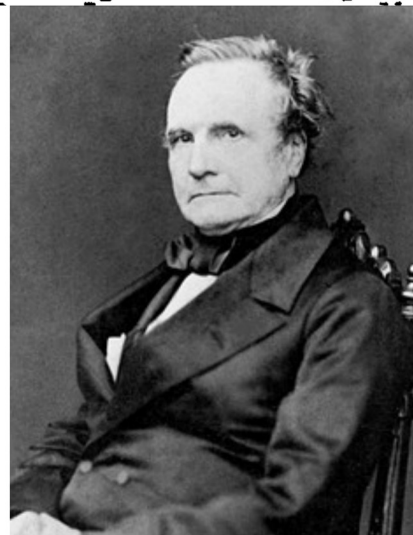
discovery of some
mutation." (initials), as he
proved to be a

licity is not at first desirable.

To all public bodies, who are in the habit of enquiring by telegraph, it is evident it must prove useful, for, at

SECRET, OR CYPHER WRITING.

SIR,—Permit me, through the “Journal of the Society of Arts,” to make known a system of secret (or cypher) writing I have lately invented and patented the apparatus, and to enclose, for the acceptance of the Society, the apparatus devised for its practical appli-



"By this communication I claim precedence in the discovery of secret correspondence on the principle of permutation." The $VBBV$, is read by $JHBT$ (my

and these alternating with another series of double alphabets in *red* letters*; the latter moving in grooves. By this arrangement you can, at pleasure, form any word or words in a line with any letter on the fixed alphabets;

* The red letters are here represented by the capitals in *italics*. Of the four examples which Mr. Thwaites refers to, it has been considered necessary to illustrate only one.



Auguste Kerckhoffs (1835-1901)

Auguste Kerckhoffs

La cryptographie militaire, 1883 :

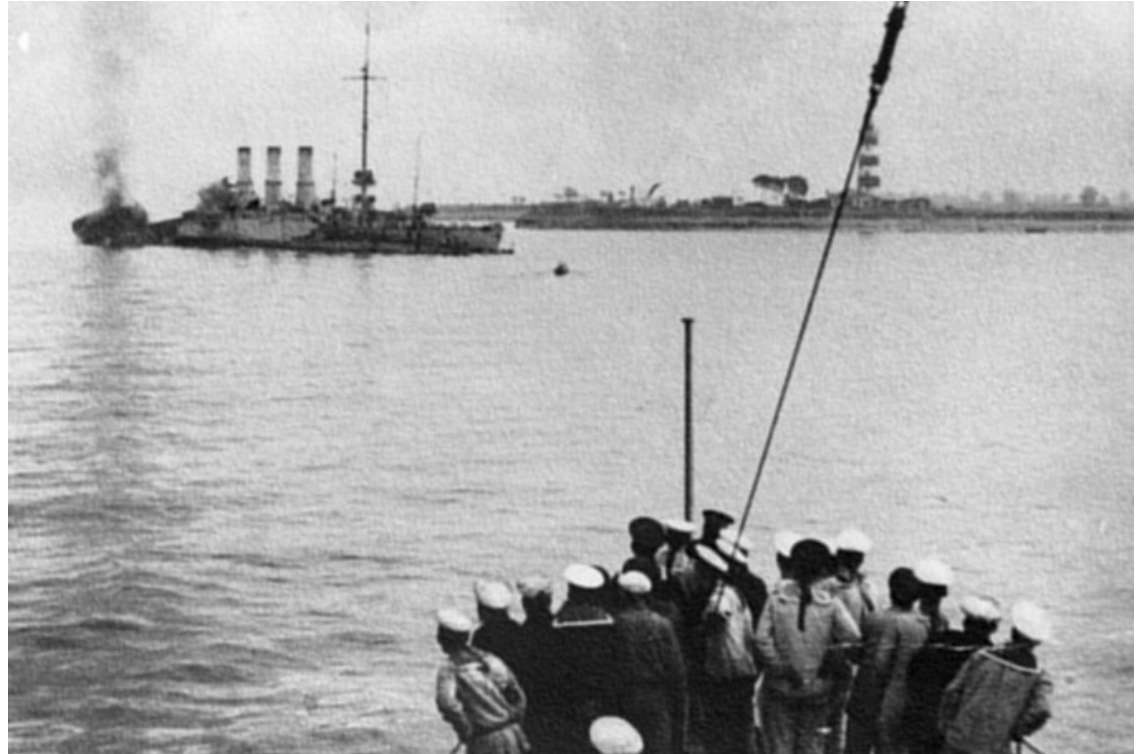
« Je tiens en terminant, à insister sur ce point, que la valeur d'un système de cryptographie destiné aux besoins de la guerre est en raison inverse du secret qu'exige son maniement ou sa composition. ... [et] qu'un chiffre n'est bon qu'autant qu'il reste indéchiffrable pour le maître lui-même qui l'a inventé : Ars ipsi secreta magistro » (un art caché au maître lui-même).



Auguste Kerckhoffs 1883 :

« Il vient d'être présenté à la Commission de télégraphie militaire un nouveau système de cryptographie qui me paraît réaliser tous les desiderata que j'ai exposé en commençant : indéchiffrabilité complète, simplicité, non nécessité du secret ; des considérations de haute convenance m'empêchent d'en dire davantage pour le moment » (sic)

« Le corps de l'un des sous-officiers allemands fut repêché par les Russes quelques heures plus tard et, serrés contre sa poitrine par des bras rendus rigides par la mort, étaient le chiffre et le livre de code de l'armée allemande » Winston Churchill (1874-1965), The World Crisis 1923



CLASS OF SERVICE DESIRED	
Fast Day Message	☒
Day Letter	☒
Night Message	☐
Night Letter	☐

Patrons should mark, as X, opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Receiving No.	3500
Class	
Time Filed	

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

GERMAN LEGATION

MEXICO CITY

130	13042	13401	8501	115	3528	416	17214	6491	11310
18147	18222	21560	10247	11518	23677	13605	3494	14936	
98092	5905	11311	10392	10371	0302	21290	5161	39695	
23571	17504	11269	18276	18101	0317	0228	17694	4473	
23284	22200	19452	21589	67893	5569	13918	8958	12137	
1333	4725	4458	5905	17166	13851	4458	17149	14471	6706
13850	12224	6929	14991	7382	15857	67893	14218	36477	
5870	17553	67893	5870	5454	16102	15217	22801	17138	
21001	17388	7446	23638	18222	6719	14331	15021	23845	
3156	23552	22096	21604	4797	9497	22464	20855	4377	
23610	18140	22260	5905	13347	20420	39689	13732	20667	
6929	5275	18507	52262	1340	22049	13339	11265	22295	
10439	14814	4178	6992	8784	7632	7357	6926	52262	11267
21100	21272	9346	9559	22464	15874	18502	18500	15857	
2188	5376	7381	98092	16127	13486	9350	9220	76036	14219
5144	2831	17920	11347	17142	11264	7667	7762	15099	9110
10482	97556	3569	3670						

BEPNSTOPFF.

Charge German Embassy.

JAN 18 1917

862.2012/324

« La solution d'un télégramme est impossible si la machine tombe dans des mains non autorisées puisqu'elle nécessite le positionnement préalable d'une clé. »



Arthur Scherbius





Enigma modèle C

- placements des trois tambours :
 $3! = 6$
- positions initiales des trois tambours : $26^3 = 17\,576$
- Nombre total de combinaisons :
 $6 \times 17\,576 = 105\,456$



Enigma modèle wehrmacht

- relier 6 paires de fiches parmi 26 :

$$\frac{26!}{(26-12)! \times 2^6 \times 6!} = 1,004 \times 10^{11}$$

- nombre total de combinaisons :

$$6 \times 17756 \times 1,004 \times 10^{11} \approx 1,059 \times 10^{16} \approx 2^{53}$$

Trois mathématiciens polonais contre l'Enigma



Marian Rejewski (1905-1980)



Jerzy Różycki (1909-1942)



Henryk Zygalski (1906-1978)



FIALKA machine soviétique à 10 rotors



Shafi Goldwasser
(Née en 1958)



Sylvio Micali
(né en 1954)



Neal Koblitz
(né en 1948)



Alfred Menezes
(né en 1965)

A more refined view

